



## netfence 4.2.1



➤ **Administration Guidance**  
Revision 2.6







# Contents

1	Getting Started .....	7
2	Control Centre .....	27
3	Configuration Service .....	41
4	Firewall .....	123
5	VPN .....	199
6	Mail Gateway .....	243
7	DHCP .....	271
8	Log Viewer .....	289
9	Statistics .....	295
10	Eventing .....	305
11	DNS .....	315
12	Proxy .....	323
13	FTP Gateway .....	351
14	Voice over IP .....	355
15	SSH Gateway .....	363
16	Anti-Virus .....	367
17	High Availability .....	375
18	phion management centre .....	387
19	SNMP .....	479
20	OSPF and RIP .....	483
21	Licensing .....	497
22	System Information .....	511
23	Appendix .....	523

# 1. Conventions in this Administration Guidance

## 1.1 Text Conventions

**Table 0-1** Text conventions of the documentation

Convention	Font	Description
<b>Bold</b>	Interstate	This style is used for highlighting certain parts of text.
<i>Italic</i>	Interstate	This style is used for indicating examples.
<b>Bold &amp; Italic</b>	Interstate	This style is used for items that can be found directly in your phion.a User Interface.
Regular	Courier	This style is used for items that have to be/may be entered (for example on command line or URLs)
>	Interstate	This character indicates a multiple step path. For example "Select  <b>Box</b> >  <b>Infrastructure Services</b> " means: first select the  <b>Box</b> entry, then select the  <b>Infrastructure Services</b> entry ...
Signal word: <b>Attention</b>	Interstate	Text equipped with the signal word <b>Attention</b> indicates important information concerning security features, potential problems, performance loss, ...
Signal word: <b>Note</b>	Interstate	Text equipped with the signal word <b>Note</b> indicates useful information for operating/configuring the netfence gateway.

## 1.2 Parameter Lists, Tables and Figures

There are two kinds of tables:

- A table containing parameters is called **parameter list** (numbering example: list 3-9, page 55).
- A table containing no parameters is called **table** (numbering example: table 3-8, page 70).

The numbering of parameter lists, tables, and figures occurs in the following way: **chapter - increasing number**.

Example: figure 3-14 means that the figure is located in chapter 3 (Configuration Service) and is the 14th figure in this chapter.

**Note:**

Tables and parameter lists have their own range of numbers.

Directories:

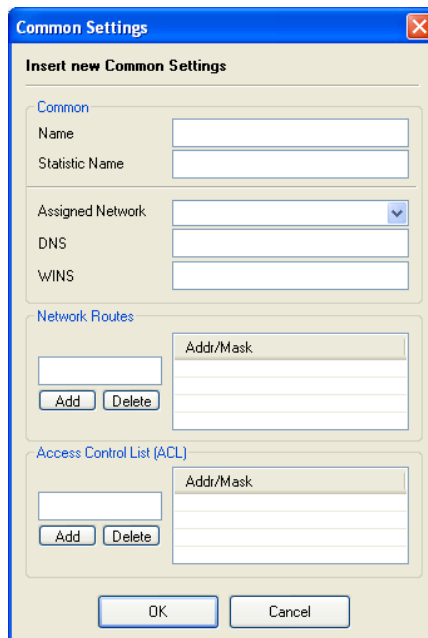
- **Parameter List Directory**, page 557
- **Table Directory**, page 584
- **Figure Directory**, page 590

### 1.2.1 Example

As you can see in the following figure, the dialogue **Common Settings** consists of three **sections**:

- **Common**
- **Network Routes**
- **Access Control List (ACL)**

**Fig. 0-1** Example: Common Settings



Three parameter lists follow this figure, one for every section:

- list 5-31 VPN configuration - Client to Site - External CA tab > Common tab - section Common
- list 5-32 VPN configuration - Client to Site - External CA tab > Common tab - section Network Routes
- list 5-33 VPN configuration - Client to Site - External CA tab > Common tab - section ACL

(Origin: **VPN** - 2.6.2.6 Common Tab, page 216)



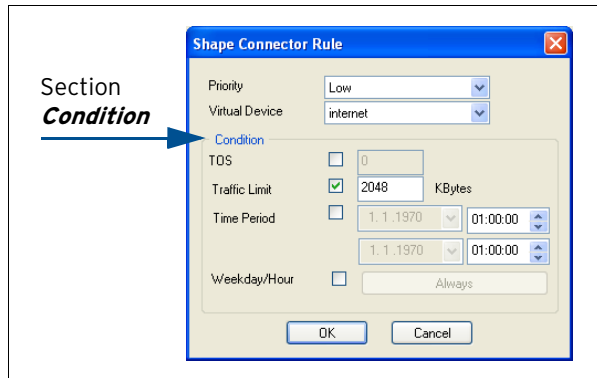
## 2. How to gather Information from this Documentation

### 2.1 Course of Action

How can you find what you are looking for? Try these procedures:

- For information about a particular parameter use the **Index of Configuration Parameters**, page 566.  
At the end of the entry you see the chapter in which the parameter occurs.
- For information about a particular section use the **Index of Dialogue Sections**, page 550.  
At the end of the entry you see the chapter in which the section occurs.

**Fig. 0-2** Example - section Condition



- If you are looking for a certain parameter list, table, or figure use the **Parameter List Directory**, page 557, **Table Directory**, page 584 or **Figure Directory**, page 590.
- For general information use the main directory (**Contents**, page 3) first, then go through the directory of the chosen chapter.
- What's new? Take a look at the **Log of Changes**, page 603.

### 2.2 Feedback

You cannot find the parameter, section, ... in this documentation because it is just not there? Sorry. Please send us an e-mail: [documentation@phion.com](mailto:documentation@phion.com). Thank you.



# Getting Started

<b>1.</b>	<b>Installation of a netfence Gateway</b>	
1.1	General .....	8
1.2	Installation from Scratch .....	8
1.3	Installation with a Saved Configuration .....	8
1.3.1	Crash Recovery .....	8
1.4	Installation & Configuration Walk-through .....	9
<b>2.</b>	<b>phion.i</b>	
2.1	General .....	10
2.2	Creating a "standard" Kickstart Disk .....	10
2.3	Creating a Disk in "Kickstart Only" Mode .....	15
2.4	Creating a Kickstart Disk for Installation via Network .....	15
2.5	phion Multi-Platform Product Support .....	16
<b>3.</b>	<b>phion.a</b>	
3.1	Logging in .....	17
3.2	User Interface .....	17
3.2.1	Start Screen .....	18
3.2.2	Menu Bar .....	18
3.2.3	Tool Bar .....	20
3.2.4	Box Menu .....	20
3.2.5	Main Window .....	20
3.2.6	Mini Map .....	20
3.2.7	Status Bar .....	20
<b>4.</b>	<b>Settings</b>	
4.1	Boxes .....	21
4.2	Client .....	22
4.3	Admin & MC Settings .....	23
4.4	Certificates & Private Keys .....	23
4.4.1	Using Keys on a netfence 4.2 .....	24
4.5	Public Host Keys .....	24
<b>5.</b>	<b>phion Notation</b>	
5.1	Comparison CIDR - phion Notation .....	25

# 1. Installation of a netfence Gateway

## 1.1 General

There are two ways of installing a netfence gateway:

- Installation from Scratch
- Installation with a Saved Configuration

## 1.2 Installation from Scratch

### Note:

This is only a short summary of the installation process. A more detailed step-by-step installation guide can be found in the Quick Start Guide located on the phion CD. Detailed information concerning the usage of the phion.i installation tool can be found at 2. phion.i, page 10.

The basic configuration of a netfence gateway is done with the phion.i installation tool.

Start phion.i from the Application & Documentation CD-ROM and leave the wizard mode at the default setting **Full**.

Enter a hostname and all other information that is needed for creation of the kick-start disk.

After the kick-start disk has been created, insert the Gateway Installation CD-ROM and kick-start disk into your system to begin installation of the netfence gateway.

### Note:

Make sure that booting from CD-ROM is enabled in the computer's BIOS. The installation process itself is fully automatic and needs minimum user interaction.

After successful installation you should be able to connect to the box using the phion.a administration GUI. All further configuration of the netfence gateway is done with the phion.a.

## 1.3 Installation with a Saved Configuration

The reinstallation of an already configured netfence gateway is prepared in two steps. First of all a PAR file (**phion Archive**) containing the complete system configuration is required. Second, the kickstart disk has to be created using the option **Create Kickstart only**.

Copy the PAR file onto the same disk as the kickstart file or, alternatively, make it available for network access. The PAR file name has to begin with "**box**" (for example box.par, box\_*boxname*.par).

Insert Gateway Installation CD-ROM and kickstart disk into your system to begin installation of the netfence gateway.

### Note:

Make sure that booting from CD-ROM is enabled in the computer's BIOS.

### Note:

For details on PAR file creation see **Configuration Service** - 5.3 Creating PAR Files, page 119.

### Note:

For details on kickstart disk creation see 2.3 Creating a Disk in "Kickstart Only" Mode, page 15.

### 1.3.1 Crash Recovery

#### Note:

A backup of the recent configuration is an absolute must for successful and fast crash recovery. A current backup should always be available (**Configuration Service** - 5.3 Creating PAR Files, page 119).

#### 1.3.1.1 Crash Recovery with Identical Hardware

Crash recovery itself works as described in 1.3 Installation with a Saved Configuration, page 8.

#### Attention:

This method only works if identical hardware (CPU-ID, MAC addresses, motherboard ID) is used for recovery.

### 1.3.1.2 Crash Recovery with New Hardware

Crash recovery itself works as described in 1.3 Installation with a Saved Configuration, page 8.

Use of a different hardware than the license has been issued to will cause the license to be invalid. The box will now run in so-called **grace mode**. Nevertheless, even in grace mode the complete functionality of the netfence gateway is guaranteed.

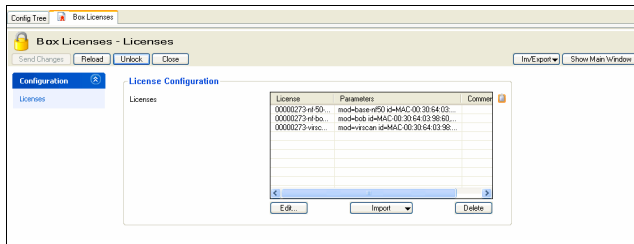
A pop-up window will be displayed as soon as grace mode expires. If, until then, no new license is available, the box gets deactivated.

**Attention:**

To keep up the integrity of the netfence gateway it is of great importance to obtain new licenses for the system as soon as possible.

To import a new license, enter the Configuration window (🔧 **Config**) of the box. There select 📦 **Box** and double-click 📄 **Box Licenses**.

Fig. 1-1 Window Box Licenses in read/write mode



Now lock the window, select the license and remove it by clicking **Delete**. Import the new license by use of the pull-down menu and selection of **Import** (from File or Clipboard).

## 1.4 Installation & Configuration Walk-through

### Step 1 Installation of the box

Gather needed information, create a kick-start floppy disk with phion.i (see 2. phion.i, page 10), and start installation. For more information, see:

- Quick Start Guide
- 2. phion.i, page 10
- **Getting Started**, page 7

### Step 2 Basic configuration

Configure networking and box services (SSH, statistics, logging, box settings, ...). For more information, see:

- **Configuration Service**, page 41

### Step 3 Server configuration

Create a new server and configure it. For more information, see:

- **Configuration Service**, page 41

### Step 4 Check settings

Log into the box with the phion.a administration GUI and check if all servers have been introduced and if box services are up and running. For more information, see:

- **Control Centre**, page 27

### Step 5 Create dedicated HA box (optional)

Create a DHA box and configure its network settings. For more information, see:

- **High Availability**, page 375

### Step 6 Create Services

Create one or more services and configure them. For more information, see:

- **Firewall**, page 123
- **VPN**, page 199
- **DNS**, page 315
- **Mail Gateway**, page 243
- **DHCP**, page 271
- **Proxy**, page 323

### Step 7 Licensing

Obtain licenses for your system (gather necessary information first) and import them. For more information, see:

- **Licensing**, page 497

### Step 8 Backup configuration

After completion of the configuration, create a first backup (PAR file) of your system. For more information, see:

- **Configuration Service** - 5.3 Creating PAR Files, page 119

## 2. phion.i

### 2.1 General

All information required for installing a netfence gateway and/or a phion management centre can be configured using the tool phion.i. The kickstart file, created at the end of a successful phion.i session, is essential for installation.

The executable phion.i is available on your netfence gateway - Application & Documentation CD-ROM and on the Gateway Installation CD-ROM.

#### Note:

Before starting phion.i, we recommend gathering information about:

- Hostname
- Time zone (local or UTC)
- Keyboard layout
- Size of hard disk(s)
- Manufacturer or chip set type of network card(s)
- Management IP of the netfence gateway
- Password for root and phion service user

#### Note:

For installation via network (either HTTP or FTP server) you need to have a proper boot image for the kickstart disk (available on your Gateway Installation CD-ROM, directory `/images`) and you need to know the path to the CD image. For information concerning how to create a bootable kickstart disk, please have a look at 2.4 Creating a Kickstart Disk for Installation via Network, page 15.

#### Note:

The phion M USB stick may be used to recover all USB enabled Heavensgate appliances.

#### Note:

Local administration rights are needed to install files on an USB stick.

#### Note:

For installation with USB stick, a supported and properly formatted USB stick is needed. One of the following formattings should be used:

**Table 1-1** USB stick - Formatting

Installation system	FAT16	FAT32
phion Appliances - M-series	✓	-
SECUDOS Appliances	✓	-
Heavensgate Appliances	✓	✓
Standard-hardware	✓	✓
Crossbeam Appliances - C-series	✓	-

### 2.2 Creating a "standard" Kickstart Disk

To start the configuration procedure, copy phion.i.exe onto your local workstation and double-click it.

#### Step 1 Selecting the wizard mode

Select **Full** mode (default) when installing a system for the first time. Select **Create Kickstart only** when reinstalling a netfence gateway (for example for disaster recovery) or when installing a netfence gateway that is administered by a management centre (see 2.3 Creating a Disk in "Kickstart Only" Mode, page 15).

Continue with **Next**.

#### Step 2 Configuring Installation-Mode Settings

Select your installation source here. This can either be a

- **CD-ROM or USB Stick** (default)
- **phion M USB Stick**
- or a network server (**Network**).

Selecting server-based installation mode activates the configuration section on the right side providing the following parameters:

**List 1-1** Configuring Installation Settings with phion.i

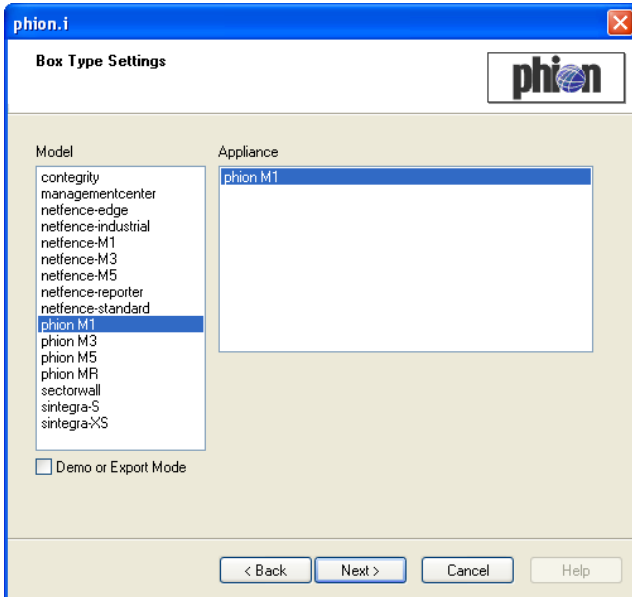
Parameter	Description
<b>URL</b>	Enter the path to the CD image here. The following syntax is appropriate: <code>ftp://user:password@server_ipaddress/path</code> <code>user:password@server_ipaddress/path/</code>
<b>IP address</b>	Enter an installation IP address here. This IP will be active during setup and must be able to communicate with the installation source.
<b>Subnet mask</b>	Enter an appropriate subnet mask here (default: <b>255.255.255.0</b> ).
<b>Gateway</b>	Enter a gateway's IP address here if it is needed.
<b>Nameserver</b>	You may optionally specify a DNS server here.
<b>Device</b>	Configure the network interface card here, which is active during installation (default: <b>eth0</b> ).

Continue with **Next**.



### Step 3 Defining Box Type settings

Fig. 1-2 Defining Box Type Settings with phion.i



Here select the hardware type you are installing.

The Model/Appliance combination determines product specific default settings and availability of services, again with typical default settings. Make the correct selection to achieve full profit from this feature.

Combine **netfence-standard/standard-hardware** if you are not using one of the listed appliance models. netfence default settings then apply for all services.

Combine **managementcenter/standard-hardware**, if you are installing a management centre.

Each type's typical characteristics are listed at the end of this chapter (2.5 phion Multi-Platform Product Support, page 16). For a list of default values see 2. Parameter Defaults for netfence Appliances, page 530.

Select the **Demo or Export Mode** checkbox if you are installing a system for testing purposes.

**Note:**

On unlicensed netfence gateways (DEMO Mode) encryption is restricted to DES. Stronger encryption is only available on systems without export flag.

Table 1-2 Types of DEMO versions in netfence 4.2

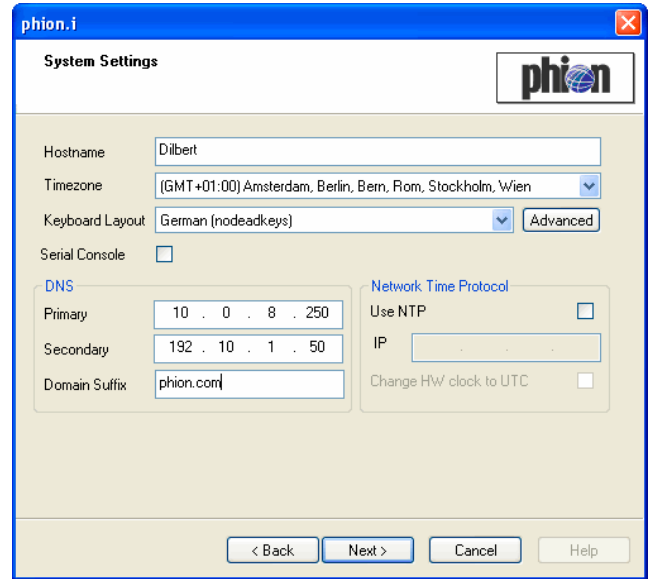
Version	Characteristics
DEMO	cryptographic weak (DES, RSA-512)
Testing License with export flag	cryptographic weak (DES, RSA-512)
Testing License without export flag	cryptographic strong

**Note:**

Box Type Settings defines the content of the configuration file **Box Properties (Configuration Service - 2.2.2 Box Properties, page 51)**.

### Step 4 Defining System Settings

Fig. 1-3 Configuring System Settings with phion.i



List 1-2 Configuring System Settings with phion.i

Parameter	Description
<b>Hostname</b>	Specify a name for the host you are installing without its domain suffix. In a hostname only characters (a-z, A-Z), numbers (0-9), and hyphens ("-") are allowed. The maximum length of this parameter is 25 characters. Later change of the hostname is possible ( <b>Configuration Service - 2.2.3.1 System Access, page 54</b> ). <b>Note:</b> This is a mandatory field. Installation cannot continue without a hostname.
<b>Time Zone menu</b>	Select the proper time zone for the netfence gateway.
<b>Keyboard Layout</b>	This menu allows you to select the required keyboard layout. <b>Note:</b> If the suggested keyboard layouts are insufficient, experienced users may select the appropriate setting by using the <b>Advanced ...</b> option.
<b>Serial Console</b>	Ticking this checkbox activates the interface for serial console. <b>Attention:</b> Make sure to activate a serial port in your server's BIOS when using this option.

List 1-3 Configuring System Settings with phion.i - section DNS

Parameter	Description
	<b>Attention:</b> If the DNS servers are located in a different subnet than the box and the phion.a administration computer, routing has to be configured correspondingly in order to make these addresses accessible for the box ( <b>Configuration Service - 2.2.5.5 Network Routes, page 68</b> ).
<b>Primary / Secondary</b>	These fields are used for defining DNS servers.
<b>Domain Suffix</b>	If the box is located in a DNS domain, the corresponding domain can be entered in this field.

List 1-4 Configuring System Settings with phion.i - section Network Time Protocol

Parameter	Description
	<b>Attention:</b> If the NTP server is located in a different subnet than the box and the phion.a administration computer, the routing has to be configured correspondingly in order to make the address accessible for the box ( <b>Configuration Service - 2.2.5.5 Network Routes, page 68</b> ).

**List 1-4** Configuring System Settings with phion.i - section Network Time Protocol

Parameter	Description
<b>Use NTP</b>	If a timeserver is available you can activate its use by ticking the checkbox 'Use NTP'. This will activate the following parameters.
<b>IP</b>	This field holds the IP address of the NTP server.
<b>Change HW clock to UTC</b>	This checkbox can be used for changing the BIOS clock to universal time. <b>Note:</b> Using this option is highly recommended.

Continue with **Next**.

### Step 5 Configuring Partition Settings

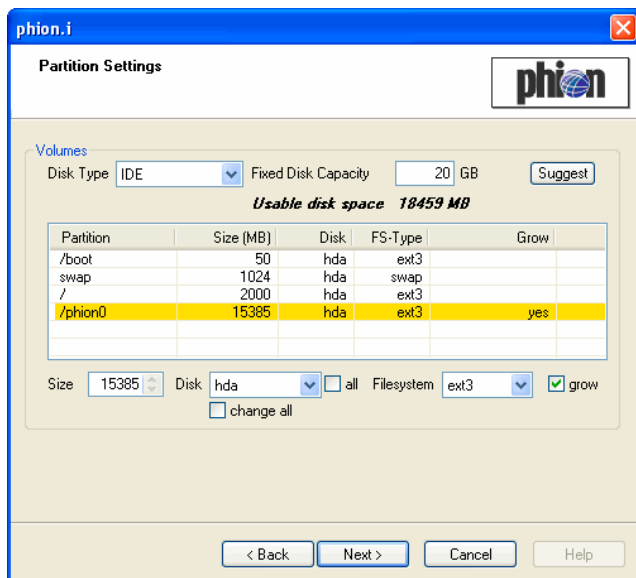
Select the **Disk Type** that suits your system. The following disk types are available for selection:

- **IDE** (default)
- **SCSI**
- **CCISS**
- **RD**

Thereafter insert the **Fixed Disk Capacity** and click **Suggest**. This will lead to an automatic partitioning suggestion, which will work for most systems. Of course you still have the option to edit each partition manually after suggestion. Select the partition you want to modify (this is now highlighted in yellow) and edit the fields shown below the partition list.

The following parameters are available for editing the partition suggestion:

**Fig. 1-4** Configuring Partition Settings with phion.i



**List 1-5** Configuring Partition Settings with phion.i

Parameter	Value																														
<b>Size</b>	Assign disk space of your choice here.																														
<b>Disk menu</b>	Disk names are assigned according to the selected <b>Disk Type</b> . <table border="1"> <thead> <tr> <th>Disk No.</th> <th>IDE (Linux)</th> <th>SCSI (Linux)</th> <th>CCISS</th> <th>RD</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>hda</td> <td>sda</td> <td>cciss/c0d0</td> <td>rd/c0d0</td> </tr> <tr> <td>2</td> <td>hdb</td> <td>sdb</td> <td>cciss/c0d1</td> <td>rd/c0d1</td> </tr> <tr> <td>3</td> <td>hdc</td> <td>sdh</td> <td>cciss/c0d2</td> <td>rd/c0d2</td> </tr> <tr> <td>4</td> <td>hdd</td> <td>sdd</td> <td>cciss/c0d3</td> <td>rd/c0d3</td> </tr> <tr> <td>5</td> <td>hde</td> <td>sde</td> <td>cciss/c0d4</td> <td>rd/c0d4</td> </tr> </tbody> </table> <p>Select the <b>all</b> checkbox to display all disk types in the <b>Disk</b> list. Select the <b>change all</b> checkbox to change the disk type for all partitions and not only for the selected one.</p>	Disk No.	IDE (Linux)	SCSI (Linux)	CCISS	RD	1	hda	sda	cciss/c0d0	rd/c0d0	2	hdb	sdb	cciss/c0d1	rd/c0d1	3	hdc	sdh	cciss/c0d2	rd/c0d2	4	hdd	sdd	cciss/c0d3	rd/c0d3	5	hde	sde	cciss/c0d4	rd/c0d4
Disk No.	IDE (Linux)	SCSI (Linux)	CCISS	RD																											
1	hda	sda	cciss/c0d0	rd/c0d0																											
2	hdb	sdb	cciss/c0d1	rd/c0d1																											
3	hdc	sdh	cciss/c0d2	rd/c0d2																											
4	hdd	sdd	cciss/c0d3	rd/c0d3																											
5	hde	sde	cciss/c0d4	rd/c0d4																											
<b>File system menu</b>	The following file systems are available for selection: <b>ext2</b> - standard Linux file system <b>ext3</b> (default) - journal extension to ext2 on Linux; journaling can result in a massively reduced time spent recovering a file system after a crash, and therefore this is recommended for high demand environments, where high availability is important. <b>reiserfs</b> - journaling file system																														
<b>grow</b> checkbox	By ticking this checkbox, the selected partition will grow to the maximum available size. This way you do not have to specify the exact size of your disk.																														

#### Note:

If you have selected a specific appliance model in the box type settings screen (see Step 3) partitioning settings will be suggested.

Continue with **Next**.

### Step 6 Configuring your network interfaces

In the next step the appropriate network interface cards (NICs) have to be configured.

For adding a new NIC, click **Add ...**. This opens a NIC reseller list.

Select a **Reseller** to display a list of available NICs. If you use more cards of a single model, you can enter the number of these cards in the upper right corner of this dialogue (field **Number**).

#### Attention:

If you use multi-port cards, each port counts as one card (for example, a dual-port card counts as two cards).

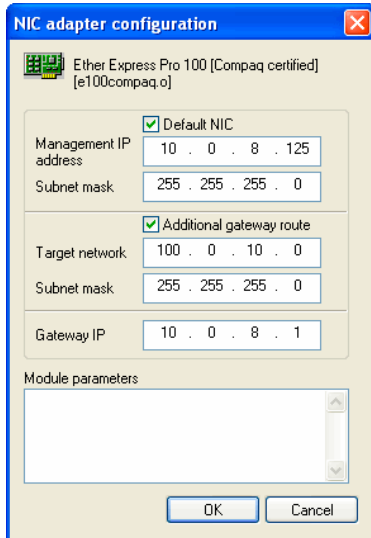
Should the offered NICs not suit your system click **Advanced ...** (lower left corner) where you can select a certain module that fits your NIC.

#### Note:

Linux does not have special drivers for every single model of network card but a family of cards using the same network chip set. Again you can insert the number of cards you wish to use.

When you click **OK** the NIC is added to your configuration and is ready for adapting. So select the NIC (now highlighted in yellow) and either click on **Properties ...** or simply double-click.

Fig. 1-5 NIC adapter configuration parameters



The following parameters are available for configuration:

List 1-6 NIC Adapter configuration parameters

Parameter	Description
<b>Default NIC</b> checkbox	Selecting the checkbox makes this NIC the default one, which means that management access to the netfence gateway will be provided across this network interface. The default NIC has a hook symbol assigned in the main dialogue.
<b>Management IP address / Subnet mask</b>	This is the IP address through which your netfence gateway will be administered.
<b>Additional gateway route</b> checkbox	This checkbox has to be selected if the box administrator's workstation is in a subnet. Selecting the checkbox makes the parameters <b>Target Network</b> , <b>Subnet Mask</b> and <b>Gateway IP</b> available for configuration. Configure the route from the workstation, which will be administering with phion.a, to the host here.
<b>Module parameters</b> field	Experienced Linux users may use this field to insert further module options for network cards. <b>Note:</b> Be aware that incorrect parameters can disable correct module loading.

Other network cards besides the default one can either be configured later using phion.a or immediately with phion.i. For configuration with phion.i simply add new NICs as mentioned above and configure them as needed.

**Note:**

If you have selected a specific appliance model in the box type settings screen (see Step 3) interface naming settings will be suggested.

Continue with **Next**.

**Step 7 Configuring Security Settings**

This dialogue offers several security-relevant parameters:

List 1-7 Configuring Security Settings with phion.i

Parameter	Description
<b>Licenses</b> list	This listing displays the available licenses. In order to import licenses, click <b>Import License from File ...</b> and select the corresponding <b>.lic</b> file. <b>Note:</b> If no license is imported here, your netfence gateway will run in demo mode until a valid license is applied.
<b>ACL</b> list	The Access Control List (ACL) contains IP addresses/netmasks which have exclusive access to the management IP address. The ACL protects the box from Denial of Service (DoS) attacks. <b>Note:</b> In order to avoid unnecessary exposure of the netfence gateway to DoS attacks, restrict the scope of the ACL to addresses from which access to the management IP address is to be granted.

List 1-8 Configuring Security Settings with phion.i - section Root Login

Parameter	Description
<b>Root RSA Key</b>	This section enables you to handle the RSA key for login on the netfence gateway. The pull-down menu <b>Create/Ex/Import</b> offers several options for this occasion.
<b>Authentication Mode</b>	This parameter is used for defining the required security features for a successful login. Available options are: <b>Key-OR-Password</b> (default), <b>Password</b> , <b>Key</b> and <b>Key-AND-Password</b> .
<b>Password</b>	This parameter is mandatory for security reasons, in order to protect the netfence gateway from unauthorised login on root level.

List 1-9 Configuring Security Settings with phion.i - section phion Login

Parameter	Description
<b>Password</b>	The parameter <b>Password</b> is mandatory for security reasons in order to protect the netfence gateway from unauthorised login on phion support level (user phion).

Continue with **Next**.

**Step 8 Selecting required Software Packages**

List 1-10 Configuring Software Packages with phion.i - section Software Packages

Parameter	Description
<b>netfence base system</b> checkbox	This checkbox is selected by default and cannot be deactivated. This is because every netfence gateway requires certain packages to run (for example phionOS, ...)
<b>Install Utilities</b> checkbox	Selecting this checkbox adds several additional programs, utilities, and, the kernel sources. <b>Note:</b> Activating this option is not recommended and only useful if you want to compile your own kernel and/or modules. Lifecycle management (for example upgrades) is not supported for systems with utilities installed.
<b>Architecture</b> menu	This menu provides the following types of software architecture: <b>Auto</b> (default) - installer selects the proper architecture automatically <b>i386</b> - architecture required for regular systems

List 1-11 Configuring Software Packages with phion.i - section Advanced

Parameter	Description
<b>Kernel Parameter</b> field	This field allows to enter kernel-related parameters. <b>Attention:</b> When using this field be absolutely sure to know what you are doing. Contact phion support before entering anything into this field. <b>Note:</b> This parameter takes no effect when parameter <b>Kickstart only</b> or <b>Install mode &gt; CD-ROM or USB Stick</b> has been selected.

List 1-11 Configuring Software Packages with phion.i - section Advanced

Parameter	Description
<b>L1LO linear</b> checkbox	Selecting this checkbox may be required by some controllers.
<b>Do not eject CD-ROM after installation</b>	Select this checkbox to prevent CD-ROM ejection after installation has completed.
<b>No graphic adapter available</b>	Select this checkbox if your system does not employ a graphic adapter and you intend administering it via a serial console.
<b>No ACPI</b>	Select this checkbox if your system does not employ an Advanced Configuration and Power Interface (ACPI). <b>Note:</b> This parameter takes no effect when parameter <b>Kickstart only</b> or <b>Install mode &gt; CD-ROM or USB Stick</b> has been selected.

Continue with **Next**.

### Step 9 Configuring Script Settings

List 1-12 Configuring Script Settings with phion.i - section Installation scripts

Parameter	Description
<b>Preinstall-script</b>	Click <b>Modify ...</b> if you want to insert a script that is started prior to the installation process. This could be some preparation of the system in order to tweak system parameters. <b>Note:</b> Before doing so, please contact phion Support
<b>Postinstall-script</b>	Click <b>Modify ...</b> to modify the script provided by phion that is started right after the installation process. Especially when installing via network and having a PAR file with pre-defined configuration, modifying this script comes handy as it also allows you to install the PAR file via network (see below for an example).  ... for i in /mnt/floppy/box*.par; do /bin/echo copying par \\${i} /bin/cp -f \\${i} /opt/phion/update/box.par done  cd /tmp wget ftp://user:password@server/ box_name.par cp box_name.par /opt/phion/update/box.par

List 1-13 Configuring Script Settings with phion.i - section Installation-script files

Parameter	Description
<b>Write USB stick</b>	Set this parameter to <b>yes</b> (default: <b>no</b> ) to allow saving installation script files to a USB stick.
<b>Save to</b>	This field specifies the kickstart file's saving location. When parameter <b>Write USB stick</b> is set to <b>yes</b> , the USB stick is selectable in this field. <b>Note:</b> If parameter <b>Write USB stick</b> is set to <b>yes</b> but no option is available, simply reconnect the USB stick, switch back to <b>no</b> and then to <b>yes</b> again.

List 1-14 Configuring Script Settings with phion.i - section Box public key

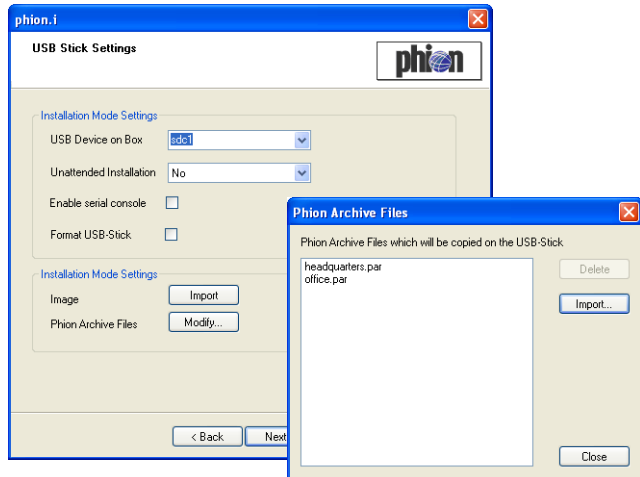
Parameter	Description
<b>Save to Disk</b> checkbox	Select this checkbox to save the box public key to the kickstart disk (path defined above).
<b>Enter in Registry</b> checkbox	Select this checkbox to insert the box public key to the local registry (Default).

### Step 10 Configuring USB Stick Settings

(only available if parameter **Write USB stick** is set to **yes**)

This configuration dialogue provides USB stick-relevant settings and additionally allows importing the ISO image.

Fig. 1-6 Configuring USB stick settings with phion.i



**Attention:**  
Consider the following restrictions:  
Only USB sticks with **one** partition are supported.  
Some BIOS versions seem to be able to manage a USB harddisk but in fact they are not.  
When using **Unattended Installation** the USB stick may contain only **one** par-file or **one** pgz-file.  
Any data on the USB stick will be lost.

The following parameters are available:

List 1-15 Configuring USB Stick Settings with phion.i - section Installation Mode Settings (1)

Parameter	Description																		
<b>USB Device on Box</b>	Linux handles USB sticks as SCSI devices and therefore addresses them as sda, sdb, sdc, ... On the box which is prepared for setup the USB stick with the installation files thus has to be mounted onto an available Linux device. There, depending on the number of already installed SCSI hard disks, the USB stick can be addressed as displayed in the following table: <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>SCSI Harddisks</th> <th>Addressed as</th> <th>USB stick addressed as</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>-</td> <td>sda1 (default)</td> </tr> <tr> <td>1</td> <td>sda</td> <td>sdb1</td> </tr> <tr> <td>2</td> <td>sda, sdb</td> <td>sdcl</td> </tr> <tr> <td>3</td> <td>sda, sdb, sdc</td> <td>sddl</td> </tr> <tr> <td>...</td> <td>...</td> <td>...</td> </tr> </tbody> </table>	SCSI Harddisks	Addressed as	USB stick addressed as	0	-	sda1 (default)	1	sda	sdb1	2	sda, sdb	sdcl	3	sda, sdb, sdc	sddl	...	...	...
SCSI Harddisks	Addressed as	USB stick addressed as																	
0	-	sda1 (default)																	
1	sda	sdb1																	
2	sda, sdb	sdcl																	
3	sda, sdb, sdc	sddl																	
...	...	...																	
<b>Unattended Installation</b>	Setting this parameter to <b>yes</b> (default: <b>no</b> ) starts the installation process completely without any user interaction (no Welcome screen, no Installation Complete screen) as soon as the USB stick is plugged in. <b>Attention:</b> Use USB sticks with activated Unattended Installation with extreme caution to avoid an "accidentally" initiated box installation. <b>Note:</b> This type of installation should only be used in conjunction with appliances.																		
<b>Enable serial console</b>	Selecting this checkbox redirects installation output to the serial console.																		
<b>Format USB-Stick</b>	Selecting this checkbox formats the USB stick before the installation files are copied onto it. <b>Note:</b> All data on the stick will be erased.																		

**List 1-16** Configuring USB Stick Settings with phion.i - section Installation Mode Settings (2)

Parameter	Description
<b>Image</b>	The pull-down menu of this parameter allows selecting the installation media: <b>Create from CD</b> - creates an ISO image directly from a CD-ROM selected in the list <b>Copy ISO image</b> - imports an already existing ISO image file to the USB stick <b>Attention:</b> Any selection starts the related process immediately without user interaction.
<b>Phion Archive Files</b>	If you are installing with USB stick you may add phion archive files (*.par) and compressed phion archive files (*.pgz) files to the kickstart disk in order to take over complete box configurations when installing. If you have added more than one archive file you will be queried which one to apply during installation.

## 2.3 Creating a Disk in "Kickstart Only" Mode

**Note:**

Kickstart files created in this mode can only be applied together with a **phion Archive (PAR) file (Configuration Service - 5.3 Creating PAR Files, page 119)**. The PAR file has to be available on either disk or network. If the PAR (.par) file is too big to be saved to the floppy disk, consider creating a compressed PAR (.pgz) file instead.

**Create Kickstart only** mode may be used when:

- reinstalling a netfence gateway (disaster recovery for example).
- installing a netfence gateway administered by a management centre.

When creating a kickstart file using mode "kickstart only", it can only include settings that cannot be included in the PAR file. These settings are:

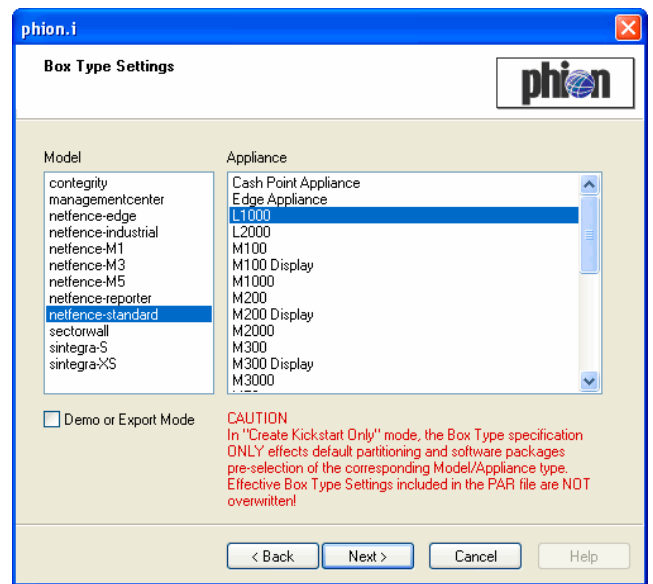
- **Box Type Settings / Software Packages** pre-selection assigned to a specific Model/Appliance type
- **Partition Settings**

To create a kickstart file in "kickstart only" mode, proceed as described in 2.2 Creating a "standard" Kickstart Disk.

**Note:**

Only the settings stated above will be effective when installing the system. Effective settings included in the PAR file will **NOT** be overwritten.

**Fig. 1-7** Box Type Settings window in Create Kickstart only mode



For a description of system installation with a PAR file see 1.3 Installation with a Saved Configuration, page 8.

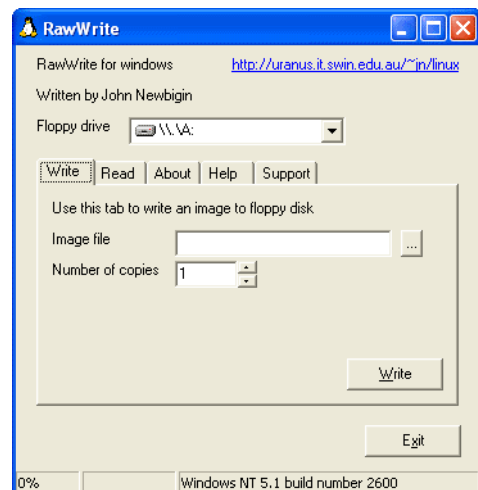
## 2.4 Creating a Kickstart Disk for Installation via Network

For creating a bootable kickstart disk, simply enter /images on your Gateway Installation CD-ROM.

**Step 1 Starting rawrwitewin.exe**

Via this tool the boot disk is equipped with the boot image. Start the tool by double-clicking rawrwitewin.exe.

**Fig. 1-8** rawrwitewin.exe - Start screen



## Step 2 Selecting the proper boot image

The boot image has to be created in dependence of the used network interface card. For determination of the correct image have a look at the README file within the /images directory.

Then select the chosen file in parameter **Image file**, insert a floppy disk and click **Write** to start the boot disk creation.

### Attention:

The disk will be formatted when creating the boot disk.

## Step 3 Configuring a kickstart disk for network installation

You can now start the configuration of the kickstart disk for network installation as mentioned above.

## 2.5 phion Multi-Platform Product Support

phion netfence 4.2 may be installed on standard server systems (A list of supported hardware can be obtained on the phion homepage), but also offers support for a big variety of appliance models distributed by phion partners. Each appliance model is equipped with specific default settings and is designated for installation of specific services.

When creating a kickstart disk, the installation tool phion.i asks for information about the to-be-installed system. Each specific Model/Appliance combination (see Step 3 Defining Box Type settings, page 11) therefore determines product specific default settings and availability of services in conjunction with typical default settings.

The list below gives an overview of service availabilities for the respective systems. Availability of services applies to both, box and MC systems likewise. A listing with the respective default settings is available in the Appendix (see 2. Parameter Defaults for netfence Appliances, page 530).

**Table 1-3** Availability of services on Appliance Models

Product	Module	netfence-standard	netfence-industrial	netfence-edge	netfence-sintegra XS	netfence-sintegra S	netfence-contegrity	netfence-sectorwall	netfence-sectorwall
Firewall	firewall	✓	✓	✓	✓	✓	-	✓	✓
DHCP Relay	dhcprelay	✓	✓	✓	✓	✓	-	✓	✓
VPN Server	vpnsrvr	✓	✓	✓	✓	✓	-	-	✓
HTTP-Proxy	proxy	✓	✓	-	✓	✓	✓	-	✓
URL Filter	cofs	✓	✓	-	✓	✓	✓	-	✓
Mail Gateway	mailgw	✓	-	-	-	✓	✓	-	✓
SPAM Filter	spamfilter	✓	-	-	-	✓	✓	-	✓
FTP Gateway	ftpgw	✓	✓	-	-	-	✓	✓	✓
SSH Proxy	sshprx	✓	✓	-	-	-	✓	✓	✓
Antivirus	virscan	✓	✓	-	-	✓	✓	-	✓
Secure Web Proxy	sslprx	✓	✓	-	-	-	✓	-	✓
Policy Server	policyserver	✓	✓	✓	✓	✓	✓	✓	✓
DNS Server	dns	✓	-	-	-	-	✓	-	✓
DHCP Enterprise Server	dhcpe	✓	✓	-	✓	✓	✓	-	✓
SNMPd	snmp	✓	✓	✓	✓	✓	✓	✓	✓
OSPFv2-Router	ospf	✓	✓	-	✓	✓	✓	✓	✓



### 3. phion.a

The program phion administration User Interface - phion.a (available on your Application CD-ROM) - is the tool to administer phion netfence.

**Note:**

It is highly recommended to use the phion.a delivered with the Application CD to ensure that all features of the netfence gateway are available. If it is necessary to change the phion.a, please contact the phion Support for detailed information which version of phion.a should be used.

#### 3.1 Logging in

Login is started by clicking twice on the phion.a executable. This opens the login dialogue (figure 1-9).

Fig. 1-9 Login dialogue



**Note:**

When logging in for the first time, an additional window pops up where you may define whether you want to use phion.a in Basic or Advanced mode. The advanced view provides additional configuration options and addresses experienced administrators. Select your configuration view by clicking either **Basic Mode** or **Advanced Mode**. However, you may change your selection globally via **Settings > Client** tab through option **Advanced Mode Configuration**. Additionally, if available, you may change the currently active view per session on the fly by selecting either **Basic View** or **Advanced View** in the navigation bar of the corresponding configuration window.

The header of this dialogue displays the version and build number of the phion.a tool:

- buttons **Box / MC**  
These two buttons define which kind of netfence system you are logging into. Especially when logging into a management centre (**MC**) a correct selection is required due to the different IP addresses that are used (**Box** - IP address of the netfence gateway itself; **MC** - Management IP address).
- **Box-Address / MC-Address** line & menu  
Enter the IP address or DNS-resolvable name to which you wish to connect. For enhanced comfort, the menu provides every IP address that was used for connection via phion.a before. At the same time, the selection **Box** or **MC** address (see above) is reassigned and does not have to be re-entered.
- **Login** line  
Enter the login name of the administrator.
- **Password** line  
Enter the password.

#### 3.2 User Interface

The User Interface is divided into five functional sections. The upper frame contains the phion.a menu and tool bar. The left frame contains the box menu. The right frame, also called mini map, displays either the currently open box configuration or a history of boxes and MCs you have already connected to. You can click on the symbols to connect to these systems again. On the bottom of the user interface you will find the status bar with a status indication. Finally, the centre of the screen contains the main configuration window.

Fig. 1-10 phion.a User Interface



### 3.2.1 Start Screen


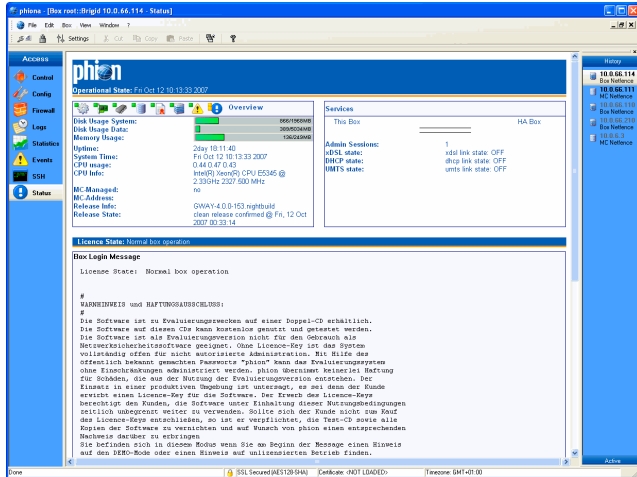
When connecting to a netfence gateway, the first screen shows a summary of the system (figure 1-11). This screen is accessible any time by selecting  **Status Info** from the box menu.

Fig. 1-11 Start screen



The line **Information Box** displays the system's uptime in hours.

Table 1-4 Contents of the Overview segment













Line	Description
Overview	Displays an overview of the system by using a colour code ( <b>green</b> - everything is OK; <b>yellow</b> - something is not working properly and a check is recommended; <b>red</b> - something is not working properly and a check is mandatory) and the following icons:
	Status of the servers ( <b>Control Centre</b> - 2.1 Server Tab, page 29)
	Status of the network ( <b>Control Centre</b> - 2.2 Network Tab, page 30)
	Status of the processes ( <b>Control Centre</b> - 2.3 Processes Tab, page 36)
	Disk usage ( <b>Control Centre</b> - 2.4 Resources Tab, page 36)
	Validity of certificates/licenses ( <b>Control Centre</b> - 2.5 Licenses Tab, page 37)
	Status of the box ( <b>Control Centre</b> - 2.6 Box Tab, page 38)
	Status of the operative-relevant event monitoring ( <b>Eventing</b> - 2.1.2 Severity Tab, page 307)
	Status of the security-relevant event monitoring ( <b>Eventing</b> - 2.1.2 Severity Tab, page 307)
Disk Usage System	Bar graph displaying the current load on the system partition ( <code>/root</code> ). On the right side of the bar the currently used and the maximum available disk space are shown.
Disk Usage Data	Bar graph displaying the current load on the data partition ( <code>/phion0</code> ). On the right side of the bar the currently used and the maximum available disk space are shown.

Table 1-4 Contents of the Overview segment

Line	Description
Memory Usage	Bar graph displaying the current memory load of the system. On the right side of the bar the currently used and the maximum available memory are shown.
Uptime	Displays uptime of the system
System Time	Displays current system time
CPU usage	Displays average CPU load (first value: load within the last minute; second value: load within the last 5 minutes; third value: load within the last 15 minutes)
CPU Info	Displays information concerning system's CPU
MC-Managed	Displays whether the netfence gateway is administered via a management centre.
MC-Address	If the netfence gateway is administered via an MC, the management IP address of the MC is displayed here.
Release Info	Displays the software version (inclusive build number) installed on this netfence gateway.
Release State	Displays software version status ( <b>Control Centre</b> - 2.5 Licenses Tab, page 37)

The **Services** section gives a quick overview of the services on the netfence gateway. Each configured service is shown with its icon, name, and type in brackets. The status of the services is displayed by four types of icons on the left:


-  Service is up
-  Service is blocked
-  Service is stopped
-  Service is blocked, stopped or disabled (inherited property because the server has been blocked, stopped, or disabled)

Additionally, this section informs about the number of active **Administration Sessions**.


The **License State** line shows the current operation mode (**Control Centre** - 2.5 Licenses Tab, page 37).

The **Box Login** Message section displays the messages that are configured as described in **Configuration Service** - 5.1.6 Message Board, page 105.

### 3.2.2 Menu Bar

The menu bar consists of the phion logo  and the menus **File, Edit, Box, View, Window** and **?**.

#### 3.2.2.1 phion Logo Menu

This menu contains commands that are known from MS Windows, such as **Restore, Move, Size, ...** The additional menu item  **Next** allows you to switch from one box interface to another (as long as multiple boxes are opened within the phion.a).

### 3.2.2.2 File Menu

- Menu entry **Login ...**  
This command starts the login window which is needed to get access to a netfence system (see 3.1 Logging in, page 17).
  - Menu entry **Login SSH ...**  
This entry starts the login screen as shown in figure 1-9, page 17. The difference is that after successful login a SSH connection to the box is started.
- Note:**  
For security reasons it is necessary to enter the correct user and password once again when entering the SSH interface.
- Menu entry **Lock**  
This command allows you to lock the phion.a user interface (for example when leaving the workplace). To unlock the phion.a, re-enter the correct user and password into the login screen, which is opened as soon as the phion.a is locked.
  - Menu entry **Settings ...**  
Due to its complexity please refer to a description of this menu item at 4. Settings, page 21
  - Menu entry **Print Setup ...**  
The phion.a allows you to print log files, rule sets, ... Configure your printer by using this menu item.
  - Menu entry **Exit**  
This command closes the phion.a application.

### 3.2.2.3 Edit Menu

The items within this menu have the same meaning and function as known from MS Windows.

### 3.2.2.4 Box Menu

The box menu contains all available services.

**Note:**  
The service item order of the pull-down box menu does not match with the order of the phion.a user interface box menu.

Currently, the following box menu entries are available:

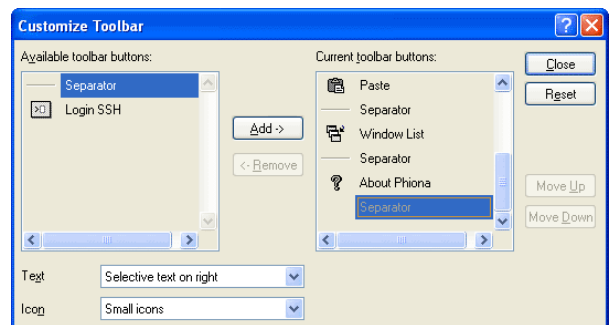
- **Config**  
**Configuration Service**, page 41
- **Control**  
**Control Centre**, page 27
- **Firewall**  
**Firewall**, page 123
- **VPN**  
**VPN**, page 199
- **Logs**  
**Log Viewer**, page 289

- **Statistics**  
**Statistics**, page 295
- **Event**  
**Eventing**, page 305
- **SSH**  
see documentation Command Line Interface
- **Message**  
**Configuration Service** - 5.1.6 Message Board, page 105
- **MailGW**  
**Mail Gateway**, page 243
- **DHCP**  
**DHCP**, page 271
- **Proxy**  
**Proxy**, page 323
- **Reload Box Service**  
This command refreshes the service icons view in the box menu of the phion.a user interface. Apply it for instance after having created a service.

### 3.2.2.5 View Menu

- Menu item **Toolbars**  
This item allows you to hide or to customise the tool bar.
- Menu item **Status Bar**  
This item allows you to hide the Status Bar (figure 1-10, page 17).
- Menu item **Mini Map**  
This item allows you to hide the Mini Map (figure 1-10, page 17).

Fig. 1-12 Dialogue for customising the tool bar



### 3.2.2.6 Window Menu

The functions of this menu are the same as known from MS Windows. The menu item **Windows ...** manages views of currently open windows.

### 3.2.2.7 ? Menu

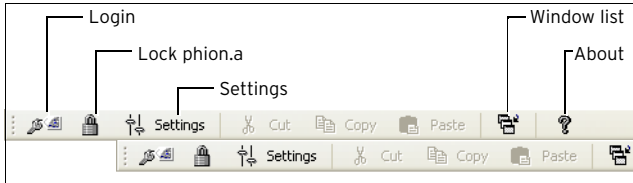
The **?** menu contains one item **About phion.a**. Select this item to display version and build number of phion.a, for example in case this information is of interest to the phion Support.

### 3.2.3 Tool Bar

**Note:**

The tool bar can be customised to personal needs. Please note that in this manual the default look of the tool bar is displayed (figure 1-13).

Fig. 1-13 Tool bar



All buttons that are available in the tool bar are also accessible via the menu bar:

- **Lock phion.a**  
see 3.2.2.2 File Menu, Menu entry **Lock**, page 19
- **Login**  
see 3.2.2.2 File Menu, Menu entry **Login ...**, page 19
- **Settings**  
see 3.2.2.2 File Menu, Menu entry **Settings ...**, page 19
- **Window list**  
see 3.2.2.6 Window Menu, page 19
- **About**  
see 3.2.2.7 ? Menu, page 19

### 3.2.4 Box Menu

The box menu of the phion.a user interface (figure 1-10, page 17) amongst others provides an icon for each "major" service. For example, such "major" services are the mail gateway service and the VPN Service.

**Note:**

The entries listed under 3.2.2.4 Box Menu, page 19 are also valid for the user interface box menu though the item order varies.

### 3.2.5 Main Window

The main window contains the configuration and information part of the phion.a. Depending on the selected item of the box menu this display changes. For detailed information have a look at the corresponding Chapter of the documentation.

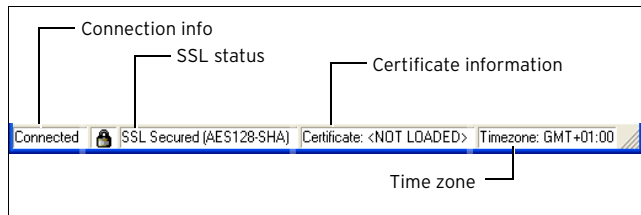
### 3.2.6 Mini Map

The mini map is an optional view and lists all opened boxes and, if available, all opened management centres. It allows quick navigation between the systems.

### 3.2.7 Status Bar

The status bar displays information about the SSL connection status (including used encryption algorithm, if available), the certificate and the time zone specified in the box time settings (translated to the corresponding GMT time zone as used in Microsoft Windows operating systems). A few linux specific time zones exist, which cannot be translated into GMT time zones. In this case, the system time of the client running phion.a will be displayed instead of box time settings.

Fig. 1-14 Status bar

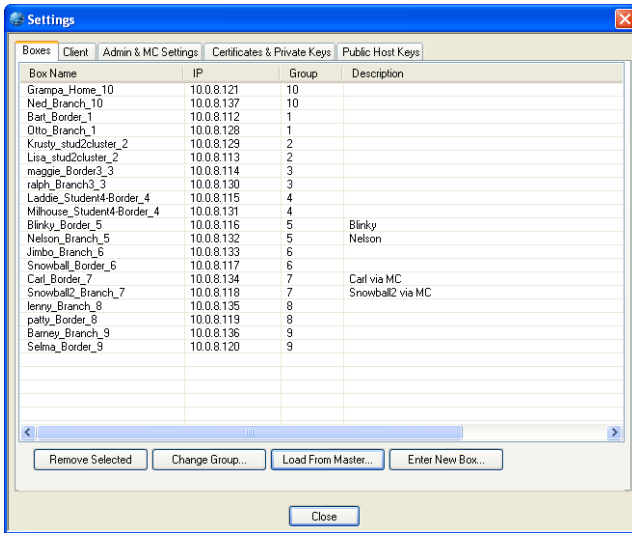


# 4. Settings

## 4.1 Boxes

This tab allows organising boxes for quick-access in the mini map.

Fig. 1-15 phion.a Settings - Boxes



The list contains the following columns:

- **Box Name**  
Name of the box
- **IP**  
IP address of the box
- **Group**  
Group the box is assigned to (see Button Enter New Box ..., page 21)
- **Description**  
Optional box description
- **Master** (if available)  
Name of the administering management centre
- **Master-IP** (if available)  
Displays the IP address of the management centre

- Button **Remove Selected**  
Select a list entry and click this button to remove the box from the list and its shortcut from the mini map.

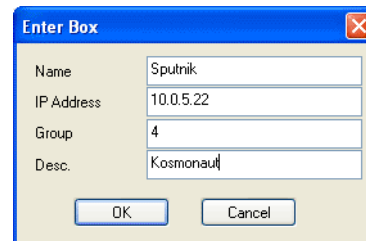
**Note:**

Pressing the keys SHIFT and/or CTRL during selection allows you to mark multiple entries at once.

The following buttons are available:

- Button **Change Group ...**  
This button allows you to change the group assignment of the selected entry/entries (see Button Enter New Box ..., page 21).
- Button **Load From Master ...**  
Use this button to load the boxes from a management centre (Master). Only MCs you have already connected to using phion.a are available for selection. The root password of the MC will be requested to load the settings.
- Button **Enter New Box ...**  
This button opens a dialogue for creating short-cuts manually.

Fig. 1-16 Enter New Box dialogue



Enter the name for the short-cut and the IP address of the box into the fields **Name** and **IP Address**. The field **Group** is used for defining categories to sort the short-cuts. According to these groups the mini map sorts the short-cuts into directories when the settings window is closed. This feature enables you to easily access and survey even big phion netfence installations.

**Note:**

If no group is entered, the short-cut will be sorted into the directory **Root** within the mini map.

**Note:**

As soon as you are logged into a box the short-cut of the box is also available in the group **Active**.

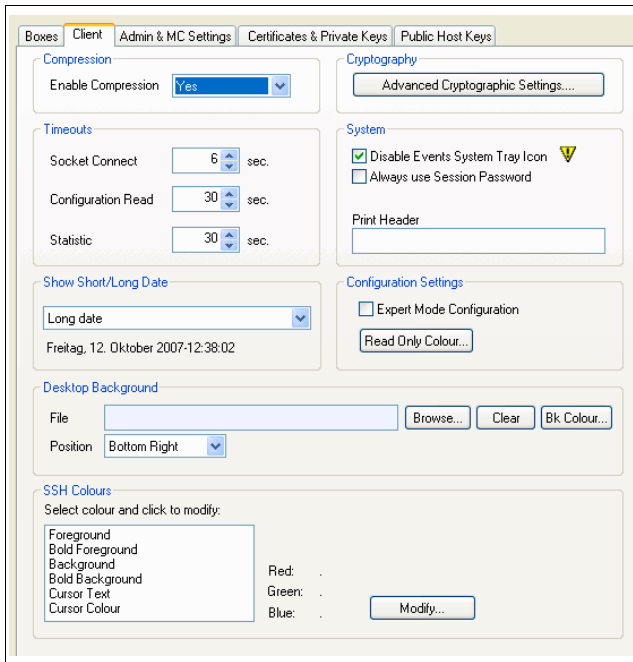
## 4.2 Client

Use this tab to configure your phion.a client.

### Note:

All parameters set here affect only the currently used phion.a. They are not saved on the phion netfence for example. You will have to repeat the configuration if you use another phion.a.

Fig. 1-17 phion.a Settings - Client tab



List 1-17 Configuring phion.a settings - Client tab - section Compression

Parameter	Description
<b>Enable Compression</b>	This parameter activates/deactivates data compression for phion.a connections (default: <b>No</b> - inactive) and increases efficiency as well as responsive management, especially over "thin" lines. <b>Note:</b> This feature is backwards-compatible, for example even older netfence releases not capable of handling compressed management connections properly may still be connected. When compression is active the connection status icon in the top right corner (🟢) changes to an icon with a cyan coloured background (🟢). <b>Attention:</b> To activate the changed compression, please reconnect to the system after having edited this parameter.

List 1-18 Configuring phion.a settings - Client tab - section Cryptography

Parameter	Description
<b>Advanced Cryptographic Settings ...</b>	Opens the <i>Advanced Crypto API Settings</i> configuration window (figure 1-18, page 23).

List 1-19 Configuring phion.a settings - Client tab - section Timeouts

Parameter	Description
<b>Socket Connect</b> [sec.]	Defines the duration a login attempt may last until in case of failure it is stopped and a failure message is displayed (default: <b>6</b> seconds). <b>Note:</b> The socket connect timeout also has impact on PAR file creation of comprehensive configurations. Temporarily set to 200 seconds or higher if necessary. See <b>Configuration Service</b> - 5.3 Creating PAR Files, page 119 for details.
<b>Configuration Read</b> [sec.]	Specifies the duration a connection attempt (through utilisation of the <b>Connect</b> button) may last until in case of failure the attempt is stopped and a failure message is displayed (default: <b>30</b> seconds). Furthermore this setting determines the read timeout of the configuration file effective in the Box Control > Licenses tab view (see 2.5 Licenses Tab, page 37). <b>Note:</b> The read timeout also has impact on PAR file creation of comprehensive configurations. Temporarily set to 200 seconds or higher if necessary. See <b>Configuration Service</b> - 5.3 Creating PAR Files, page 119 for details.
<b>Statistic</b> [sec.]	Defines how long (in seconds) a statistic-view attempt may last until the attempt is stopped and a message is displayed (default: <b>30</b> seconds). Increase this parameter if you expect large statistics files.

List 1-20 Configuring phion.a settings - Client tab - section System

Parameter	Description
<b>Disable Events System Tray</b>	Clear this checkbox to disable the icon in the system tray which indicates an active event.
<b>Always use session password</b>	This setting triggers phion.a always to use the last known password when reconnecting to a box after a session has been disconnected. The session password loses its validity when phion.a is closed.
<b>Print Header</b>	Allows entering a custom header for prints. Especially when multiple administrators use one printer this feature becomes handy because it allows identifying the owner very easily.

List 1-21 Configuring phion.a settings - Client tab - section Show Short/Long Date

Parameter	Description
<b>Show Short/Long Date</b>	This setting determines the date format display which is used in various overview listings (for example MC Control Centre)

List 1-22 Configuring phion.a settings - Client tab - section Configuration Settings

Parameter	Description
<b>Advanced Mode Configuration</b>	Clear this checkbox to enable the Advanced View for configuration entities by default.
<b>Read Only Colour...</b>	This button opens a window for defining the background colour for configuration files in read-only mode.

List 1-23 Configuring phion.a settings - Client tab - section Desktop Background

Parameter	Description
<b>Desktop Background</b>	This section allows defining a bmp file as "wallpaper" for phion.a start screen (for example your company logo).
<b>File</b>	Define a wallpaper (.bmp files only) for phion.a here.
<b>Browse ... Clear BK Colour...</b>	Select or clear a wallpaper here, or define a general background colour for the phion.a main window.
<b>Position</b>	Align the wallpaper here. Available options are: <b>Tile</b> , <b>Center</b> , <b>Stretch</b> , and <b>Bottom Right</b> .

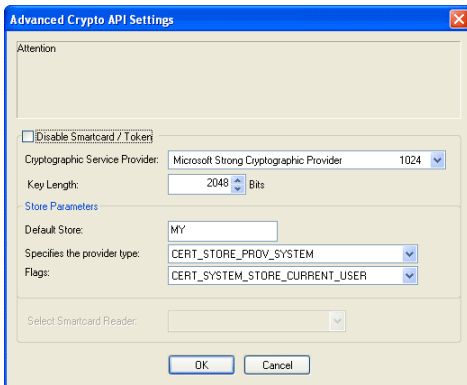
List 1-24 Configuring phion.a settings - Client tab - section SSH Colours

Parameter	Description
<b>SSH Colours</b>	Define the layout of the SSH Login interface here.
<b>Modify ...</b>	Chose one of the modifiable options ( <i>Background</i> , <i>Bold Background</i> , <i>Cursor Text</i> , <i>Cursor Colour</i> ) and change its colour with <b>Modify ...</b>



The following parameters are available for configuration in the **Advanced Cryptographic Settings** dialogue:

Fig. 1-18 Configuring Advanced Cryptographic Settings



List 1-25 Configuring Advanced Cryptographic API Settings

Parameter	Description
<b>Disable Smartcard / Token</b>	<b>Note:</b> Selecting the checkbox <i>Disable Smartcard / Token</i> deactivates the complete configuration section.
<b>Cryptographic Service Provider</b>	phion supports all CSPs (Cryptographic Service Provider) using the Microsoft Crypto API. All CSPs installed on your local workstation are enlisted.
<b>Key Length</b>	The key length depends on the selected CSP. Minimum, maximum and default value for key lengths are displayed in the <i>Cryptographic Service Provider</i> menu.

List 1-26 Configuring Advanced Cryptographic API Settings - section Store Parameters

Parameter	Description
<b>Default Store</b>	This parameter defines the default store for certificates (default: <i>MY</i> ).
<b>Specifies the provider type</b>	This parameter allows defining where the certificate is living. The following options are available: <b>CERT_STORE_PROV_SYSTEM</b> - Certificate available in MS Management Console <b>CERT_STORE_PROV_PHYSICAL</b> - Certificate available on eToken/Smartcard
<b>Flags</b>	This parameter defines the availability of the certificate. Possible values are 'current user only' or 'local workstation' regardless of the logged-in user. Use one of the values below for configuring: <b>CERT_SYSTEM_STORE_CURRENT_USER</b> - Certificate is dedicated to this user only <b>CERT_SYSTEM_STORE_LOCAL_MACHINE</b> - Certificate is dedicated to local workstation
<b>Select Smartcard Reader</b>	Allows selecting an available Smartcard Reader. If no Smartcard Reader is available on the system, this parameter is inactive.

### 4.3 Admin & MC Settings

#### ➤ Section *MC Selection*

This section allows you to view the certificates of management centre(s) you have logged into using this phion.a. To remove MCs from the view of phion.a click **Remove Entry**.

Otherwise chose an available MC in the field **MC** and click **Show Certificate** to display a detailed view of the certificate.

**Note:**  
After having removed an MC you will have to accept the certificate again when logging into it the next time.

#### ➤ Section *Change Administrator Password*

This section offers the opportunity to change passwords of management centre and single box local administrators.

To change a password of a management centre marked in the section **MC Selection**, select **Change Admin Credentials for MC Admin** from the pull-down menu, enter the administrator's login name, the current (old) password and the new password (twice, for security reasons). Click **Change Password** to activate the new settings.

To change the password of a single box local administrator, select **Change Admin Credentials for Local Admin (Single Box)** from the pull-down menu. A new field **Box IP Address** now appears to the right of the menu. Enter the box IP address and proceed as described above to change the password.

#### ➤ Section *Change Administrator Key*

If, for a successful login procedure, key files are needed in addition to the password, this administration key is to be edited/assigned in this section.

To change an administrator key, enter the correct login name and password and import the proper key via **Import. Change Admin Key** activates the new settings.

### 4.4 Certificates & Private Keys

➤ This tab contains the private key administration. Login and authentication of the administrator on a netfence gateway are processed using a 2-factor authentication technique. The authenticity of the admin workstation is verified with a challenge-response method. Beyond this the administrator has to authenticate himself with a personal password.

**Note:**  
Despite the fact that it is not mentioned in the tab header, it is also possible to use eToken and smartcards. However, they are used in the same way.

#### ➤ **Creating a new Certificate**

To generate a new certificate/key by using **Microsoft Strong Cryptographic Provider v1.0** click **Create New Certificate/Key ...** This opens a window where several values (for example Country, State, Name, Expiring date, ...) have to be entered. After confirming your entry the new certificate is displayed in the list.

The columns in the main tab derive from the information entered while creating the certificate. However, two columns differ:

- column **Hash** contains a short information concerning the key in order to make it easier to verify whether keys are equal or not.
- column **Key Container** displays the unique name of the CSP key container

New certificates are usually not generated with phion.a. They will normally be available on the domain controller and will from there be transferred to the specified default store.

#### ➤ Deleting a Certificate

This is done by selecting the required certificate and clicking **Delete Certificate/Key**.

#### ➤ Viewing and Exporting a Certificate

Certificates cannot be viewed and exported with phion.a. You can use Microsoft Management Console (MMC) for this purpose instead. Please refer to the manuals provided by the manufacturer for further information.

### 4.4.1 Using Keys on a netfence 4.2

Keys in PEM format cannot be used on netfence systems anymore since netfence 2.4.2. phion.a 4.2 enables conversion of already existing keys into certificates, though.

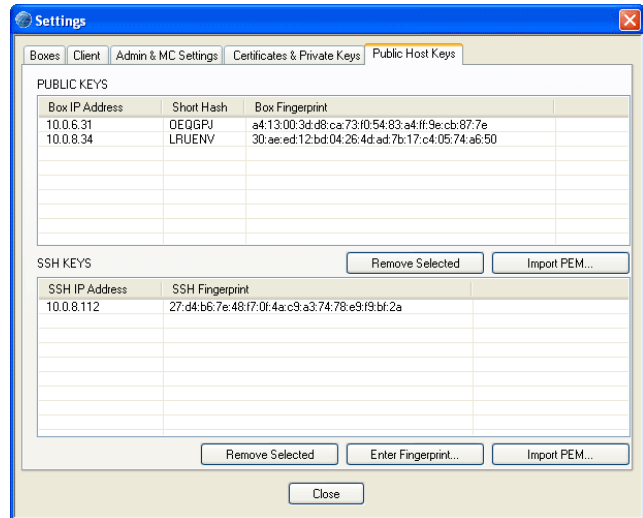
If you have netfence 2.4.1 keys in your registry, phion.a for netfence 4.2 provides an additional button in this dialogue called **Migrate Keys to Cert ...** Click this button to open a password request for the available keys.

After entering the proper password, the keys are converted into certificates. The subsequent dialogue (**Registry Keys converted to Microsoft Certificate Management - Remove Registry Keys?**) offers two options:

- **Yes** - Removes the keys in PEM format from the registry; Recommended when only administering netfence 3.2/3.4/3.6/4.0.
- **No** - Keeps the keys in PEM format in the registry; Recommended when administering both, netfence 2.4.1 and netfence 3.2/3.4/3.6/4.0 from the same workstation.

## 4.5 Public Host Keys

Fig. 1-19 phion.a Settings - Public Host Keys tab



#### ➤ Section **Public Keys**

This section shows all netfence gateways which were accessed with this computer. The list includes the **Box IP Address**, a **Short Hash** of the key and the unique **Box Fingerprint**.

The button **Remove Selected** is used for deleting a selected entry from the list. A security request will pop up the next time you log in to the box.

The button **Import PEM ...** allows you to import PEM-files. Security is increased by using certificates in this place, at the same time a security request is avoided.

#### ➤ Section **SSH Keys**

This section shows all netfence gateways which were accessed via a SSH connection from this computer. The list includes the **SSH IP Address** and the unique **SSH Fingerprint**.

In addition to the buttons Remove Selected and Import PEM ..., both having the same purpose as described above, the button **Enter Fingerprint ...** is available. Click this button to enter the unique fingerprint and the corresponding IP address manually into a dialogue box.

## 5. phion Notation

The notation, which is used within the phion netfence to define network masks, is different from the CIDR notation. As a rough guide keep in mind that the higher the phion notation the bigger the network (in contrary to CIDR notation). The phion notation can be calculated very easily: "phion" = 32 - "CIDR".

### 5.1 Comparison CIDR - phion Notation

Table 1-5 Comparison CIDR - phion notation


Quad	CIDR	phion
255.255.255.255	32	0
255.255.255.254	31	1
255.255.255.252	30	2
255.255.255.248	29	3
255.255.255.240	28	4
255.255.255.224	27	5
255.255.255.192	26	6
255.255.255.128	25	7
255.255.255.0	24	8
255.255.254.0	23	9
255.255.252.0	22	10
255.255.248.0	21	11
255.255.240.0	20	12
255.255.224.0	19	13
255.255.192.0	18	14
255.255.128.0	17	15
255.255.0.0	16	16
255.254.0.0	15	17
255.252.0.0	14	18
255.248.0.0	13	19
255.240.0.0	12	20
255.224.0.0	11	21
255.192.0.0	10	22
255.128.0.0	9	23
255.0.0.0	8	24
254.0.0.0	7	25
252.0.0.0	6	26
248.0.0.0	5	27
240.0.0.0	4	28
224.0.0.0	3	29
192.0.0.0	2	30
128.0.0.0	1	31
0.0.0.0	0	32




# Control Centre

<b>1.</b>	<b>Overview</b>	
1.1	Control Window .....	28
<b>2.</b>	<b>Control Tabs</b>	
2.1	Server Tab .....	29
2.1.1	Section Server Status .....	29
2.1.2	Section Service Status .....	29
2.2	Network Tab .....	30
2.2.1	Interface/IPs Tab .....	30
2.2.2	IPs Tab .....	31
2.2.3	Interfaces Tab .....	31
2.2.4	Proxy ARPs Tab .....	32
2.2.5	ARPs Tab .....	32
2.2.6	Statistics Tab .....	32
2.2.7	OSPF Tab .....	32
2.2.8	Tables .....	32
2.3	Processes Tab .....	36
2.4	Resources Tab .....	36
2.5	Licenses Tab .....	37
2.5.1	Section Version Status .....	37
2.5.2	Section Active Licenses .....	37
2.5.3	Section License Values .....	37
2.5.4	Section Host IDs .....	37
2.6	Box Tab .....	38
2.6.1	Section Network Configuration .....	38
2.6.2	Section Operating System .....	39
2.6.3	Section Time Control .....	39
2.6.4	Section Dynamic Network Connections .....	39
2.6.5	Section Authentication Level .....	39
2.6.6	Section BOX SCEP Status .....	40
2.7	Sessions Tab .....	40
2.8	Mainboard Tab .....	40

# 1. Overview

The  **Control** window is an essential monitoring and administration tool that provides real-time information about the status of a system and makes a variety of fundamental administration tasks available. Important information it displays is related to the following:

- Server/Service and Network status
- Status of disk usage
- Status of currently active processes and sessions
- Hardware information
- License information  
(keys and status of installed licenses)
- Release information  
(version numbers and build-dates of installed phion software modules)

To access the Control window, click  **Control** in the box menu.

## Note:

The Control window may as well be accessed from the **Status Map** tab in the management centre **Control Centre (phion management centre - 5.2 Status Map Tab, page 397)**.




## 1.1 Control Window

The contents of the Control window are arranged in eight tabs:

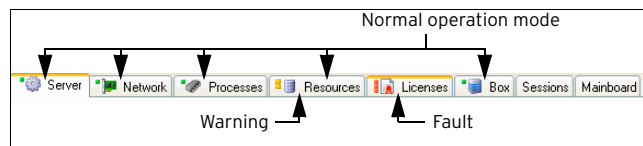
- Server tab - see 2.1 Server Tab, page 29
- Network tab - see 2.2 Network Tab, page 30
- Processes tab - see 2.3 Processes Tab, page 36
- Disks tab - see 2.4 Resources Tab, page 36
- Licenses tab - see 2.5 Licenses Tab, page 37
- Box tab - see 2.6 Box Tab, page 38
- Sessions tab - see 2.7 Sessions Tab, page 40
- Mainboard tab - see 2.8 Mainboard Tab, page 40

All tabs but the latter two are flagged by a status indicator icon, which indicates the current status of the respective box subsystem.

**Table 2-1** Status icons flagging tabs in the Control window





Icon	Meaning	Comment
	OK	Normal operation
	Warning / Activation	Abnormal condition not affecting normal operation and activation box - network
	Critical condition	Seriously abnormal condition

**Fig. 2-1** Tabs in the Control window flagged by status icons



In addition, the connection status is indicated by the icons listed below. To connect to or to disconnect from the system, click the **Connect** or **Disconnect** button respectively.

**Table 2-2** Connection status icons

Icon	Meaning	Comment
	Connected	
	Compressed connected	
	Not connected	
	Disconnected	Established connection terminated abnormally



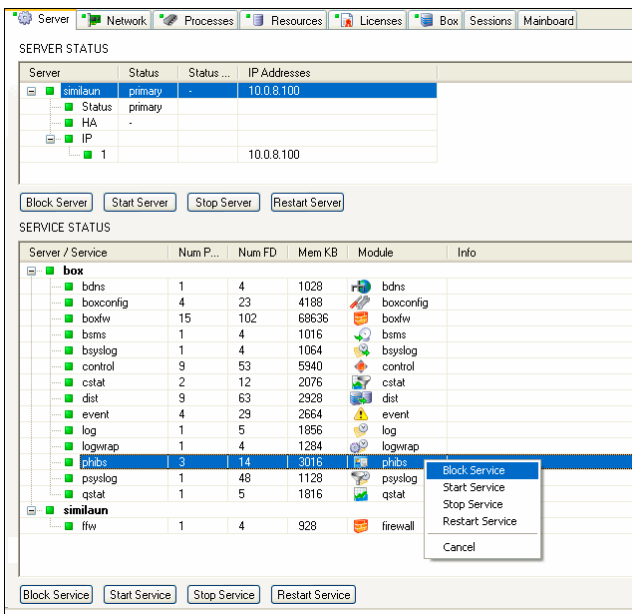
## 2. Control Tabs

### 2.1 Server Tab

The Server Tab displays status information about the phion server/service subsystem and allows influencing server and service operation. The view of the Server tab is divided into two sections, the upper **SERVER STATUS** section displaying information about the status of available servers, and the lower **SERVICE STATUS** section displaying information about the status of available services.

At the bottom of each section, buttons are arranged that allow changing the operational status of a server or service. In addition, the operational status may be changed by selecting a server or service, then right-clicking to open the context menu, and then clicking the appropriate menu item in the list.

Fig. 2-2 Server Tab



#### 2.1.1 Section Server Status

The listing in the Server Status section displays status and configuration information of servers available on the box.

➤ **Server** column

In this column, servers and sub-elements defining their state are arranged in a hierarchical structure.

The root entry indicates the server name. Below that **Status**, **HA** (optional) and **IP** are arranged as sub-elements, whereby the **IP** tree item again contains sub-elements for each defined server IP (**Configuration Service** - 3. Configuring a New Server, page 94).

Icons indicate the current status of each server:

- Server is up
- ⚠ Server is blocked
- Server is stopped
- ✖ Server is disabled

➤ **Status** column

This column displays the states of server and HA partner box. Column entries have the following significance:

Table 2-3 Server status and configuration

Entry	Comment
Primary	Server is up and running, either as a single system or as the primary part of a high availability setup.
Secondary	Server is up and running on the backup machine of a high availability setup.
Standby	Server is in standby state and is waiting to take over if the high availability partner goes down.
Down	Server is not running but able to start automatically when triggered.
Block	Server is blocked and unable to start automatically even if the high availability partner goes down. <b>Note:</b> A blocked server always has to be started manually.
Disabled	Server is disabled due to environmental conditions for example because monitoring IP or monitoring interface is not available.
-	The en dash (-) indicates a server running stand-alone without configured HA (High Availability) partner.

➤ **Status HA Partner** column

This column displays the status of the HA partner. Column entries have the same significance as in the **Status** column.

➤ **IP Addresses** column

This column lists the IP address(es) a server is listening on.

At the bottom of the Server Status section, buttons are arranged that allow changing the operational status of a server:

➤ **Block Server**

➤ **Start Server**

➤ **Stop Server**

➤ **Restart Server**

To perform a status change, select a server, then click the appropriate button. Else, select a server, then right-click to open the context menu, then click the appropriate menu item in the list.

#### 2.1.2 Section Service Status

The listing in the Service Status section displays status and configuration information of services available on the box.

➤ **Server / Service** column

In this column, servers and their services as sub-elements are arranged in a hierarchical structure.

The main level indicates the server name. Below that available services are arranged as sub-elements. The listing begins with the main level **box**. Sub-elements of this entry are all global services, such as boxfw, control, event, log,... Other main levels begin with the corresponding server name. Sub-elements of these

entries are specific services available on the corresponding server.

Icons indicate the current status of each server and service:

- Service is up
- ⚠ Service is blocked
- Service is stopped
- ✖ Service is blocked, stopped or disabled (inherited property because the server has been blocked, stopped or disabled)

**Note:**

When evaluating a service status, make sure to evaluate the current server status.

- **Num Proc** column  
This column displays the number of processes for each service.
- **Num FD** column  
This column displays the number of file descriptors used by the service processes.
- **Mem KB** column  
This column displays the total memory (exclusive and shared) used by the service processes.
- **Module** column  
This column displays name and corresponding icon of the installed software module. This information is important regarding services running on user defined servers, as these may be named without indication to the service type.

At the bottom of the Service Status section, buttons are arranged that allow changing the operational status of a service:

- **Block Service**
- **Start Service**
- **Stop Service**
- **Restart Service**

Select a service, then click the appropriate button to perform a status change. Else, select a service, then right-click to open the context menu, then click the appropriate menu item in the list.

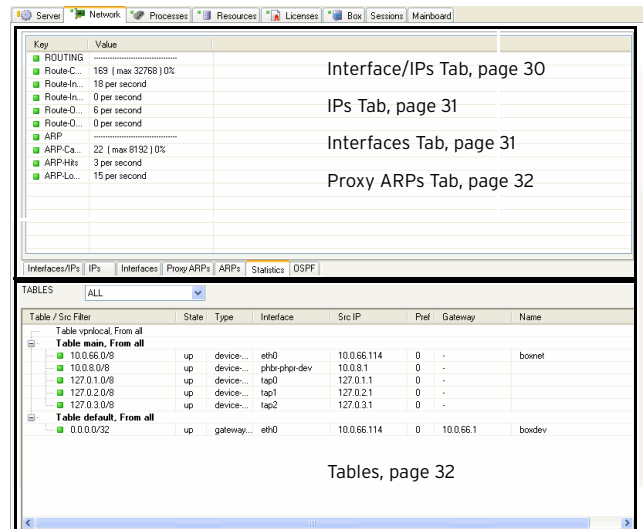
**Attention:**

In order to block/start/stop/restart the firewall service the service `box > boxfw` has to be restarted. Blocking/starting/stopping/restarting the service `<servername> > fw` will have no effect.

## 2.2 Network Tab

The Network Tab gives a detailed account of the current status of the network subsystem of the box.

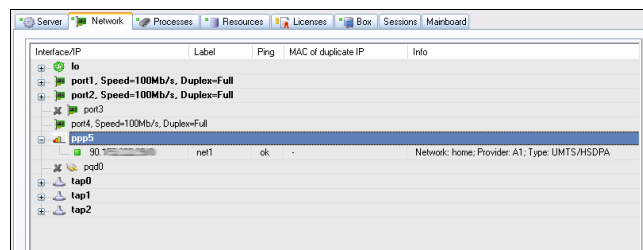
Fig. 2-3 Network Tab



### 2.2.1 Interface/IPs Tab

This tab contains all interfaces, their current state (visualised with an icon, see below) and the IP addresses that are assigned to the interface.







Fig. 2-4 Interface/IPs Tab



#### ➤ Interface/IP column

In this column, network interfaces and their assigned IP addresses as sub-elements are arranged in a hierarchical structure. The **main level** indicates the network interface name with corresponding icon and, regarding Ethernet network adapters, additional information on speed and duplex setting. Below the main level IP addresses living on the network interface are arranged in **sublevels** issued with corresponding netmasks (phion Notation). Each sublevel is issued with a status icon. The following icons indicating the network interface type are available:

Table 2-4 Icons for network interface types

Icon	Description
	Ethernet network adapter
	Token ring network adapter
	Loopback interface
	phion queuing interface (used for traffic shaping)
	DHCP interface; used for xDSL/DHCP connections
	gre0; used for IP-to-IP tunnelling

**Table 2-4** Icons for network interface types

Icon	Description
	tap interface (internal interface for SYN proxying & VPN)
	Tunnel interface

The following icons indicating the network connection status are available:

**Table 2-5** Icons for network connection status

Icon	Description
	up
	signal strength, varying from red (low) to green (high)
	down or duplicate

**Note:**

Any IP address changing to state "down" will trigger change of the network subsystem to a critical condition. Critical conditions are flagged with the icon in the tab label.

**Note:**

A single network connection status change will not lead to a network tab indicator status change.

**Note:**

Not all UMTS cards support the signal strength feature. To use this feature you need an UMTS card with 2 channels and you have to set the parameter **Activate 2nd Channel** to **yes** (**Network > UMTS > UMTS Connection Details**). For parameter description see **Configuration Service - 2.2.5.7 UMTS**, page 76.

Please consult the Hardware Compatibility List (HCL) available in Myphion area on [www.phion.com](http://www.phion.com) for details.

- **Label** column  
A label is available for every interface that is in state "up" ( icon). Multiple predefined labels exist, such as **mip0** (for the primary administrative network of the box), **loop** (for the loopback interface 127.0.0.1/8), **fw** (for network 127.0.1.1/8 on interface tap0), **vpn** (for network 127.0.2.1/8 on interface tap1), and **vpnpers** (for network 127.0.3.1/8 on interface tap3). IP addresses associated with server processes are labelled according to the name of the server. Additionally configured networks are named according to the label name in the network in the configuration file/dialogue.
- **Ping** column  
This column indicates whether the corresponding IP address is configured to reply to pings (entry **ok**) or not (entry **NO**) (**Configuration Service - 3. Configuring a New Server**, page 94).
- **MAC of duplicate IP** column  
As soon as an IP address is used twice, the MAC address of the other interface is shown.

## 2.2.2 IPs Tab

This tab contains the same information as given in the Interface/IPs Tab, but the content is sorted according to IP addresses instead of interfaces.

The **State** column shows the state of the IP address/netmask as does the icon in the **IP** column.

The **Interface** column is formatted as follows: Name of the interface used (for example, eth0, tr0, tap0, ...) followed by a colon and the label of the interface. For a description of the label syntax, please have a look at 2.2.1 Interface/IPs Tab, Label column, page 31.

## 2.2.3 Interfaces Tab

This tab allows a quick view at all necessary interface settings at a glance.

- **Interface** column  
This column displays similar parameters as the **Interface/IP** column described above. Speed and duplex settings are arranged in a separate column though (see below).
- **MAC** column  
The unique MAC address for each interface is displayed here.
- **Link** column  
The data here lets you verify if an interface is physically connected or not.
- **Speed** column  
Here the maximum transfer rate for an adapter is displayed in Mbit/s.
- **Duplex** column  
This columns displays the duplex settings of the NIC (**Half** or **Full**).
- **Neg.** column  
Shows whether auto negotiation is **on** or **off**.
- **MTU** column  
This columns displays the set MTU size (Maximum Transmission Unit) of the NIC. This parameter is described in 2.2.5.1 Networks, page 61.
- **Bytes** column  
Shows the byte throughput and is calculated by the average number of bytes/s (obtained from a 10 second sampling interval) passing through the interface.
- **Packets** column  
Shows the packet throughput and is calculated by the average number of packets/s (obtained from a 10 second sampling interval) passing through the interface.
- **Errors** column  
This column contains the total number of errors and is calculated by the average number of all errors on the interface (obtained from a 10 second sampling interval).
- **Realm** column  
For each interface, the appropriate **Interface Realm** can be configured (**Configuration Service - Interface Realm**, page 69). This realm is shown in this column.
- **Flags** column  
The following entries are possible:
  - **UP**- interface is up
  - **BROADCAST**- broadcast active

- **LOOPBACK** - loopback active
- **NOARP** - ARP requests will not be responded
- **POINT-TO-POINT** - used for PPTP
- **PROMISC** - accepts every packet regardless whether the MAC address matches

#### ➤ **Features** column

The following entries are possible:

- **SGI/O** - Scatter gather Input/Output (DMA)
- **NOCSUM** - no checksum required
- **HWCSUM** - interface is capable of hardware checksum
- **IPCSUM** - interface is capable of checksum for IP packets
- **HW-VLAN-TX** - interface is capable of VLAN tagging transmits
- **HW-VLAN-RX** - interface is capable of VLAN tagging receives
- **HIGH-DMA** - I/O memory above 64 K
- **DYNALLOC** - used for virtual interfaces

#### ➤ **IRQ** column

This columns contains the IRQ number (Interrupt ReQuest line) for each interface.

#### ➤ **Base-Addr** column

I/O port address

## 2.2.4 Proxy ARPs Tab

Proxy ARPs are additional IP addresses/netmasks the firewall responds to.

- **IP/Mask** column  
This columns shows all configured/created IP addresses/netmasks.
- **Interface** column  
Displays the interface where the IP address/netmask resides.
- **Origin** column  
Contains the origin of the Proxy ARP (by whom it is created).
- **Exclude** column  
Displays networks that are excluded from proxy APR creation.
- **Source Restriction** column  
Displays network addressed to which the proxy ARP request has been limited.

## 2.2.5 ARPs Tab

The Address Resolution Protocol is needed for translating an IP address into a physical address.

- **IP** column  
Shows the used IP addresses
- **MAC** column  
Displays the MAC address of each assigned IP address
- **Vendor** column  
Shows the NIC manufacturer

## 2.2.6 Statistics Tab

Shows informations about the routing and ARP cache of the box.

#### **Note:**

Loading these informations takes some seconds. In the meantime **Data Pending ...** and **please wait** are shown in the list.

## 2.2.7 OSPF Tab

Shows information about the OSPF states **Neighbour** and **Interfaces** of the box if applicable (if a OSPF/RIP service is running on the box).

## 2.2.8 Tables

This section of the **Network** tab shows the defined routing tables. Without policy routing there are two of them, the main table and the default table, where the default route lives.

Fig. 2-5 Table section

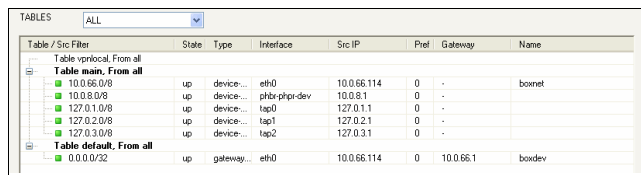


Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table vrrpical, From all							
Table main, From all	up	device...	eth0	10.0.66.114	0	-	bonnet
10.0.66.0/8	up	device...	pbr-pbr-dev	10.0.8.1	0	-	
10.0.8.0/8	up	device...	tap0	127.0.1.1	0	-	
127.0.1.0/8	up	device...	tap1	127.0.2.1	0	-	
127.0.2.0/8	up	device...	tap2	127.0.3.1	0	-	
127.0.3.0/8	up	gateway...	eth0	10.0.66.114	0	10.0.66.1	boxdev
Table default, From all							
0.0.0.0/32	up	gateway...	eth0	10.0.66.114	0	10.0.66.1	boxdev

The pull-down menu on the top of this section allows you to filter for predefined table types (for example, **ALL** shows all routing tables, whereas **main** hides all other tables except for the main table).

Without policy routing activated, all routes except the default routes will go into table **main**. Default routes will go into table **default**. With policy routing activated additional tables become available as specified in the configuration dialogue.

The context menu contains the option **Delete Wild Route** that can be used to delete routes marked as wild. Wild routes are routes for which there is no corresponding entry in the network configuration file. Usually wild routes appear as a consequence of manual introduction of additional routes through the command line interface or when direct or gateway routes have been deleted using the option **Soft** network activation (see 2.6 Box Tab, **Soft**, page 38).

#### ➤ **Table / Src Filter** column

This column is structured according to the routing tables to provide all required information about the routed netmasks at a glance.

The sublevel of the structure contains the netmasks concerned and their current status (depicted using the icon described above).

#### ➤ **State** column

Displays the state of the routing. Available entries are **up, down, wild, disabled, off**.

For detailed information see 2.2.8.1 Handling of Routes by the Control Daemon, page 33.

➤ **Type** column

The following types of routes are available:

- **direct** routes point to directly connected networks. No next hop is involved. The network is directly accessible via the specified interface.
- **gateway** routes are routes to networks which are only accessible via a next hop. The next hop must be reachable through a direct route.

➤ **Interface** column

Shows the interface through which traffic to the destination network passes.

**Note:**

For direct routes the interface must be specified within the network configuration. For gateway routes it is automatically determined from the available direct routes.

➤ **Src IP** column

Contains the route source IP address.

**Note:**

The control daemon will pick the most appropriate source address automatically from the pool of available IPs unless a source address has been explicitly specified in the network configuration.

➤ **Pref** column

The preference of the route, with 0 indicating the highest preference.

➤ **Gateway** column

Shows the address of the next hop for gateway routes. For direct routes this field is left empty (denoted by a single -).

➤ **Name** column

This column shows the given name of the route.

**2.2.8.1 Handling of Routes by the Control Daemon**

controld reads out the currently active network configuration from file `/opt/phion/config/active/boxnet.conf`. One of the tasks of the controld daemon is to verify that the routes configured therein are actually valid. The basis logic goes as follows:

controld does not introduce IPs with a mask other than 0 (single IPs). By this means controld looks after server IPs and proxyARPs but not after networks local to the box.

This does however not mean that controld will not mark networks as down. It will merely refuse to reintroduce deleted box IP addresses.

As far as routing is concerned controld will play a more lively role and will activate and deactivate routes depending on available configuration information and environmental conditions.

One of the features of phion boxes is that you may configure what we call pending direct routes. These routes are special insofar as they point to a target network via an available interface to which no IP address has yet been assigned. As such the route cannot be introduced directly as no source IP address is available.

The behaviour of controld is now governed by the configuration parameter **Foreign IP Sufficient**. Initially controld will display the route as in state off (icon ). If the mentioned parameter is set to **y** (yes - default) then any IP activated on the associated interface will bring up the route. Typically this IP is a server IP. You would use this feature if you wish to make a route available only when a certain server functionality is available. If this parameter is set to **no** then only an IP address belonging to the target network will trigger activation of the route.

In order to illustrate this in more detail consider the following example. Assume box 10.0.8.112 is configured to have a leg in three networks:

**Table 2-6** Example: Route handling, networks

Network	Local IP address	on Interface
10.0.0.0/8	10.0.0.18	eth0
10.14.55.64/5	10.14.55.66	eth1
10.11.22.0/8	10.11.22.33	tr0

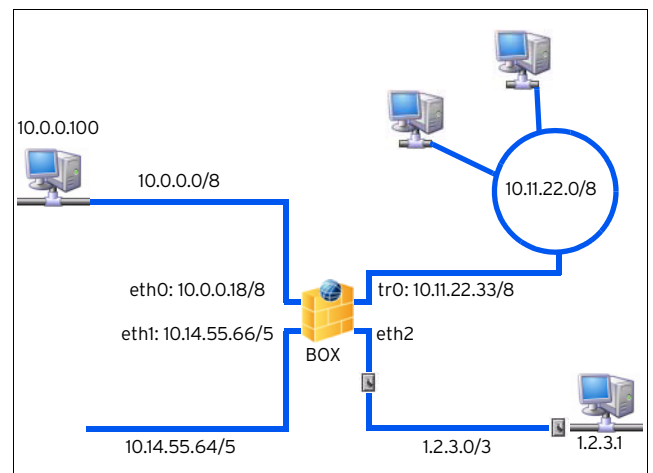
Bringing up each of these networks will automatically trigger the introduction of a corresponding direct route:

**Table 2-7** Example: Route handling, corresponding direct route

Target network	Source IP address	Table	on Interface
10.0.0.0/8	10.0.0.18	main	eth0
10.14.55.64/5	10.14.55.66	main	eth1
10.11.22.0/8	10.11.22.33	main	tr0

Box 10.0.0.18 is additionally connected to a further network 1.2.3.0/3 accessible through interface eth2 but the box itself does not have a leg in this network as depicted in figure 2-6.

**Fig. 2-6** Network diagram illustrating the concept of a pending route



Now suppose you have already configured a corresponding direct route under section **Section Main Routing Table (Configuration Service - 2.2.5.5 Network Routes, page 68)** of the network configuration dialogue.

**Table 2-8** Example: Route handling, no Source IP address

Target network	Source IP address	Table	on Interface
1.2.3.0/3	-	main	eth2

Quite evidently this route cannot be introduced right away as no valid source IP address is available. However, since it has been configured it will be displayed as in state off (icon ) by the control daemon.



We now assume that the following gateway routes have also been introduced:

**Table 2-9** Example: Route handling, gateway routes

Target network	Gateway	Table	Preference
0.0.0.0/32	1.2.3.1	default	100
0.0.0.0/32	10.0.0.100	default	200

**Note:**

A route is automatically assigned to table default if and only if the target is equal to 0.0.0.0/32.

Clearly the preferred default route via gateway 1.2.3.1 cannot be activated as no active route to address 1.2.3.1 is available. The control daemon will thus display this route as in state off (icon ✖). We refer to such gateway routes as pending gateway routes, as their introduction only takes place pending a prior successful introduction of a not yet available but configured direct route.

If gateway 10.0.0.100 is pingable and the address is not local to the box itself then this route will be active, which means in state up (icon ▲), as the presently preferred default route. If gateway 10.0.0.100 is not pingable then the route will be marked as in state dis (disabled). Since no alternative route is available to the same target network icon (■) is used to indicate that the networking subsystem is in a critical condition.

**Note:**

If the gateway address is pingable but local to the box the route will be considered as in state off (icon ✖). We will come back to a discussion of why and when such a scenario will arise when we discuss special aspects of interoperation with a router further below. Note that routes marked as off are not part of the routing tables of the box and thus only known to the control daemon.

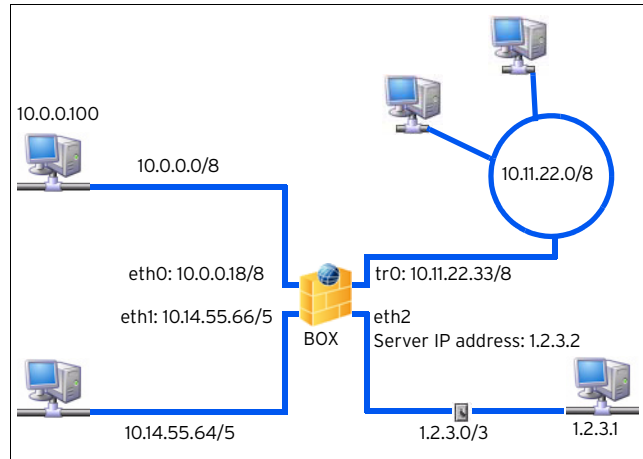
Now assume that a stand alone server IP 1.2.3.2/0 is activated on the box (figure 2-7). Due to the available routing information this IP must reside on interface eth2. As a consequence a valid source IP has become available for our inactive pending direct route allowing the control daemon to introduce it as a valid route into table main.

**Table 2-10** Example: Route handling, valid source IP address

Target network	Source IP address	Table	on Interface
1.2.3.0/8	1.2.3.2	main	eth2

The Network diagram in figure 2-7 illustrates the way in which pending direct routes and gateway routes depending on them are activated by firing up an IP address on the so far not configured interface eth2:

**Fig. 2-7** Network diagram, pending direct routes and gateway routes



The route will immediately have its status changed from off ✖ to up ▲. All pending gateway routes requiring this direct route will also be introduced into the routing tables. If gateway 1.2.3.1 is pingable and the address is not local to the box (as in the example) then this route will be displayed as in state up ▲, as the presently preferred default route (due to its lower preference number). If gateway 10.0.0.100 is not pingable then the route will be marked as in state **dis** (disabled). Since an alternative route is available to the same target network the icon is used to indicate that the networking subsystem is in an unsound yet uncritical condition.

If gateway 10.0.0.100 is pingable or arpable then this route will be marked as in state up ▲ as well.

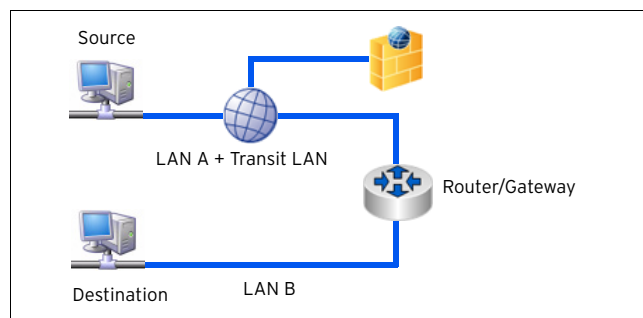
**Note:**

Whenever a gateway is not pingable and not arpable control will change its preference (metric) to a new value by adding 65536 to the assigned preference number.

## 2.2.8.2 Interoperation with a Router

An interesting routing issue arises when the firewall box is meant to work together with a router in what is called a screened host setup commonly used to separate LAN segments from one another.

**Fig. 2-8** Example for a screened host setup



With help of a small transit LAN scenarios may be visualised in which a logical separation of LAN A and LAN B may even be achieved with a single NIC at the firewall. In order for this to work the firewall and a router or gateway exclusively share a small transit network (usually 2 to 3 bits).

The advantages of such a single homed setup are evident. If you have to deal with various kinds of network traffic within a large WAN or LAN at the same time, for example SNA, IPX, and IP, you have to let SNA and IPX traffic bypass the firewall. At the same time you would like to use the firewall to manage and monitor your IP traffic. This is not possible if the firewall is dual homed in the traditional sense since then everything has to run through the firewall. Thus it is better to resort to a dual homed setup in address space. The single firewall NIC is configured to have network addresses that make it part of LAN A and additional network addresses from a small transit network it shares exclusively with the router/gateway component. The router/gateway does not have a valid IP address within LAN A.

For all IP traffic the router will use one of the transit network IPs of the firewall box as its next hop for traffic from LAN B to LAN A. Within LAN A routing is configured in such a way that one of the firewall's addresses in LAN A is the default gateway for traffic into LAN B. The firewall passes on this traffic via the transit network to the router/gateway, which then knows where to send it further.

At the same time all non IP traffic passes unharmed from LAN A to LAN B via the router/gateway since a direct physical link is established and all IP routing information is ignored.

Below is an example configuration for the successful interplay of router and firewall (redundant scenario included) to realise a single homed setup:

**Table 2-11** Example configuration for router and firewall

Object	Address
LAN A	10.x.y.0/8
LAN A default gateway	10.x.y.100
Transit LAN	10.255.128.0/3 (shared by firewall and router)
FW-box-IP	10.x.y.108
FW2-box-IP	10.x.y.109 (optional in case of a redundant setup)
FW-default GW	10.255.128.1 (router's transit LAN address) when active 10.x.y.100 when inactive
FW-Transit Netw.-IP	10.255.128.2
FW2-Transit Netw.-IP	10.255.128.3 (optional in case of a redundant setup)
Firewall service IP	10.x.y.100 and 10.255.128.4

The two different router configurations needed for an active and inactive firewall, respectively:

**Table 2-12** Router configuration

Firewall	Interface address	Additional routing table entries
active	transit LAN: 10.255.128.1	static routes: 10.x.y.0/8 via 10.255.128.4 + OSPF propagation 10.x.y.108 via 10.255.128.2 10.x.y.109 via 10.255.128.3

**Table 2-12** Router configuration

Firewall	Interface address	Additional routing table entries
not active	no transit LAN 10.x.y.100	

As far as the routing setup for the firewall is concerned the firewall boxes must clearly have two default routes with different preferences configured. The preferred one will be the one corresponding to active firewall operation.

The following scenarios may occur:

- the router operates in its firewall configuration

**Table 2-13** Routing state on active firewall box

Target network	Gateway	Table	Preference	Status
0.0.0.0/32	10.255.128.1	default	100	up
0.0.0.0/32	10.x.y.100	default	200	up

**Note:**

The backup default route is not up but off since 10.x.y.100 is pingable but also local to the currently active firewall.

**Table 2-14** Routing state on backup firewall box

Target network	Gateway	Table	Preference	Status
0.0.0.0/32	10.255.128.1	default	100	up
0.0.0.0/32	10.x.y.100	default	200	up

**Note:**

Both default routes are **up** since 10.x.y.100 is pingable on the active firewall box.

- router operates in its non firewall configuration

**Table 2-15** Routing state on both firewall boxes

Target network	Gateway	Table	Preference	Status
0.0.0.0/32	10.255.128.1	default	100	dis
0.0.0.0/32	10.x.y.100	default	200	up

Note that the preferred default route is not **up** but **disabled** since 10.255.128.1 is no longer pingable. In order to make sure that the box still has a valid default route the firewall IP 10.x.y.100 will be deactivated on the active firewall box.

**Note:**

This behaviour is only triggered by specifying the router's transit LAN IP 128.255.128.1 to be pingable as a necessary prerequisite for firewall operation.

- router failure  
If the router is down completely both default routes would be in state **disabled**.

**Table 2-16** Routing state on both firewall box

Target network	Gateway	Table	Preference	Status
0.0.0.0/32	10.255.128.1	default	100	dis
0.0.0.0/32	10.x.y.100	default	200	dis



## 2.3 Processes Tab

The character of the processes view is purely informational. A single panel lists status information about all currently active processes on the box. An additional single status line displays the current time, machine uptime, number of logged in users, load average and memory usage. Three average load values are listed: first value - average load within the last minute; second value - average load within the last five minutes; third value - average load within the last fifteen minutes. Memory usage is additionally illustrated graphically by a status bar. As for disk usage the bar is divided into three sections. Throughout the first section 0 < memory < 70 % the bar is green, for 70 % ≤ memory < 90 % the bar is yellow, and for memory ≥ 90 % the bar is red. The memory status affects the overall status of the processes view.

Fig. 2-9 Sample process status view

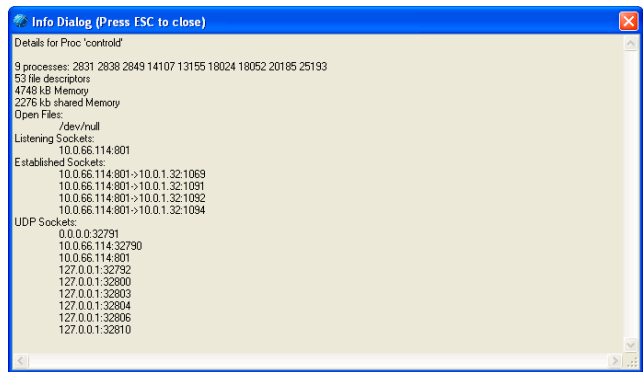
Name	Proc	%CPU	NumFD	Memory	Shared	Listen	Establ.	UDP	Syn Sent	Close
TOTAL	81	1	486	21184	95360	18	9	29	0	0
sshd	1	0	0	0	0	0	0	0	0	0
sshd	1	0	4	289	740	0	0	0	0	0
boxconfigd	4	0	23	1469	2730	1	1	1	0	0
ssm	1	0	4	276	740	0	0	0	0	0
sshd	1	0	4	316	740	0	0	0	0	0
sshd	1	0	6	128	932	1	1	0	0	0
control	9	1	53	4749	2294	1	4	9	0	0
control	1	0	8	76	924	0	0	0	0	0
ctd	2	0	9	240	1728	0	0	1	0	0
sshd	1	0	11	112	812	0	0	0	0	0
sshd	1	0	5	340	1476	1	1	0	0	0
sshd	9	0	63	536	2292	1	0	0	0	0
sshd	2	0	23	630	2274	1	0	2	0	0
sshd	1	0	13	242	1512	4	0	2	0	0
sshd	1	0	1	60	420	0	0	0	0	0
sshd	1	0	0	0	0	0	0	0	0	0
sshd	1	0	0	0	0	0	0	0	0	0
sshd	3	0	0	0	0	0	0	0	0	0
sshd	1	0	0	0	0	0	0	0	0	0
sshd	1	0	0	0	0	0	0	0	0	0
sshd	1	0	0	0	0	0	0	0	0	0
sshd	1	0	5	336	1520	1	0	0	0	0
sshd	1	0	4	232	1052	0	0	0	0	0
sshd	1	0	0	0	0	0	0	0	0	0
sshd	3	0	9	168	320	0	0	0	0	0
sshd	1	0	11	380	2004	0	0	2	0	0
sshd	1	0	5	192	972	0	0	1	0	0
sshd	3	0	14	532	2484	1	0	2	0	0
sshd	1	0	18	2420	996	0	2	1	0	0
sshd	1	0	48	256	772	0	0	1	0	0
sshd	1	0	5	340	1476	1	0	0	0	0
sshd	1	0	4	188	760	0	0	0	0	0
sshd	3	0	9	204	412	0	0	0	0	0
sshd	1	0	10	236	1220	2	0	0	0	0
sshd	1	0	9	144	604	1	1	0	0	0
sshd	15	0	102	6980	82576	2	0	7	0	0

Table 2-17 Tabular listing of the elements of the process status panel.

Label	Meaning	Comment
Last ACK	Number of sockets in state LAST_ACK owned by processes with this name	

After selecting a single process name from the status panel the button **Show Details** may be used to retrieve more in-depth information about the status of the selected process.

Fig. 2-10 Sample Info Dialogue window



This pop-up window allows you to retrieve more detailed information on the following items:

- process IDs of all processes with the same name
- detailed list of all open files
- IP addresses and ports of listening TCP sockets
- local IP:port and remote IP:port combinations of all established sockets
- IP addresses and ports of UDP sockets

Using the option Single PID allows tracking each task down to single processes. This can be helpful for tasks such as ssh which forks one process for each connection or for the firewall processes.

For each of the listed processes or process groups the following information is displayed:

Table 2-17 Tabular listing of the elements of the process status panel.

Label	Meaning	Comment
Name	Name of the process	
Proc	Number of processes with the same name	
%CPU	Used CPU load in percent	
Num FD	Number of file descriptors used by processes with this name	
Memory	Memory in kB used exclusively by processes with this name	
Shared	Shared memory in kB used by processes with this name	
Listen	Number of listening TCP sockets owned by processes with this name	
Establ.	Number of established sockets owned by processes with this name	
UDP	Number of UDP sockets owned by processes with this name	
Syn Sent	Number of unanswered SYN packets sent by processes with this name	Number of unanswered SYN packets for which the time out has not yet expired.
Close	Number of sockets owned by processes with this name	

## 2.4 Resources Tab

This tab displays the current usage (fill state) of all currently mounted file systems. Each file system is identified by its mount point. The current usage is indicated by a coloured bar and a small line of text. The coloured bar is separated into three distinct regions. Within the first region (0 %-70 %) the bar is green, within the next region (70 % < usage < 90 %) the bar is yellow, and within the last region (usage > 90 %) the bar will be red. Status information is updated in real time.

**Note:**  
 The status condition of the disk subsystem as a whole changes from green ■ to yellow ■ or red ■ as soon as a single file system reaches the respective status.  
 Usage will hardly ever fall short of 5 % for an ext2 file system as this amount is reserved by default for operating system specific purposes.

In a phion default installation the following file systems should at least be present:

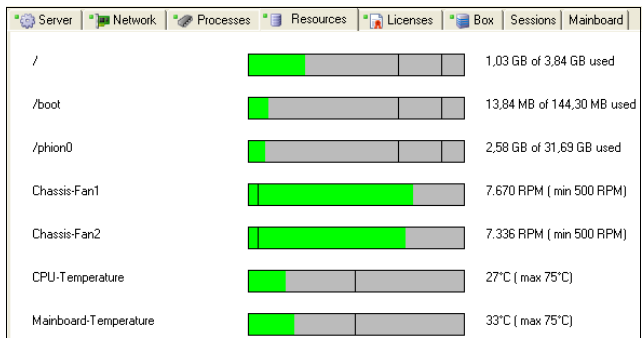
- `/` - file system root directory
- `/boot` - holds boot images (usually located at the beginning of a disk)
- `/phion0` - holds logs and statistical data

**Note:**  
CD-ROMs and floppy disks are not shown in this view.

Furthermore, the following speed and temperature information is presented:

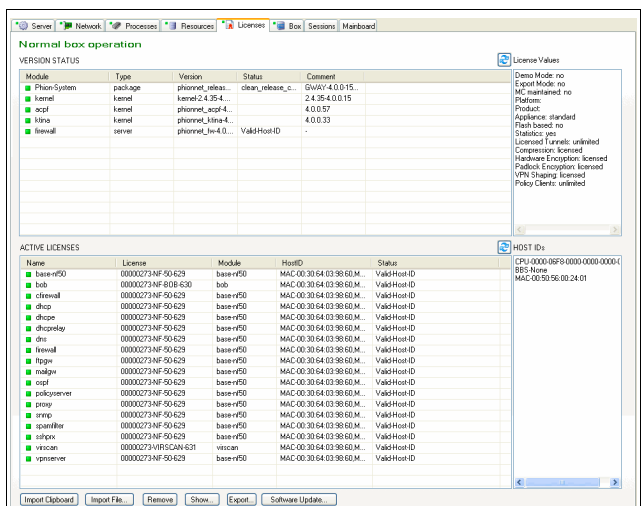
- **Chassis-Fan1** - speed of fan 1
- **Chassis-Fan2** - speed of fan 2
- **CPU-Temperature** - temperature of the CPU
- **Mainboard-Temperature** - temperature of the main board

Fig. 2-11 Sample Resources tab



## 2.5 Licenses Tab

Fig. 2-12 Box Control > Licenses Tab



The **Licenses** tab is the license management tool serving license control. It gives an overview of the license status, can be used to import and export licenses and to execute software updates on single boxes. License handling is

described in detail in a separate chapter (**Licensing**, page 497).

### 2.5.1 Section Version Status

This section lists the version and build date of the installed phion software modules. Double-click an entry to view information in more detail. The following is of major importance:

Table 2-18 Version Status - Properties

Label	Value	Description
Module		Module name
Type		Type of module
Version		Version number
Status	Latest Kernel	The latest phion compiled kernel
	Clean Release	Release Version number/binary match
	Dirty Release	Release Version number/binary mismatch
	No License Found	No license found for this module
	Not Used	This module is not used
Comment		Comment

### 2.5.2 Section Active Licenses

This section lists all active licenses. The list content can be edited by using the following available buttons:

- **Import Clipboard**  
Imports a license from the clipboard.
- **Import File ...**  
Imports a license from a (.lic) file.
- **Remove**  
Removes a selected license from the system.
- **Show ...**  
Displays the certificate the license is included in.
- **Export ...**  
Exports the license to a (.lic) file. Use this feature for saving and recovery purposes.
- **Software Update ...**  
Specify the path to the update package (\*.rpm or .tgz) and click **Open**. A consistency check is performed and after a positive check the install routine has to be confirmed to install a Software Update.

### 2.5.3 Section License Values

This section lists important license details.

### 2.5.4 Section Host IDs

This section lists hardware IDs available in the system node-locked licenses can be attached to. For details on significance of HOST IDs see **Licensing**, page 497.

## 2.6 Box Tab

The **Box** tab of the control window is used for controlling key aspects of box operation. It consists of three sections and a report window.

Fig. 2-13 Network Activation dialogue

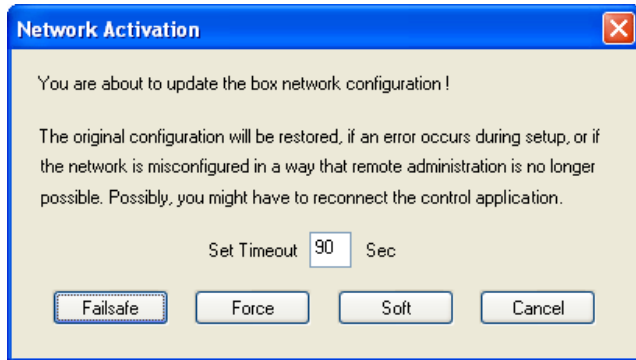
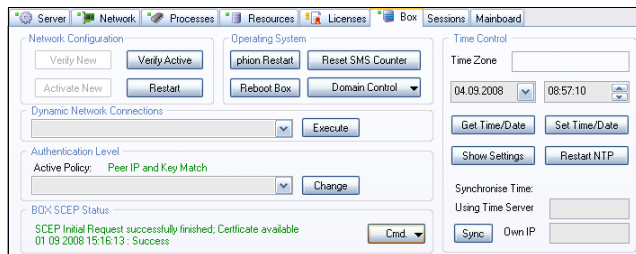


Fig. 2-14 View of the box control window



### 2.6.1 Section Network Configuration

This section allows the administrator to control the network configuration of a box.

#### ➤ **Verify New**

Used to verify a new network configuration.

#### **Attention:**

Altering the network configuration of a remotely controlled box represents a critical operation. A new configuration file will not automatically be activated upon transmission from the single box or master server (if managed via an MC). This button will thus only be active when a new network configuration file has been sent but not yet activated. You must first locally (on the box itself) verify the logical consistency of the new network configuration file. The report window will display the results of the consistency check. In case of a seemingly flawed file you must not activate the new configuration. Correct the errors and scrutinise the altered network configuration file again.

#### **Note:**

The newly received network configuration file is stored in `/opt/phion/preserve/boxnet.conf`.

#### ➤ **Activate New**

Activates the new network configuration.

When the new network configuration file has successfully passed the consistency check, the new configuration may be activated. Clicking this button

opens a window with the following buttons and corresponding functions:

List 2-1 Types of network activation

Network activation type	Impact
<b>Failsafe</b>	<p>Fail-safe network activation is the safest way to activate configuration changes. Always use this network activation type on productive systems, for example, to:</p> <ul style="list-style-type: none"> <li>➤ add/delete network interfaces</li> <li>➤ change network interface configurations</li> <li>➤ add/delete policy routes</li> <li>➤ delete direct/gateway routes</li> </ul> <p>Failsafe network activation is processed in the following way:</p> <ul style="list-style-type: none"> <li>➤ The system creates a backup file of the active network configuration.</li> <li>➤ It then temporarily activates the configuration changes and verifies that the system can still be contacted by the graphical administration interface <code>phion.a</code>.</li> <li>➤ If this verification is successful the network is restarted so that the changes are activated permanently.</li> <li>➤ If verification fails within the timeout defined in the <b>Set Timeout</b> field, the original network configuration is restored.</li> </ul> <p><b>Note:</b> Especially when activating network configuration changes via a VPN connection, you might sometimes lose connection to the box. This will lead to connection verification failure between the system and the graphical administration tool <code>phion.a</code> and cause that the original configuration is restored. You might have to use Force network activation if you experience this issue. <b>Use with due care.</b></p>
<b>Force</b>	<p>Forced network activation immediately activates the new network configuration without the checking routine described above and without backup creation.</p> <p><b>Attention:</b> Use forced network activation with due care.</p>
<b>Soft</b>	<p>The following additions may be done through soft network activation:</p> <ul style="list-style-type: none"> <li>➤ adding of direct routes</li> <li>➤ adding of gateway routes</li> </ul> <p>Soft network activation appends routes that have been configured in the Routing tab (<b>Configuration Service</b> - 2.2.5.5 Network Routes, page 68) of the box network configuration to the system's routing table.</p> <p><b>Note:</b> Soft network activation cannot be used to add/delete policy routes or to delete direct or gateway routes permanently.</p> <p><b>Note:</b> Direct/gateway routes that have been deleted using Soft network activation will be marked as wild in the Box Control &gt; Network tab (see 2.2.8 Tables, page 32). Use Failsafe network activation instead or subsequently activate route deletion permanently by restarting the network (see <b>Restart</b> button below).</p>
<b>Cancel</b>	<p>Cancels activation of network configuration changes.</p>

#### ➤ **Restart**

Re-initialises networking. Shuts down and subsequently restarts networking.

#### **Note:**

The server subsystem is unaffected by this procedure. Yet, server/service functionality will be unavailable for a short time as the network goes down and up.

- **Verify Active**  
Verifies the active network configuration. Does exactly the same as **Verify New** but using the active configuration file.

## 2.6.2 Section Operating System

- **phion Restart**  
Clicking this button will shutdown and subsequently restart all servers and services belonging to the phion subsystem. This includes the phion firewall engine.

**Attention:**  
All connections will be lost after clicking this button. This includes non-phion proprietary services such as secure shell (SSHd) and network time protocol (NTPd).

Clicking on this button is almost the same as invoking the following two commands from the command line:  
`/opt/phion/bin/phionctrl shutdown`  
`/opt/phion/bin/phionctrl startup`  
 The only difference is that the control daemon itself is not stopped and started. To perform this, you have to actually login on the shell.

- **Reboot Box**  
As a more radical re-initialisation you can perform a reboot of the box. Some systems might have problems with BIOS settings and do not perform the reboot correctly or get stuck on a lower layer. You may have to worry about getting the box back online if it is not easily physically accessible to you. Use with adequate care.
- **Reset SMS Counter**  
This button resets the SMS parameters described in **Configuration Service** - 2.2.3.7 SMS Control, page 57.
- **Domain Control**  
Click this button to display the registration status of a box at a Windows domain (**Show Registration Status**) or to register a box as Windows domain member at a domain controller (**Register at Domain**). Utilisation of this button requires prior MSCHAP profile configuration (**Configuration Service** - 5.2.1.2 MS-CHAP Authentication, page 112). After clicking the button a **User Authentication** window expects authentication of a user with appropriate administrative rights to add the box to the domain.

Fig. 2-15 Box Domain Registration dialogue



## 2.6.3 Section Time Control

This section provides functionality for adjustment of time settings.

- **Get Time/Date**  
Click this button to view current time and date.
- **Show Settings**  
Click this button to view current NTP settings.
- **Set Time/Date**  
Insert date and time into the fields above, and click this button to change current time settings. Remember that on systems, which are configured to synchronise date and time with an external time server, manual changes will be overwritten by the succeeding time synchronisation.
- **Restart NTP**  
Click this button to restart all NTP services.
- **Sync**  
Click this button to synchronise time settings with a NTP server manually.  
If the **Using Time Server / Own IP** is unspecified, the synchronisation process binds to the system's primary management IP. This synchronisation method will work flawlessly with a time server that is placed in the same network as the primary management IP.  
For time synchronisation with a public time server, insert the external IP address of the firewall into the **Own IP** field, to prevent that the time server's response is blocked by the firewall.

## 2.6.4 Section Dynamic Network Connections

If configured and available, dynamic network connections can be manually manipulated (off, on, start, stop, restart, reset) by selecting the appropriate item from the menu and clicking the **Execute** button. The following network connections may appear in the list: xDSL-, ISDN-, and DHCP (cable)-connections, UMTS and MGMT (box management) tunnel connections.

## 2.6.5 Section Authentication Level

This section allows selecting the level of authentication that is effective for non-interactive management centre logins and HA synchronisation. The following authentication levels are available:

Table 2-19 Possible authentication options

Setting	Meaning and effect
No Authentication	Level -1: anything goes. The system allows any attempt to send or fetch configuration data. <b>Note:</b> Use only if necessary and revoke as soon as possible.
Check Key or IP address	Level 0: Login is accepted if either IP address or key challenge are successful. Still quite insecure.
Check IP address	Level 1: Still quite insecure.
Check Key	Level 2
Check Key and IP address	Level 3: This is the default setting that should not be changed unless there is need to lower the security level temporarily.

The default setting **Check Key and IP address** is the highest authentication level and should not be changed



# Configuration Service

<b>1.</b>	<b>Overview</b>	
1.1	phion Management Concept .....	43
1.1.1	The Administrative Layer .....	43
1.1.2	The Physical Layer .....	43
1.1.3	The Logical Layer .....	44
1.1.4	The Functional Layer .....	44
1.2	Elements of the Configuration Window .....	44
<b>2.</b>	<b>Configuring a New System</b>	
2.1	General .....	48
2.1.1	Screenshots .....	48
2.1.2	User Interface .....	48
2.2	Setting up the Box .....	49
2.2.1	Context Menus of the Configuration Tree .....	51
2.2.2	Box Properties .....	51
2.2.3	Administrative Settings .....	53
2.2.4	Identity .....	60
2.2.5	Network .....	61
2.2.6	Traffic Shaping .....	81
2.2.7	Administrators .....	91
2.2.8	Box Licenses .....	93
<b>3.</b>	<b>Configuring a New Server</b>	
3.1	General .....	94
3.2	Server Configuration on Single Boxes .....	95
3.2.1	General .....	95
3.2.2	Monitoring .....	95
3.2.3	Scripts .....	96
3.3	Server Configuration on MC-administered Boxes .....	96
3.3.1	Identity Tab .....	96
3.3.2	GTI Networks .....	96
<b>4.</b>	<b>Introducing a New Service</b>	
4.1	Configuration .....	97
4.1.1	General view .....	97
4.1.2	Statistics view .....	97
4.1.3	Notification view .....	98

## 5. Managing the System

5.1	Box Settings - Advanced Configuration .....	100
5.1.1	System Settings .....	100
5.1.2	Bootloader .....	101
5.1.3	System Scheduler .....	102
5.1.4	Inventory .....	103
5.1.5	Log Cycling .....	103
5.1.6	Message Board .....	105
5.1.7	Access Notification .....	105
5.1.8	SSH .....	106
5.1.9	Software Update .....	108
5.1.10	Watchdog .....	108
5.2	Box Settings - Infrastructure Services .....	111
5.2.1	Authentication Service .....	111
5.2.2	Host Firewall Rules .....	115
5.2.3	Syslog Streaming .....	115
5.2.4	Control .....	117
5.2.5	Statistics .....	118
5.2.6	Eventing .....	118
5.2.7	General Firewall Configuration .....	118
5.2.8	Log Configuration .....	119
5.3	Creating PAR Files .....	119
5.4	Restoring/Importing from PAR File .....	119

## 6. Repository

6.1	Creating a Repository .....	121
-----	-----------------------------	-----



# 1. Overview

## 1.1 phion Management Concept

Before delving into the depths of configuration issues we first have to get acquainted with the basic configuration entities which phion operated systems rely on. It is of paramount importance to develop an understanding for these entities and to understand how they are linked together to achieve the required administrative and operative interaction of function units.

phion management is based on the following three configuration entities:

- **Box**
- **Virtual Servers**
- **Assigned Services**

These are the key elements of a hierarchical data model. They also exist as separate elements in the configuration tree. A further entity is **module**. You will encounter module only indirectly when specifying the very nature of a service.

To represent the phion management model a hierarchical database design has been adopted. For lean database management and simple database backup phion has chosen to implement this proprietary database entirely in file-space. The database is session and transaction based. Referential integrity is warranted by database design and assisted by separate tree maintenance and reconstruction utilities.

The available configuration entities and their interdependencies are visualised by help of the schematic diagram depicted in figure 3-1, page 43. The diagram shows four distinct layers to which the entities are assigned. We distinguish between a physical, a logical, a functional, and an administrative layer. Note that the module entity is associated with required software functionality and system design. The module entity is thus on par with the service entity.

We may assign a particular configuration layer to each entity:

- The **Box** as a piece of hardware represents the physical layer.
- The **Virtual Servers** represent the network addresses under which certain services are made available. Since a server can be assigned to more than one box (for high availability purposes) it extends the traditional notion of a server as a piece of hardware. The server entity belongs to what we refer to as the logical layer.
- The **Assigned Services** as the actual workhorse belongs to the functional layer. To provide the required functionality the services make use of software modules.
- Administrator=Root constitutes a further **administrative layer** which is of no particular significance in case of a single box.

### 1.1.1 The Administrative Layer

This layer comprises the only administrator of a single box, the root administrator. As such it is of no particular relevance for a single box. Whereas the single box management does not foresee administrative roles it allows for the introduction of root aliases. Root aliases make it possible that several administrators (in each case with root permission) may manage the box. Each of them has his own login ID and password or public RSA key. For each configuration item in the tree a history file with detailed file actions, origin, and root alias exists. Tree history will thus show which of the root aliases has modified which files respectively.

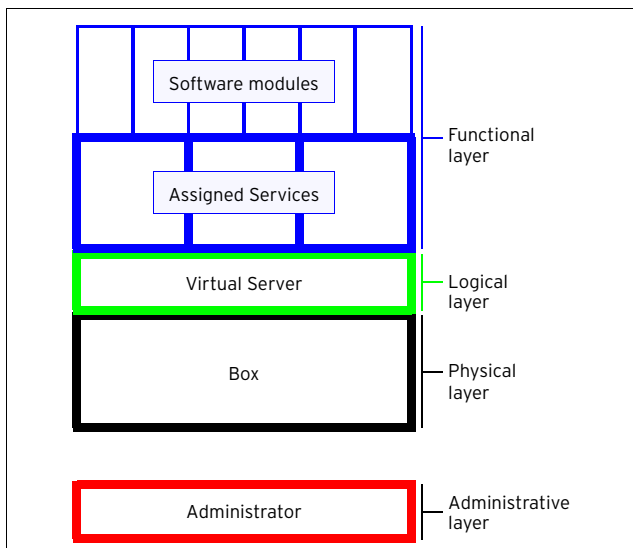
The remaining three layers comprise what might be referred to as the operational entities.

### 1.1.2 The Physical Layer

This layer contains a single entity named box. The box corresponds to a piece of hardware with an operating system and a number of phion software modules required for the management of the box. The box acts as the basic platform for higher-level software functionality (for example firewalling, VPN-Service, SMTP-gatewaying, ...) provided by server/service combinations. The box contents itself with providing the required underlying networking functionality, basic administrative services, such as logging or accumulation of statistical data, and a daemon for remote configuration updates. Most notably it also hosts the control daemon which is in charge of watching and controlling the operation of all additional advanced software functionality as well as advanced networking needs.

In a manner of speaking one could refer to the primary IP address of the box as a default server address under which all functionality required for the management of the box is made available. We refer to the services providing this functionality as box services, see also the section on the control, event, log, and statistics windows.

Fig. 3-1 Interdependencies of the various basic configuration entities



Each box service corresponds to a different software module.

The following modules are available as box services:

**Table 3-1** Required software modules sufficient for management and controlled low level operation of a box

Module name	Daemon	Task
bdns	bdns	Local DNS service
boxconfig	boxconfigd	Management of configuration updates
boxfw	boxfw	Local Firewall
bsms	bsms	Service for control via SMS
bsyslog	bsyslogd	Syslog streaming of log data to a remote log host
control	controld	Control of box and server/service operation
cstat	cstatd	Collection of statistics
dist	distd	Transfer daemon for High Availability and management centre
event	eventd	Configurable active notification via mail, SNMP traps or pop-up window
log	logd	Logging
logwrap	logwrapd	Log file rotation and indexing
phibs	phibsd	Authentication service facility
psyslog	psyslogd	Connectivity bridge to syslogd
qstat	qstatd	Handling of statistics queries

**Note:**

The box services (except for cstat which does require a license to write statistics to the disc) do not require a license to be active. They form, what we refer to as, the **phion box infrastructure**.

Since the box represents the platform that hosts higher-level software functionality it may also operate completely independently. For this reason the box itself as a configuration object does not need to know anything about servers or services.

### 1.1.3 The Logical Layer

This layer contains a single entity named server. For phion operated systems the server in main incorporates one or several IP addresses, which enables utilisation of higher-level software functionality. The functionality itself is not directly provided by the server but by software modules called services (see 1.1.4 The Functional Layer). In contrast to the traditional concept of a server as a piece of hardware providing some functionality the phion approach facilitates a separation into a physical server (box) and logical server(s) (server).

**Note:**

Since all software functionality is made available under the server's own IP addresses we may easily transfer functionality from one box to another by simply transferring the respective IP addresses. High availability is thus achieved by assigning a server to a primary and a secondary box, which both hold all relevant configuration data. Moreover it becomes quite simple to migrate a server from one box or from a pair of boxes to another box or a pair of boxes.

A server has to be assigned to at least one box to have any operational impact. Moreover a server can be assigned to a

pair of boxes to achieve High Availability (**High Availability**, page 375).

### 1.1.4 The Functional Layer

The functional layer comprises two entities, service and module, as shown in figure 3-1, page 43.

phion ships all available software modules as part of the standard distribution. You will need an appropriate license key to activate a module's functionality beyond the trial period.

The service entity is basically the outer shell for a software module. Therefore a service provides the software functionality it inherits from an encapsulated software module. Moreover, a service carries all further information required to actually harness the software functionality. This includes the IP port under which functionality is made available, as well as other settings.

A service is explicitly assigned to a single server.

## 1.2 Elements of the Configuration Window

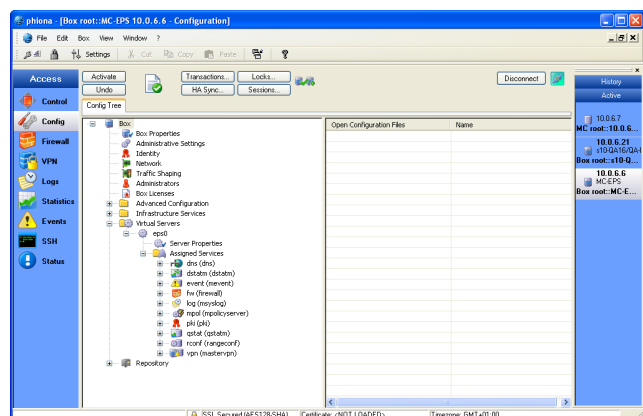
As soon as you establish a connection to the box configuration daemon (boxconfig) you are allotted your own private session. The ID of your session is shown in the window bar of the config dialogue window.

**Note:**

The GCSID (**Generic Configuration Session ID**) contains the following elements: IP and source port of connecting client followed by the PID of the server process (daemon **boxconfigd**) handling the current connection.

Session based operation is a necessary prerequisite for two major reasons: Firstly, it forms the basis for simultaneous access of several administrators to non overlapping regions of configuration space. Secondly, changes are made to a copy of the configuration tree, thereby not affecting the momentary operational status. In case you wish to have changes made undone sessioning lets you carry out an undo. In order to commit your changes you will have to click **Activate**, which requires a separate wilful act.

**Fig. 3-2** Box configuration window in compressed connection state



The box configuration window is divided into three main areas:

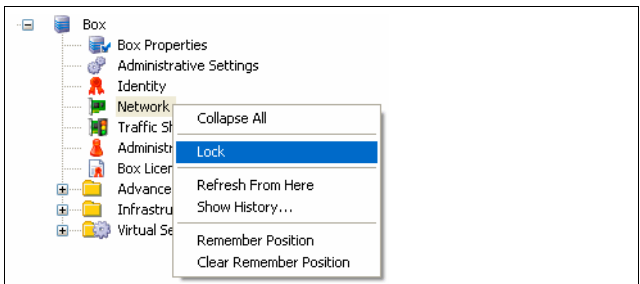
- The upper part is reserved for several control buttons and combo boxes used to retrieve tree, session, and update status information, change the view of the tree, and activate or undo configuration changes made during the current session.
- The left frame contains all configuration entities.
- The right frame shows all open configuration files

In order to prevent inconsistencies in the tree configuration files, an administrator who wishes to modify has to lock the configuration. This guarantees that only one single authority has write access to the file at one time.

To create a lock move the mouse over the desired configuration item in the configuration tree, press the right mouse button and select **Lock** from the menu.

**Note:**  
If you lock a directory or a whole branch of the tree, all items belonging to this directory or branch will also be locked.

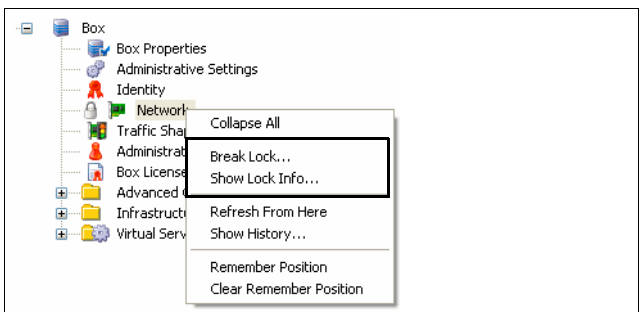
**Fig. 3-3** Menu after pressing right mouse button on yet unlocked item



**Table 3-2** Lock indicator icons

Symbol	Meaning	Comments
	Own lock on branch	After locking a whole branch of the tree this icon is displayed next to the branch icon.
	Foreign lock on branch	Icon denoting a lock on a whole branch by another session.
	Own sublock	After locking a whole branch of the tree this icon is displayed next to the icon of each item in the branch.
	Foreign sublock	Icon denoting a lock on an item of a branch by another session.

**Fig. 3-4** Menu after pressing right mouse button on locked item from another session



If someone else has created a lock you may want to find out to whom the lock belongs to. Therefore simply move the mouse over the locked item in question and press the

right mouse button. Then, select **Show Lock info ...** from the menu.

You may break foreign locks if they belong to broken sessions older than 10 minutes. Locks belonging to intact or active sessions may not be broken. This is necessary in order to not interfere with other administrator's sessions.

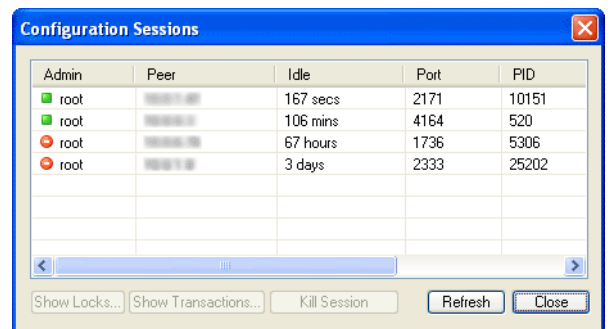
However, you may kill the session that owns the lock. Your ability to do so depends on both, your range affiliation (principal range) and authorisation level.

**Note:**  
An active session turns into a broken session when the associated client is suddenly disconnected and has not successfully reconnected.

**Attention:**  
Killing a session means initiating a forced undo on the database. As a consequence the admin owning the session will lose all not yet activated configuration changes made to the tree.

The **Configuration Sessions** window is invoked by clicking on the **Sessions** button located in the upper part of the configuration window.

**Fig. 3-5** Configuration Sessions window



We strongly advise against indiscriminate killing of active foreign sessions. We recommend to make use of the **Show Locks ...** and **Show Transactions ...** buttons of the session window to retrieve detailed information on the current and past activities inside the targeted session.

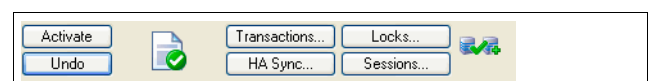
Newly introduced elements are marked by the "new indicator" icon . Altered items such as edited files are marked with the "changed indicator" icon . Items to be deleted are marked with a "deleted indicator" icon .

**Note:**  
You may not delete arbitrary items. Deletable items need to be deleted via the right mouse button menu. Currently only services, servers, and HA partner boxes are deletable.

All of these indicators apply to items inside your session.









The cumulative session status (upper part, figure 3-2, page 44) will automatically change from a "no modifications" state to a "some modifications" state if only a single item has been introduced, changed or marked for deletion.

**Fig. 3-6** Box configuration window - detail



The following states are available:

**Table 3-3** Box configuration window - icons

Icon	Description
	no changes in session
	node: changes in session but not yet sent global: changes not yet activated
	session locked (read-write mode)
	session locked by another administrator (read-only mode)
	RCS file imported but not yet accepted
	configuration file write protected
	linked configuration file
	configuration file is going to be deleted

**Note:**

Status changes of the tree (locks triggered by someone else) are not necessarily immediately visible to you as the management console only periodically retrieves tree status information. You may speed up the process by making use of the right mouse button menu item **Refresh From Here / Refresh Complete Tree** (right mouse button on the box itself).

It is advisable to unlock (again by holding down the right mouse button) all locked configuration files before quitting a session or temporarily quitting after another task. You may find out about your own locks by making use of **Locks ...** located in the upper part of the configuration window.

An active session that gets terminated unexpectedly may be resumed by simply reconnecting to the box. This feature gives extra protection against loss of configuration changes due to network hick-ups. If you disconnect or logout properly your session will be cleared (undo on database).

Note that configuration dialogue windows (for each item) are issued with a **Lock** and a **Send Changes** button. Thus after double-clicking a yet unlocked item you may also lock the item from within the respective configuration dialogue.

**Send Changes** is of particular importance as all changes that have not been sent only reside within the GUI, but have not yet been added to your session. This means that further configuration changes depending on not yet sent changes will not be possible. Moreover, unsent configuration information will not be recoverable by a reconnect in case of unexpected connection termination. The notable difference here is introduction or deletion of either server or service, where invoking the action as such automatically involves a send changes operation. In order to actually activate the changes made within a session you have to activate them.

To this end the main configuration window features a button labelled **Activate**. Before activating you may investigate the effects your configuration changes will have on the various configuration entities and the tree.

- Clicking **Send Changes** only sends the changed configuration to the management centre (or Box configuration service if the changes are performed directly on a netfence gateway) were it is associated with the current session ID. In this state the performed changes are neither sent to the gateway nor merged into the configuration tree at the management centre. The latter also means that the configuration changes are not visible to other administrators, as each configurative connection gets its own session ID assigned.
- Clicking **Transactions ...** opens a new window listing all pending changes associated with the current session ID (for example changes executed from the current phion.a window). As configuration changes may depend on each other (changing the bind IP in the Service Configuration section may require server IP changes in the Server Configuration section) configurative changes are not activated immediately. Activate pending changes by clicking **Activate**.
- When you click on **Undo** all pending transactions (configuration changes which have not been activated yet) are undone. Click **Transactions** to view currently pending configuration changes.
- **HA Sync** allows management of the configuration synchronisation between the boxes and visualises the synchronisation status (in case of HA boxes or a HA management centre). The window contains the following elements:
  - **Synchronisation Status** - Status of the configuration synchronisation. If a HA sync is pending the appropriate information is displayed, otherwise the informational text will be "Nothing to synchronise".
  - **Last Action** - displays details about the last HA sync, for example date and time when the last synchronisation sequence was performed or failure reasons if the last sync failed.
  - **HA Partner IP** - This field allows configuration on how synchronisation should be performed. The HA partner IP can either be the primary Box IP of a HA partner or in case of a dedicated HA link a management IP within the HA network. Selecting the checkbox on the left labelled **Change Address** enables read-write mode.
  - **Use Sender IP** - Here the sender IP for the HA synchronisation can be changed. In general this IP will be the primary Box IP. Selecting the checkbox on the left labelled **Change Address** enables read-write mode.
  - **Do Update** - If a HA sync is pending the synchronisation can be triggered immediately by clicking this button. If configuration has not changed since the last successful synchronisation procedure, nothing is done.
  - **Do Complete Update** - Synchronises the complete configuration tree of the current box to the HA partner box.
  - **Discard Update** - Discards a pending configuration synchronisation.

↗ **Clear Dirty Status** - If the primary box fails, configuration changes have to be performed on the secondary box. In normal operation it is not possible to alter configuration via the secondary box. If there is the need to do so, the HA box has to be switched to the Emergency Override mode. After re-establishing the primary box, the synchronisation has to be started manually.

Previous versions of netfence required shell access with root permissions to manually restore a clean configuration state. Instead of using the command line netfence 4.2 allows restoring a clean configuration state by using the GUI. The administrative role "Manage HA Sync" grants this privilege even to non-root administrators.

↗ **Refresh** - Refreshes the current window thus reflecting the new Synchronisation Status and displays up to date information in the "Last Action" field.

↗ **Close** - Closes the HA Box synchronisation window.

**Table 3-4** Buttons of configuration window for session management and status retrieval

Button	Description
<b>Send Changes</b>	Transfers changes from the management console to the session held at the CAS.
<b>HA Sync</b>	Displays update status in case of a HA reinforced installation.
<b>Transactions</b>	Displays transaction to be carried out to the tree by changes made during the session.
<b>Undo</b>	Undoes all not yet activated changes made during a session.
<b>Activate</b>	Activates changes made during the session on the configuration tree on the CAS.



## 2. Configuring a New System

### 2.1 General

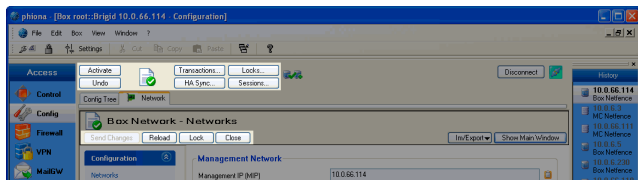
#### 2.1.1 Screenshots

The screenshots below are examples and may therefore slightly differ from the current display of your system. When configuring a netfence, the parameter sequence described in this document has to be adjusted to your settings.

#### 2.1.2 User Interface

##### 2.1.2.1 General Buttons

Fig. 3-7 User Interface



First let us have a look at the lower button bar (figure 3-7):

##### ➤ **Send Changes** button

With regard to the multi-administrator concept of phion netfence, configuration changes are not carried out in the productive environment of the netfence gateway. The concept requires you to send modifications to the netfence system manually, and thereafter activate the new configuration explicitly by clicking **Activate** in the upper button bar (described below).

##### ➤ **Reload** button

Pressing this button reloads the currently active settings. Use **Reload** to undo configuration changes.

#### Attention:

Clicking **Reload** undoes all configuration changes which have not yet been sent with **Send Changes**.

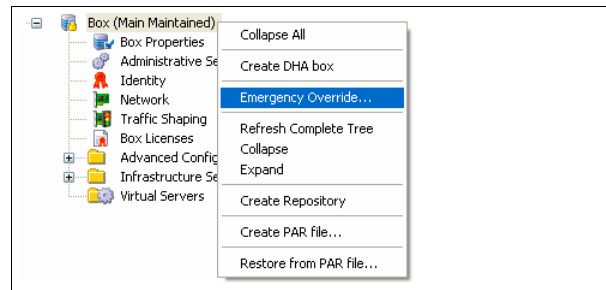
##### ➤ **Lock / Unlock** button



With regard to the multi-administrator concept of phion netfence, the default state of a configuration object is set to read-only. Its state has to be set to read-write to make it editable. Click **Lock** to lock an object for your exclusive use. You will now be able to edit it. Click **Unlock** to allow locking for other administrators. When sending changes you will be asked if locks should be kept.

#### Note:

Should it be required to edit the configuration of an MC-managed box locally, the state of the box has to be set to **Emergency Override** mode. Select **Emergency Override** from the context menu of the box to do so (see below).

Fig. 3-8 Config tree - Emergency Override



As soon as the box is in emergency override mode the box icon changes from  to .


Please consider that any configuration change on a box in emergency override mode has to be repeated on the management centre.


##### ➤ **Close** button

This button closes the configuration dialogue. When closing a modified dialogue without sending changes, a pop-up with respective information will open. Choose the appropriate answer to confirm or cancel your action.

The upper button bar (figure 3-7, page 48) is described in Elements of the Configuration Window, page 44.

#### 2.1.2.2 Configuration User Interface

Mandatory parameters / parameter sections are indicated using the  icon.

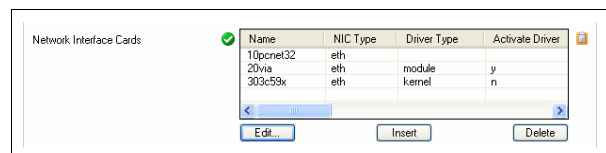
Modified parameters / parameter sections are indicated using the  icon.

The following phion.a-specific configuration masks need closer examination:

##### ➤ **Edit ... / Insert ... / Delete** mask

Some masks will display a listing with the format Edit/Insert/Delete.

Fig. 3-9 Example for an Edit ... / Insert ... / Delete mask



To edit an already existing entry, select it and click **Edit ...**

To create a new entry, click **Insert ...**

Both, **Edit ...** and **Insert ...**, open the same configuration dialogue.

To remove an existing entry, select it and click **Delete**.

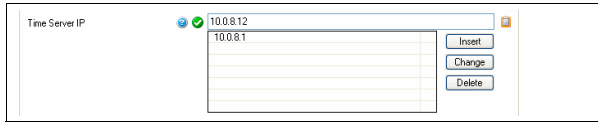
##### ➤ **Change / Insert ... / Delete** mask

This mask supplies a field for entering values on the left side and a list of possibly already existing values on the right side.

The example in figure 3-10 shows 10.0.8.1 in the value list and 10.8.8.12 in the field meant for adding new entries. Sending changes and activating them will only activate 10.0.8.1. 10.0.8.12 will be ignored as it has not

yet been added to the list. Always be aware that only values appearing in the list will be added to the configuration.

**Fig. 3-10** Change / Insert ... / Delete mask

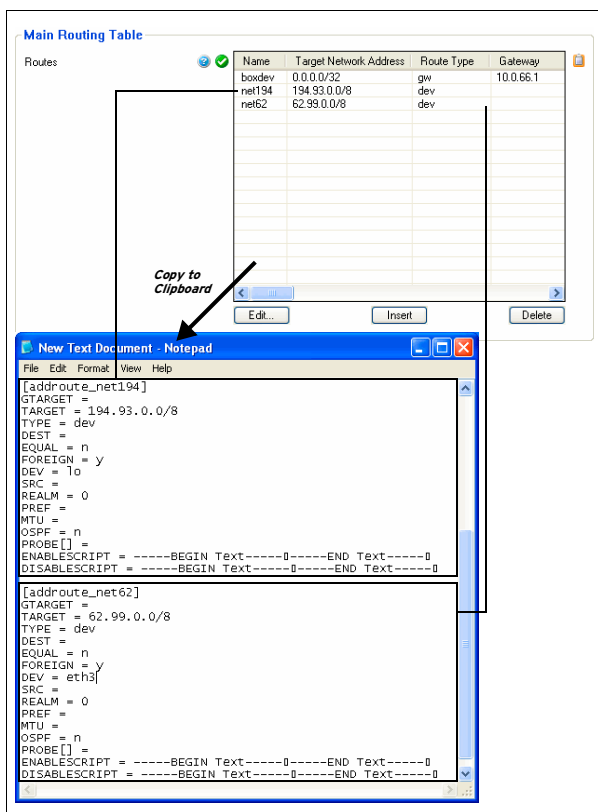


To edit an already existing entry, select it, modify the value in the field on the left side and click **Change**.  
 To create a new entry, enter the desired value into the field on the left side and click **Insert ...**  
 To remove an existing entry, select it and click button **Delete**.

As shown in the screenshots above, each parameter keeps the icon ready. Click on the icon to allow for the following interaction with the clipboard:

- **Copy to Clipboard**  
 Copies the value (or several values in case of lists or subsections) from the current parameter to the clipboard. The clipboard contains a special header. The content is formatted as plain text.
- **Replace With Clipboard**  
 If the clipboard contains a valid configuration entry (plain text and a special header as is generated by copying to clipboard using phion.a) the current section/parameter is replaced by the clipboard content.
- **Merge With Clipboard**  
 The current section/parameter is merged and/or replaced with the values from the clipboard. Consider the following example for better understanding:

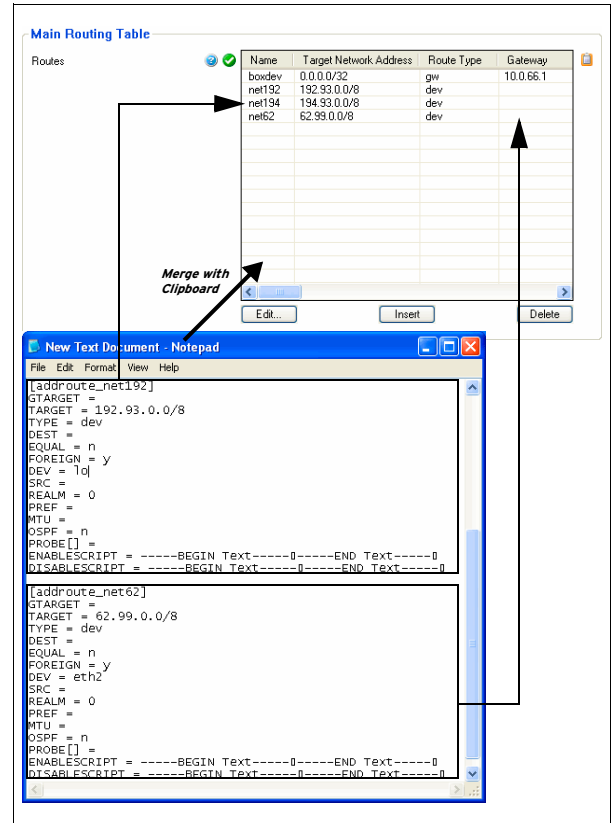
**Fig. 3-11** phion.a Configuration list and part of Clipboard content after Copy to Clipboard



Let us assume the following modifications:

- new routing **net192** (using **net194** as template)
- interface (entry DEV =) of routing **net62** from **eth3** to **eth2**

**Fig. 3-12** Part of Clipboard content and phion.a Configuration list after Merge with Clipboard



As you can see in figure 3-12, a merge of the modified clipboard content with the configuration file content results in:

- overwritten interface value of entity net62
- added entity net194
- untouched entity net192

**Note:**  
 The clipboard functions are only available within fields of the same kind.

## 2.2 Setting up the Box

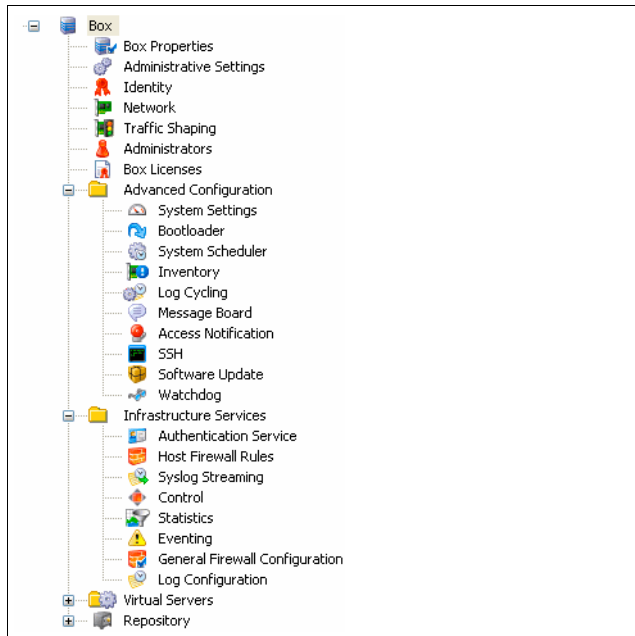
The box is a vital configuration entity which actually corresponds to a solid piece of hardware. The box as a whole is a rather complex configuration object. However, as far as the basic configuration is concerned only very little information has to be supplied. However, the settings the box comes up with after installation will not suffice to exploit the full potential of a phion system.

The box is special insofar as it represents the hosting platform for a phion system. It is essential that all relevant aspects of the basic box operations are individually adjustable. As a consequence of this the tree belonging to an individual box contains a number of box specific configuration files.









In this part of the document you will get familiar with the configuration aspects that are directly associated with the box as a piece of hardware, such as the network configuration, which is the most notable one, as most services can never function without the network being configured correctly.

Fig. 3-13 Structure of the config tree






Unless already open click on the topmost tree element **Box** to unfold the configuration tree.

You will encounter the following distinct elements:

- Four files named  **Box Properties**,  **Administrative Settings**,  **Identity** and  **Network**
- A directory named  **Advanced Configuration**
- A directory named  **Infrastructure Services**
- A directory named  **Virtual Servers**
















The configuration scope of a box borrows from all these elements.

In a first step of issuing a box with more advanced capabilities, it initially suffices to concentrate on the two principal configuration files named  **Administrative Settings** and  **Network**. We will thus start out with a discussion of these two. Next in line is  **Identity** which is security related and is used to set or change the identity, with which the box advertises itself to the world.

**Note:**


The plus sign (+) is used to emphasise the importance of a file. Importance normally goes hand in hand with a certain inherent complexity. The networking configuration is always box specific as it contains the box' IP addresses and thus must not be shared.



Table 3-5 Box specific configuration items

Icon	GUI label	Importance	File name	Description	see ...
	<b>Box Properties</b>	++	box.conf	identification and operational settings	page 51
	<b>Administrative Settings</b>	++	boxadm.conf	administrative parameters, DNS settings, root password, NTP settings, ...	page 53
	<b>Identity</b>	++	boxkey.conf	digital certificate and keys identifying the box	page 60
	<b>Network</b>	+++	boxnet.conf	network configuration of the box	page 61
	<b>Traffic Shaping</b>		boxqos.conf	configuration for traffic shaping	page 81
	<b>Administrators</b>		admindb.conf	specifications of administrator's rights	page 91
	<b>Box Licences</b>		boxlic.conf	contains the license information required for non-demo mode operation of the box	page 103
	<b>System Settings</b>	++	boxsys.conf	important system settings (kernel sysctrls)	page 91
	<b>Bootloader</b>		bootloader.conf	boot behaviour and Linux kernel update settings	page 101
	<b>System Scheduler</b>	+	boxcron.conf	custom cron jobs, for example log file deletion, cooking of statistical data	page 102
	<b>Inventory</b>		boxtype.conf	hardware inventory without operational component	page 103
	<b>Log Cycling</b>		logstore.conf	settings for the log storage utility, the utility is invoked by crond as specified by the settings in cron	page 103
	<b>Message Board</b>		messageboard.conf	enabling/disabling welcome messages for phion.a and system login	page 105
	<b>Access Notification</b>		notification.conf	contains eventing or notification policy for GUI and system logins	page 105
	<b>SSH</b>	+	ssh.conf	fine tuning of settings for openssh based SSH daemon	page 106
	<b>Software Update</b>		swupdate.conf	behaviour upon successful or flawed completion of a software update	page 108
	<b>Watchdog</b>		watchdog.conf	set certain limits on critical system resources and ensure to have them checked at least once a minute	page 108
	<b>Authentication Schemes</b>		authentication schemes.conf	contains configuration for external authentication schemes like MSNT, Radius, LDAP	page 111
	<b>Host Firewall Rules</b>	++	boxfw.fwrule7	defines the local firewall rule set	page 115
	<b>Syslog Streaming</b>		bsyslog.conf	used for (filterable) log data streaming	page 115
	<b>Control</b>		control.conf	settings for automatic session logout, configurable limits for Events 30/31 and parameters for HA partners	page 117
	<b>Statistics</b>	+	cstat.conf	settings for all statistics modules (cstat, qstat, dstats)	page 118
	<b>Eventing</b>	++	event.conf	settings for the event daemon	page 118
	<b>General Firewall Configuration</b>	++	fwparam.conf	settings for both local and forwarding firewalls	page 118
	<b>Log Configuration</b>		log.conf	settings for the log daemon	page 119



## 2.2.1 Context Menus of the Configuration Tree

### 2.2.1.1 Box Context Menu

The context menu is opened by clicking with the right mouse-button onto  **Box** in the configuration tree. It provides the following items:

- **Collapse All**  
Closes all open nodes in the configuration tree down to the top level.
  - **Create DHA box**  
Creates an additional node named  **HA Box**. This node holds an entry  **HA Network** where the network settings for the HA partner have to be configured. The configuration itself is the same as the regular network configuration (2.2.5 Network, page 61). You can only create one HA partner for each box.
- Note:**  
When initially creating the HA box IPs in section Additional Local Networks the IP addresses are automatically set in the HA network. Before installing the HA box check for correct additional IPs in the HA Network node.
- **Emergency Override**  
This entry is only available if the box is administered by a management centre. It allows local configuration of a box.
- Attention:**  
Be aware that if doing so the synchronisation with the management centre has to be carried out manually
- **Refresh Complete Tree**  
Updates the view of the configuration tree.
  - **Collapse**  
Closes all open nodes in the configuration tree down to the top level.
  - **Expand**  
Opens all nodes in the configuration tree.
  - **Create Repository**  
See 6. Repository, page 121 for details.
  - **Create PAR file ...**  
See 5.3 Creating PAR Files, page 119 for details.
  - **Restore from PAR file ...**  
See 5.4 Restoring/Importing from PAR File, page 119 for details.

### 2.2.1.2 Other Context Menus

- **Collapse All**  
Closes all open nodes in the configuration tree down to the top level.
- **Lock / Unlock**  
Changes the status of the corresponding file from read-only to read-write (and vice versa) and thus makes it editable/static.
- **Create Server / Create Service**  
These menu items are only available when opening the context menu of the nodes  **Virtual Servers** or  **Assigned Services**.
- **Copy To Repository**  
Copies the selected configuration file to the corresponding repository section. This menu item will only be available if a repository has already been created.
- **Refresh From Here**  
Updates the view of the configuration tree from the selected position on downwards.
- **Show RCS Versions ...**  
This entry is only available in on the management centre box. It provides RCS (**R**evision **C**ontrol **S**ystem) information for the selected configuration files, including exact date/time and administrator's name/IP address with reference to the config modification made.
- **Show History ...**  
Displays a list with the config modification history since creation of the box.
- **Remember Position / Clear Position**  
This item allows you to save the current position in the configuration tree. On next start phion.a will open at the saved position.  
**Clear Position** removes the saved position.

## 2.2.2 Box Properties


The file **Box Properties** contains box specific configuration data (box name, description, ...). It is either created as part of the kickstart disk when installing a new system with phion.i (**Getting Started** - 2.2 Creating a "standard" Kickstart Disk, page 10, and then Step 3 Defining Box Type settings), or when creating a new box in the configuration tree of a management centre using Create Box ... from the context menu (**phion management centre** - 6.10.1.1 Create Box ..., page 424). Once created only few file contents may be changed retroactively.

The box config file is divided into two sections: **Identification Settings** and **Operational Settings** (available on MC-administered boxes only). The operational settings define information needed for interoperation between box and MC. The box config file has to be maintained for each box individually.





**Note:**  
On MC-administered boxes the box configuration should always be edited on the management centre and not on the box itself.

**Note:**

On an MC you can also use a wizard to create a box, see **phion management centre** - 6.6.1 Create Box Wizard, page 420.

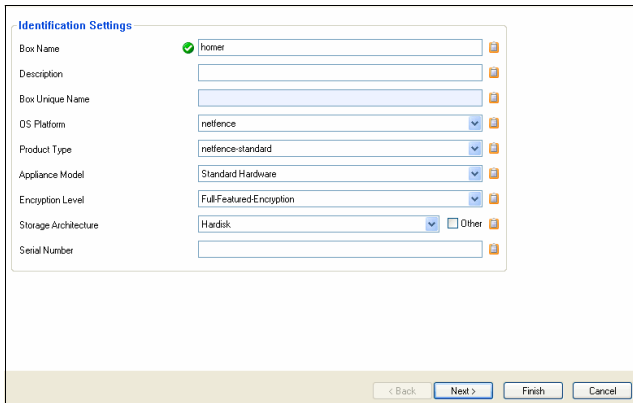
Open the box configuration by double-clicking  **Box Properties**.

**Note:**

To view configuration options of the read-only fields in the box config file browse to  **Multi-Range** >  <rangenam> >  <clusternam> >  **Boxes** on the MC and select **Create Box ...** from the context menu (figure 3-14). The Box Config itself is shown in figure 3-15.

### 2.2.2.1 Creating a Box - Identification Settings


Fig. 3-14 Creating a box on an MC



List 3-1 Box Config - section Identification Settings

Parameter	Description
<b>Box Name</b>	This is the name of the box as specified during box creation on the MC. The box name may differ from the box hostname (see <b>Hostname</b> , page 11). The maximum length of this parameter is 25 characters. Once defined, the box name may not be altered, thus this is a read-only field. The <b>Box Name</b> field is empty on self-managed netfence gateways and on the MC itself.
<b>Description</b>	This field takes optional additional information (no length limitation).
<b>Box Unique Name</b>	This is the name of the box that is used in the management unit. The content of this field is generated when the box is added to the configuration tree of the MC. The name is generated as follows: boxname_clusternam_rangenam. The <b>Box Unique Name</b> field is empty on self-managed netfence gateways and on the MC itself.
<b>OS Platform</b>	This setting specifies the OS platform the netfence gateway is installed on. Selection can be made between <b>netfence</b> and <b>crossbeam-X</b> . <b>Note:</b> Once created, this setting cannot be changed. The OS platform determines the values available through parameters <b>Product Type</b> and <b>Appliance Model</b> (see below). <b>Note:</b> On management centres this field is defined by the entry <b>Management-Centre</b> .
<b>Product Type</b>	Depending on the value specified for <b>OS Platform</b> , the available Product Type choice varies in this place. Each selection limits the view to compatible <b>Appliance Models</b> shown in the next field. <b>Note:</b> The <b>Product Type</b> corresponds with the field <b>Model</b> in phion.i ( <b>Getting Started</b> - 2.2 Creating a "standard" Kickstart Disk, page 10, and then Step 3 Defining Box Type settings).

List 3-1 Box Config - section Identification Settings

Parameter	Description
<b>Appliance Model</b>	Available appliance model types are dependent on the selection for the product type. In this place choose the appliance type, which matches the label of your appliance model. <b>Note:</b> The <b>Appliance Model</b> corresponds with the field <b>Appliance</b> in phion.i ( <b>Getting Started</b> - 2.2 Creating a "standard" Kickstart Disk, page 10, and then Step 3 Defining Box Type settings). <b>Note:</b> Each OS Platform, Product Type, and Appliance Model combination determines product specific default settings. It also determines availability of services and default settings of these services. To profit from this feature, correct settings already have to be configured, either when creating the box installation file with phion.i ( <b>Getting Started</b> - 2.2 Creating a "standard" Kickstart Disk, page 10, and then Step 3 Defining Box Type settings) or when creating the box on the MC. Have a look at <b>Getting Started</b> - 2.5 phion Multi-Platform Product Support, page 16 to find out about each type's typical characteristics.
<b>Encryption Level</b>	This setting determines the system's suitability for productional use. Unlicensed systems or systems with export-restricted licenses with weak encryption have to be set to <b>Export-Restricted-Encryption</b> . Licensed systems may be set to <b>Full-Featured-Encryption</b> . Have a look at table 1-2, page 11 for an overview of netfence demo versions. <b>Note:</b> <b>Export-Restricted-Encryption</b> will be set in this field if the checkbox <b>Demo or Export Mode</b> has been selected when defining box type settings with phion.i ( <b>Getting Started</b> - 2.2 Creating a "standard" Kickstart Disk, page 10).
<b>Storage Architecture</b>	This attribute allows for discrimination between <b>Harddisk</b> based and <b>Flash-RAM</b> (CF-Card) based boxes. The following properties are applicable for Flash-RAM based boxes: <ul style="list-style-type: none"> <li>➤ Harddisk size between 2 and 8 GB.</li> <li>➤ No SMART values</li> <li>➤ No DMA</li> </ul> <p>Note that when CF-based is selected additional configuration options become available within the  <b>System Settings</b> configuration node (see 5.1.1.5 Flash Memory, page 101). Misconfiguration of the storage architecture option triggers the event [70] <b>Flash RAM auto detection</b>. An error is reported when one of the following situations arises:</p> <ul style="list-style-type: none"> <li>➤ Flash-RAM has been configured but cannot be detected.</li> <li>➤ Flash-RAM has not been configured but is detected.</li> <li>➤ Flash-RAM has not been configured but hardware properties indicate that the box might possibly be a Flash-RAM based box.</li> </ul>
<b>Serial Number</b>	This field has informational character. For example it allows you to enter the hardware ID of the system. This field is only available on MC-administered boxes.

**Note:**

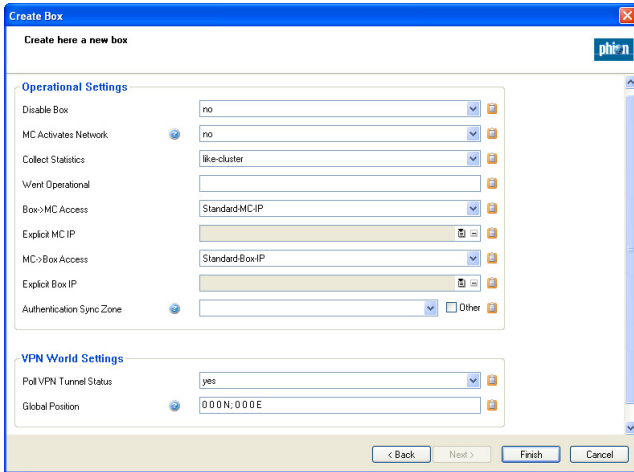
The configuration parameters **OS Platform**, **Product Type** and **Appliance Model** are designed to offer enhanced multi-platform product support. The types chosen determine specific default settings of the box and in some cases they determine, which services can be installed and configured. Have a look at **Getting Started** - 2.5 phion Multi-Platform Product Support, page 16 to find out about each type's typical characteristics.

### 2.2.2.2 Creating a Box - Operational Settings

**Note:**

The section **Operational Settings** is only available on MC-administered boxes.

Fig. 3-15 Box config file on an MC-administered box



List 3-2 Box Config - section Operational Settings

Parameter	Description
<b>Disable Box</b>	Ticking this checkbox deactivates the box on the MC. A deactivated box will no longer receive configuration updates. It will be displayed with a grey background in the status map of the MC. Nonetheless the box will still receive and commit events, it will transfer statistics, and it will further on be included in licensing and software updates.
<b>MC Activates Network Changes</b>	When set to <b>yes</b> (default: <b>no</b> ) the MC automatically triggers execution of a <b>failsafe</b> box network activation, when the network configuration of the box has been updated. Activating this attribute avoids manual box network activation on the box itself (2.6 Box Tab, <b>Section Network Configuration, page 38</b> ). The network activation is processed in the following way after <b>Send Changes</b> and <b>Activate</b> buttons have been executed: <ul style="list-style-type: none"> <li>➤ The system creates a backup file of the active network configuration.</li> <li>➤ It then temporarily activates the configuration changes and verifies that the management centre can still be contacted.</li> <li>➤ If this verification is successful the network is restarted so that the changes are activated permanently.</li> <li>➤ If verification fails, the original network configuration is restored.</li> </ul>
<b>Collect Statistics</b>	This attribute directs the MC how to collect statistics data from this box. Setting to <b>no</b> deactivates statistics collection. Setting to <b>yes</b> activates statistics collection. Setting to <b>like-cluster</b> inherits the configuration from the <b>Cluster Config</b> (see 6.5 Cluster Configuration <b>Collect Statistics</b> , page 418) file.
<b>Went Operational</b>	This field has informational character and allows you to enter the date when the system went into operational status.

List 3-2 Box Config - section Operational Settings

Parameter	Description
<b>Box-&gt;MC Access</b>	Here the MC IP address is defined which is used by the box for fetching licenses, sending events / status information, ... The available options are: <b>Standard-MC-IP</b> - first server IP of the MC is used <b>Explicit-MC-IP</b> - an alternative server IP of the MC is used (activates parameter <b>Explicit MC IP</b> , see below).
<b>Explicit MC IP</b>	This parameter is only available with parameter <b>Box-&gt;MC Access</b> set to <b>Explicit-MC-IP</b> and is used for defining the alternative MC server IP address.
<b>MC-&gt;Box Access</b>	Here the box IP address is defined, which is used by the MC for sending configuration updates, committing events, software updates, ... The available options are: <b>Standard-BOX-IP</b> - main box IP / virtual box IP (if configured) is used <b>Explicit-BOX-IP</b> - an alternative management IP is used (for example further network management IP, activates parameter <b>Explicit Box IP</b> , see below).
<b>Explicit Box IP</b>	This parameter is only available with parameter <b>MC-&gt;Box Access</b> set to <b>Explicit-BOX-IP</b> and is used for defining the alternative management IP address.
<b>Authentication Sync Zone</b>	Select one of the synchronisation zones to add the box to a named zone. This effectuates authentication information to be synced to all other boxes belonging to the same zone. Also, authentication information from all other boxes of the zone are synced to this box. The selection contains all existing entegra trustzones as well as all so called <b>Non-Policy-Trustzones</b> . It is not required to configure this on a box where a policy service is running: a policy service is adding the box to the corresponding authentication sync zone automatically. This configuration option is used to add a box on which no policy service is running, but authentication information (gathered on a different box) should be used with the firewall configuration to the sync zone. Furthermore, it enables firewall authentication synchronisation without running a policy service.

List 3-3 Box Config - section VPN World Settings

Parameter	Description
<b>Poll VPN Tunnel Status</b>	Choose <b>yes</b> or <b>no</b>
<b>Global Position</b>	Enter the global position of the box: The global position for new box by default is 0 0 0 N; 0 0 0 E.

### 2.2.3 Administrative Settings

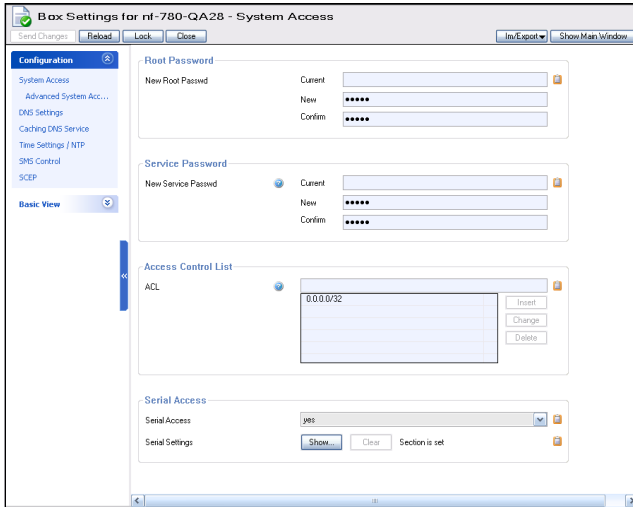
The configuration file **Administrative Settings** contains information relevant for proper operation of a phion system as the one contained in file **Network**.

Its nature is, however, such that per se it does not necessarily contain data specific to the exact location of a box within the network. Thus a single instance of this file may be shared amongst a number of boxes.

Open the network configuration by double-clicking the **Administrative Settings** node.

### 2.2.3.1 System Access

Fig. 3-16 Administrative Settings - System Access



List 3-4 Administrative Settings - System Access - section Root Password

Parameter	Description
<b>New Root Passwd</b>	The root password of the phion subsystem and the Linux OS. Passwords with less than 5 characters are not permitted.

List 3-5 Administrative Settings - System Access - section Service Password

Parameter	Description
<b>New Service Password</b>	The password of an unprivileged Linux OS user with name <b>phion</b> . <b>Note:</b> Passwords with less than 5 characters are not permitted.

List 3-6 Administrative Settings - System Access - section Access Control List

Parameter	Description
<b>ACL</b>	Access control list to protect the box from denial of service (DOS) attacks. Array of IP/mask pairs for which exclusive access to the administrative IP addresses of the box at TCP port 22 (secure shell) and TCP ports 800-820 is granted. TCP based access from all other addresses to these port/address combinations is administratively prohibited. By default, access is allowed from an arbitrary address. <b>Attention:</b> To avoid unnecessary exposure of your phion system to DOS attacks against administrative addresses you should restrict the scope of the ACL to the set of IP addresses from which administrative access is required. <b>Attention:</b> Changing the access control list does not terminate already established sessions. Manually terminate active sessions within the Firewall Active tab to enforce ACL changes.

List 3-7 Administrative Settings - System Access- section Serial Access

Parameter	Description
<b>Serial Access / Serial Settings</b>	Click the <b>Edit ...</b> button to enter the configuration dialogue.
<b>Access Types</b>	<b>ConsoleOnly (COM1)</b> This setting enables box access using a terminal emulation program such as hyperterm via a the serial interface COM1 (terminal emulation: ansi; baud rate: 19200). <b>Note:</b> The parameters <b>Mgmt COM Port</b> and <b>Mgmt Baud Rate</b> are inactive when this option is set.

List 3-7 Administrative Settings - System Access- section Serial Access

Parameter	Description
<b>Management Only</b>	With this setting the box can be accessed with the phion.a GUI via COM1 (therefore <b>Mgmt COM Port</b> is inactive; default <b>Mgmt Baud Rate</b> : 57600).
<b>Console(COM1) And Management</b>	This option combines the two above (default <b>Mgmt COM Port</b> : COM1; default <b>Mgmt Baud Rate</b> : 57600).
<b>Mgmt COM Port</b>	This option defines the serial port that is to be used.
<b>Mgmt Baud Rate</b>	With this setting the Baud Rate is defined.

### 2.2.3.2 Advanced System Access

**Note:**

This parameter group is only available in **Advanced View** mode.

List 3-8 Administrative Settings - section Advanced Access Settings

Parameter	Description
<b>Authentication Mode</b>	Choose from <b>Key-OR-Password</b> , <b>Password</b> , <b>Key</b> or <b>Key-AND-Password</b> . Note that the usage of keys should always be favoured over usage of passwords, as no security relevant information needs to be exchanged when authentication takes place via public-key cryptography (challenge-response approach).
<b>Root Public RSA Key</b>	Allows you to import a public RSA key from a file or the clipboard. With an appropriate authentication mode the phion box will authenticate an admin via public key cryptography. As a necessary prerequisite phion.a needs to have loaded the matching private RSA key. <b>Note:</b> For security reasons you should not use unencrypted private keys. <b>Note:</b> The root public RSA key is only applicable for controlled phion.a logins. If a key for automated SSH login is required use the <b>Authorized Root Keys</b> option instead (see below).
<b>Root Aliases</b>	<b>Note:</b> Root Aliases are only available on MC-administered boxes. On single boxes multiple administrator roles may be created in <b>Admins</b> (accessible via <b>Config &gt; Box</b> , see 2.2.7 Administrators, page 91). Click the <b>Insert</b> button to insert a new root alias name. <b>Inactive</b> A newly introduced root alias is ready for use immediately after creation (default setting: <b>no</b> ). Set to <b>yes</b> to disable its login temporarily. <b>Authentication Mode/Password/Public RSA Key</b> These values specify the root aliases' authentication mode. See the same named parameters above for further information.



**List 3-8** Administrative Settings - section Advanced Access Settings

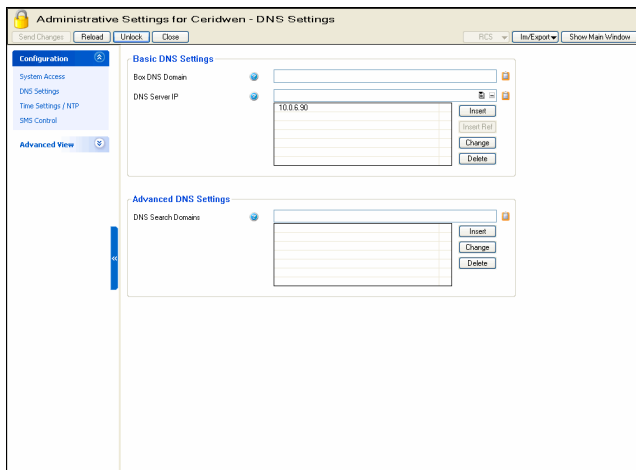
Parameter	Description
<b>Authorized Root Keys</b>	<p>The <b>Authorized Root Keys</b> field may be used to insert public keys assigned to user root in OpenSSH format. Public keys apply for key-based authentication using SSH and can be employed, for example to enable automated key based SSH logins for backup creation reasons, ...</p> <p>The inserted string is appended to the <code>authorized_keys2</code> file assigned to user root, thus permitting login with an OpenSSH Client disposing of the corresponding private key. Details on OpenSSH Client configuration are available at <a href="http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/sl-openssh-client-config.html">http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/sl-openssh-client-config.html</a>.</p> <p><b>Note:</b> Insert multiple keys one per line.</p> <p>Public keys available in another than SSH format may be converted using the <code>ssh-keygen</code> utility (refer to <code>man ssh-keygen</code> for details). On UNIX systems, the user's public keys are usually written to <code>~/.ssh/id_rsa.pub</code> (for RSA based keys) or <code>~/.ssh/id_dsa.pub</code> (for DSA based keys).</p> <p><b>Note:</b> The <b>Authorized Root Keys</b> option is only required for automated logins by user root. Key-based SSH login option (controlled and automated) for non-root users is configurable in the following places:</p> <ul style="list-style-type: none"> <li>➤ <b>On single boxes</b> ➤ <b>Config</b> &gt; <b>Box</b> &gt; <b>Administrators</b> &gt; <b>Public RSA Key</b> (see 2.2.7 Administrators, page 91)</li> <li>➤ <b>On MC-administered boxes</b> ➤ <b>Admins</b> &gt; <b>Details</b> tab &gt; <b>Public Key (phion management centre - 8.3 Admin User Interface, page 433)</b></li> </ul>

**List 3-10** Administrative Settings - DNS - section Advanced DNS Settings

Parameter	Description
<b>DNS Search Domains</b>	Names of those domains, which should automatically be appended to an alias name when performing a DNS query. Separate multiple domains with spaces.
<b>DNS Query Rotation</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>When multiple DNS servers are used, this parameter defines whether DNS queries should regularly rotate between them. Set to <b>yes</b> (default: <b>no</b>) to activate rotation.</p>
<b>DNS Query Timeout</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Defines the timeout [sec] for DNS queries. When the timeout exceeds the specified value, the next DNS server is queried.</p>
<b>Known Hosts (Host Name/Host IP/Full Name/Aliases)</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Use this section to add user-defined entries to the system's file <code>/etc/hosts</code>. This file will by default always be consulted first for name resolution. It is useful to specify address/name pairs of locally known hosts here, for which no name resolution via DNS is available. The name specified in the first column <b>Name</b> of this section will as well be used as alias.</p> <p>To open the <b>Known Hosts</b> configuration window click <b>Insert</b>.</p> <p>As the bare minimum you will have to supply the <b>Host IP</b> address. This address is associated with the name of the section instance. Optionally, you may specify a fully qualified domain name (dots as name space delimiter) and a whole list of additional <b>Aliases</b> (no dots).</p>

### 2.2.3.3 DNS

**Fig. 3-17** Administrative Settings - DNS



**List 3-9** Administrative Settings - DNS - section Basic DNS Settings

Parameter	Description
<b>Box DNS Domain</b>	Name of the DNS domain the box belongs to. You may only specify a single domain. The length of the domain's name is limited to 46 characters.
<b>DNS Server IP</b>	<p>List of DNS server IP addresses serving the domain specified above.</p> <p><b>Note:</b> Both, <b>Box DNS Domain</b> and <b>DNS Server IP</b>, have to be set when using a proxy service. Otherwise the proxy service cannot start.</p> <p>The resolver system layer does not monitor the <code>/etc/resolv.conf</code> file. Thus, services using this layer (in contrast to services using the phion resolver) will not recognise changed DNS server settings automatically. Examples for services using the resolver layer are a number of phibs authenticators, proxy, snmp and dhcprelay. Therefore, when changing <b>DNS Server IP</b> settings phion services should be restarted manually. Do so by clicking the <b>phion Restart</b> button (see <b>phion Restart</b>, page 39).</p>

### 2.2.3.4 Caching DNS Service

**Note:**  
This parameter group is only available in **Advanced View** mode.

**List 3-11** Administrative Settings - Caching DNS Service - section Advanced DNS Settings

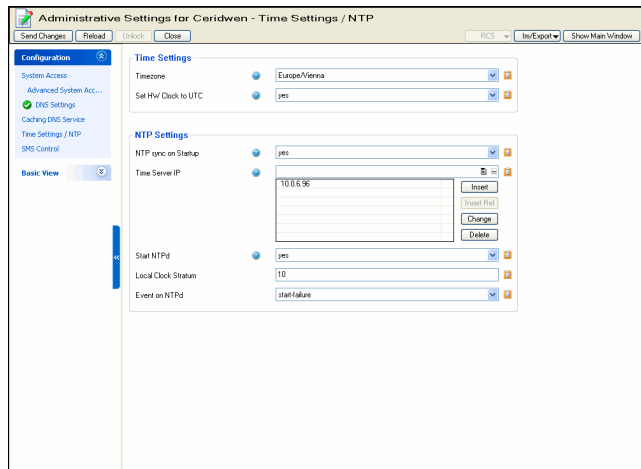
Parameter	Description
<b>Run Forwarding / Caching DNS</b>	<p>This parameter activates/deactivates a local caching or forwarding DNS service (default <b>no</b> = deactivated). DNS queries will be forwarded to or cached from the servers specified under <b>DNS Server IP</b>. Setting to <b>yes</b> activates the field <b>Log DNS Queries</b> (see below).</p> <p><b>Attention:</b> Forwarding/Caching DNS (bdns) configuration collides with a running DNS Server (<b>DNS - 2. Installation, page 316</b>). The <code>bdns</code> service must run exclusively. Do NOT install both services.</p>
<b>Run Slave DNS</b>	This parameter activates/deactivates a local Slave DNS service (default <b>no</b> = deactivated). Setting to <b>yes</b> activates the fields <b>Default Master DNS</b> and <b>DNS Slave Zones</b> (see below). The slave DNS service obtains its slave zone configuration from the entries specified through <b>DNS Slave Zones</b> field and additionally fetches further zone configuration files from the servers specified in the <b>Default Master DNS</b> field.
<b>Query Source Address</b>	<p>This parameter allows to specify which IP address to use as source address when querying the DNS or Master DNS server(s). The following settings are possible:</p> <ul style="list-style-type: none"> <li>➤ <b>Wildcard</b> (default) - IP selection is accounted for dynamically according to definitions in the routing table.</li> <li>➤ <b>VIP</b> (on MC administered boxes only) - Uses the system's <b>Virtual Management IP</b>.</li> <li>➤ <b>MIP</b> - Uses the system's management IP, which is the <b>Main Box IP</b>.</li> <li>➤ Select checkbox <b>Other</b> to specify an IP address explicitly.</li> </ul>

**List 3-11** Administrative Settings - Caching DNS Service - section Advanced DNS Settings

Parameter	Description												
<b>DNS Query ACL</b>	Here single IP addresses or netmasks can be defined that may access the DNS service via a local redirect firewall rule. <b>Note:</b> Do not forget to create this rule in the Forwarding Firewall Rule set.												
<b>Log DNS Queries</b>	If this parameter is set to <b>yes</b> (default: <b>no</b> ) every DNS query will be logged.												
<b>Default Master DNS</b>	This parameter takes a single or a list of DNS servers, the local slave DNS service queries for zone files.												
<b>DNS Slave Zones</b>	Click the <b>Insert ...</b> button to create a new slave zone entry. Enter the fully qualified domain name of the zone into the <b>Name</b> field of the newly opened <b>DNS Slave Zone</b> window. The following parameters are then available for configuration: <table border="1" data-bbox="204 667 686 1628"> <tbody> <tr> <td><b>Active Zone</b></td> <td>A newly created zone is active by default (setting: <b>yes</b>). The configuration can be deactivated temporarily by setting the parameter value to <b>no</b>.</td> </tr> <tr> <td><b>Zone Type</b></td> <td>This value determines the DNS zone type (<b>Forward</b> (default), <b>Reverse</b> or <b>Both</b>). Setting to <b>Reverse</b> or <b>both</b> activates the fields <b>Reverse Lookup Net</b> and <b>Reverse Lookup Netmask</b> below.</td> </tr> <tr> <td><b>DNS Master IP</b></td> <td>This parameter takes a single or a list of DNS servers, which the local slave DNS service queries for this zone. If specified, this setting overrides the globally defined DNS Master IP. If left empty, the field is ignored.</td> </tr> <tr> <td><b>Reverse Lookup Net</b></td> <td>These fields define network and netmask the specified zone resides in.</td> </tr> <tr> <td><b>Reverse Lookup Netmask</b></td> <td></td> </tr> <tr> <td><b>Transfer Source Address</b></td> <td>This parameter allows specifying which IP address to use as source address when querying the Master DNS server(s), thus overriding the globally defined value. The following settings are possible:               <ul style="list-style-type: none"> <li>➤ <b>Wildcard</b> (default) - IP selection is accounted for dynamically according to definitions in the routing table.</li> <li>➤ <b>Query Source</b> - This setting uses the IP address of the client initiating the query.</li> <li>➤ <b>VIP</b> (on MC administered boxes only) - Uses the system's <b>Virtual Management IP</b>.</li> <li>➤ <b>MIP</b> - Uses the system's management IP (<b>Main Box IP</b>).</li> <li>➤ Select checkbox <b>Other</b> to specify an IP address explicitly.</li> </ul> </td> </tr> </tbody> </table>	<b>Active Zone</b>	A newly created zone is active by default (setting: <b>yes</b> ). The configuration can be deactivated temporarily by setting the parameter value to <b>no</b> .	<b>Zone Type</b>	This value determines the DNS zone type ( <b>Forward</b> (default), <b>Reverse</b> or <b>Both</b> ). Setting to <b>Reverse</b> or <b>both</b> activates the fields <b>Reverse Lookup Net</b> and <b>Reverse Lookup Netmask</b> below.	<b>DNS Master IP</b>	This parameter takes a single or a list of DNS servers, which the local slave DNS service queries for this zone. If specified, this setting overrides the globally defined DNS Master IP. If left empty, the field is ignored.	<b>Reverse Lookup Net</b>	These fields define network and netmask the specified zone resides in.	<b>Reverse Lookup Netmask</b>		<b>Transfer Source Address</b>	This parameter allows specifying which IP address to use as source address when querying the Master DNS server(s), thus overriding the globally defined value. The following settings are possible: <ul style="list-style-type: none"> <li>➤ <b>Wildcard</b> (default) - IP selection is accounted for dynamically according to definitions in the routing table.</li> <li>➤ <b>Query Source</b> - This setting uses the IP address of the client initiating the query.</li> <li>➤ <b>VIP</b> (on MC administered boxes only) - Uses the system's <b>Virtual Management IP</b>.</li> <li>➤ <b>MIP</b> - Uses the system's management IP (<b>Main Box IP</b>).</li> <li>➤ Select checkbox <b>Other</b> to specify an IP address explicitly.</li> </ul>
<b>Active Zone</b>	A newly created zone is active by default (setting: <b>yes</b> ). The configuration can be deactivated temporarily by setting the parameter value to <b>no</b> .												
<b>Zone Type</b>	This value determines the DNS zone type ( <b>Forward</b> (default), <b>Reverse</b> or <b>Both</b> ). Setting to <b>Reverse</b> or <b>both</b> activates the fields <b>Reverse Lookup Net</b> and <b>Reverse Lookup Netmask</b> below.												
<b>DNS Master IP</b>	This parameter takes a single or a list of DNS servers, which the local slave DNS service queries for this zone. If specified, this setting overrides the globally defined DNS Master IP. If left empty, the field is ignored.												
<b>Reverse Lookup Net</b>	These fields define network and netmask the specified zone resides in.												
<b>Reverse Lookup Netmask</b>													
<b>Transfer Source Address</b>	This parameter allows specifying which IP address to use as source address when querying the Master DNS server(s), thus overriding the globally defined value. The following settings are possible: <ul style="list-style-type: none"> <li>➤ <b>Wildcard</b> (default) - IP selection is accounted for dynamically according to definitions in the routing table.</li> <li>➤ <b>Query Source</b> - This setting uses the IP address of the client initiating the query.</li> <li>➤ <b>VIP</b> (on MC administered boxes only) - Uses the system's <b>Virtual Management IP</b>.</li> <li>➤ <b>MIP</b> - Uses the system's management IP (<b>Main Box IP</b>).</li> <li>➤ Select checkbox <b>Other</b> to specify an IP address explicitly.</li> </ul>												

## 2.2.3.5 TIME/NTP Tab

**Fig. 3-18** Administrative Settings - TIME/NTP



**List 3-12** Administrative Settings - TIME/NTPs - section Time Settings

Parameter	Description
<b>Timezone</b>	Select the desired time zone for your phion system. Note that changing the time zone later on is a rather momentous measure as far as its implications for data accounting, logging, and eventing are concerned. <b>Note:</b> Time zones available for configuration in the pull-down menu are stated in POSIX compliant style according to their derivation from a UNIX system. This means that in Etc/GMT time zones, hours preceded by a minus (-) are counted to the east of the Prime Meridian, and hours preceded by a plus (+) are counted to the west of the Prime Meridian. Conversion to daylight saving time (DST) is not considered in Etc/GMT time zones. To do so, time settings in Country/City format have to be used. Accordingly, Etc/GMT-1 (GMT+1 without the preceding Etc on Microsoft Windows operating systems) specifies the time zone 1 hour to the east of Greenwich Mean Time without, and Europe/Berlin specifies the same time zone with consideration of DST conversion. <b>Note:</b> Please consider that daylight saving times are an unreliable factor in cross-national networks. If you are administering multiple systems situated in different time zones with an optional phion management centre, switching to UTC uniformly is recommended.
<b>Set HW Clock to UTC</b>	Choose <b>yes</b> to set the hardware clock (aka CMOS or BIOS clock) to UTC (Universal Time, Coordinated) (default: <b>no</b> ). Reference time will be your system time. Running the hardware clock with UTC will immunise your system against unexpected time lapses caused by changes from or to daylight saving time (DST). We recommend to use this feature in combination with a prior synchronisation to an external reference clock (time server), as explained below.

**List 3-13** Administrative Settings - TIME/NTPs - section NTP Settings

Parameter	Description
<b>NTP sync on Startup</b>	If set to <b>yes</b> the box will try to obtain the correct time from an external reference clock whenever the network is restarted. <b>Note:</b> Continuous time synchronisation may be achieved by running an NTP daemon on the system. The box will use its primary box IP as source address when contacting a time server. Consequently, a phion system placed at the border of your network will typically contact a time server belonging to the protected LAN side. Event-IDs 2080/2081/2082 may be generated in conjunction with parameter <b>Start NTPd</b> set to <b>yes</b> ( <b>System Information</b> - 5. List of Default Events, page 516). <b>Note:</b> Every synchronisation attempt with a time server will be brought to your attention by eventing in NTPd has been started. This is due to the fact that we consider maintaining an appropriate time standard on the system as a prerequisite for reliable system operation.



List 3-13 Administrative Settings - TIME/NTPs - section NTP Settings

Parameter	Description
<b>Time Server IP</b>	<p>Array of IP addresses of NTP protocol conform time servers.</p> <p>Try to specify as many independent server addresses as possible. These addresses will be contacted in turn during every restart of the network subsystem for the purpose of time synchronisation. The first successful synchronisation will suppress further synchronisation attempts until the next restart occurs. For continuous synchronisation you must run an NTP daemon on your system (see comment below) or run ntpdate from a cronjob every so often.</p> <p>Note that the latter approach may incur backward time glitches causing the log and statistics daemons to complain about clock skews.</p> <p><b>Note:</b> On a firewall system you may not bind to 0.0.0.0 and will have to specify the source address to be used by ntpdate. You may do so by making use of the phion-added flag -A &lt;IP&gt;. Note that the network consistency check logic will also check whether or not these addresses are reachable (routes available) from the box with the box management IP as source address. If you run the system as a remote box (administration via a tunnel to a management instance) then the source address is the so-called virtual IP (VIP) instead.</p> <p><b>Note:</b> If available phion recommends using the management centre as time server.</p>
<b>Start NTPd</b>	<p>If set to <b>yes</b> the system will continuously aim for keeping its time in sync with the external references specified above in order to improve the reliability of your time standard. Note that the trade-off here is increased UDP traffic from the box to those IPs. Your phion system in turn also becomes an NTP time server that may be queried by clients on your LAN. The addresses under which this service is made available are the administrative IPs at UDP port 123.</p> <p><b>Attention:</b> Be aware that running an NTP daemon on your phion system makes the system vulnerable to NTP specific exploits and UDP based denial of service attacks. Never direct your phion system to not trusted reference time servers or run a time server in a completely hostile environment.</p>
<b>Local Clock Stratum</b>	<p>This setting configures the stratum value of the local clock for the NTP daemon. The time reference has a fixed stratum value <b>n</b> and each subsequent computer in the NTP chain has a stratum value <b>n+1</b>. The preconfigured default value <b>10</b> should be set to <b>9</b> on the MC box to make clear that the MC box is the preferred source.</p>
<b>Event on NTPd</b>	<p>Only relevant when <b>Start NTPd</b> is set to <b>yes</b>. You may configure the NTPD related conditions that trigger event notification (Event-IDs 2070-2073). You may choose from 4 different settings:</p> <ul style="list-style-type: none"> <li>➤ <b>start-failure</b> (default)</li> <li>➤ <b>+stop-failure</b></li> <li>➤ <b>++start-success</b></li> <li>➤ <b>+++stop-success</b></li> </ul> <p>The list is additive, which means items further down the list automatically include all previous ones. Events will as well be triggered when the NTP daemon is restarted via the <b>Control&gt; Box</b> tab in (<b>Control Centre</b> - 2.6 Box Tab, page 38):</p> <ul style="list-style-type: none"> <li>➤ <b>Restart NTP</b> button In this scenario the control daemon induces NTPd to restart.</li> <li>➤ <b>Sync</b> button Synchronisation processes are triggered through the script <code>ctrltime</code>. <code>ctrltime</code> stops NTPd and then executes <code>ntpdate</code> on port 123.</li> </ul> <p><b>Note:</b> You will not be notified when NTPd is killed manually or just dies unexpectedly. The settings here only pertain to NTPd behaviour during controlled start or stop sequences.</p>

### 2.2.3.6 A small Digression into Linux Time Management

(excerpted from "Linux-Clock HOWTO", v2.1, Nov. 2000 by Ron Bean)

The Linux "system clock" actually just counts the number of seconds past Jan. 1, 1970, and is always in UTC. UTC does not change as DST (**Daylight Savings Time**) comes and goes - what changes is the conversion between UTC and local time. The translation to local time is done by library functions that are linked into the application programs.

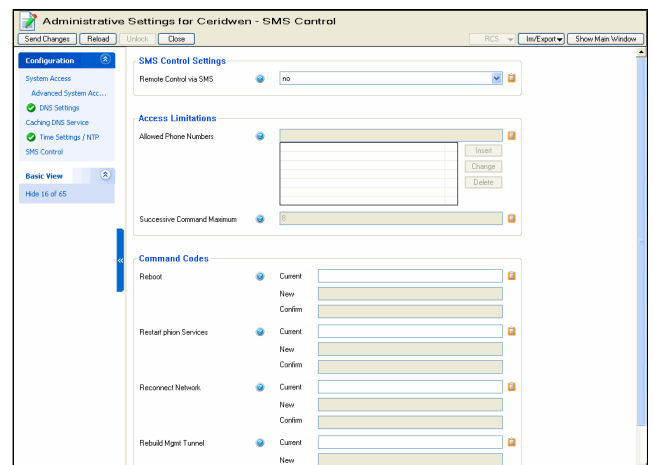
This has two consequences: First, any application that needs to know the local time also needs to know what time zone you're in, and whether DST is in effect or not. Second, there is no provision in the kernel to change either the system clock or the RTC (real time clock) as DST comes and goes, because UTC doesn't change. Therefore, machines that only run Linux should have the RTC set to UTC, not local time. Unfortunately, there are no flags in the RTC or the CMOS RAM to indicate standard time vs. DST. This means that, if the RTC has been set to local time, the system must assume that the RTC always contains the correct local time.

If Linux is running when the seasonal time change occurs, the system clock is unaffected and applications will make the correct conversion. But if Linux has to be rebooted for any reason, the system clock will be set to the time in the RTC, which might be off by up to an hour since DST information is not stored in the RTC or CMOS RAM.

Some other documents have stated that setting the RTC to UTC allows Linux to take care of DST properly. This is not really wrong, but it doesn't tell the whole story - as long as you don't reboot, it does not matter which time is in the RTC (or even if the RTC's battery dies). Linux will maintain the correct time either way, until the next reboot. In theory, if you only reboot once a year (which is not unreasonable for Linux), DST could come and go and you'd never notice that the RTC had been wrong for several months, because the system clock would have stayed correct all along. But since you can't predict when you'll want to reboot, it's better to have the RTC set to UTC if you're not running another OS that requires local time.

### 2.2.3.7 SMS Control

Fig. 3-19 Administrative Settings - SMS Control



For gateways that have been equipped with the UMTS extension and a UMTS modem card that is compatible with the adopted SMS implementation (see *Inbound SMS Handling*, page 76) remote execution of four restorative maintenance tasks is possible.

Use the SMS Control Settings to define how to deal with inbound SMS triggering command execution.

**List 3-14** Administrative Settings - SMS Control - section SMS Control Settings

Parameter	Description
<b>Remote Control via SMS</b>	<p>Set this to <b>yes</b> (default: <b>no</b>) to allow for SMS triggered command execution. This feature will only work if an appropriate GSM/UMTS card supporting it is installed. The following events are associated to this feature when it is activated:</p> <ul style="list-style-type: none"> <li>➤ [135] <b>Resource Limit Pending</b> Less than 50 % of maximum command value remain.</li> <li>➤ [136] <b>Resource Limit Exceeded</b> The maximum command counter has been reached or has been exceeded.</li> <li>➤ [4111] <b>Authentication Failure Warning</b> The ACL does not match.</li> <li>➤ [4112] <b>Authentication Failure Alert</b> Password authentication failure and/or unsuccessful command match.</li> <li>➤ [4126] <b>Remote Command Execution Alert</b> Successful authentication and command is accepted.</li> </ul>

**List 3-15** Administrative Settings - SMS Control - section Access Limitations

Parameter	Description
<b>Allowed Phone Numbers</b>	Access is controlled via a mandatory phone ACL, which matches either sender number or in its absence SMSC number. Insert the numbers, which are allowed to trigger command execution with SMS into the list. Include country prefixes in the phone number omitting leading zeros and plus sign.
<b>Successive Command Maximum</b>	This setting limits the maximum number of successive commands that the interface will accept (default: <b>0</b> ). Note that once this limit has been reached the counter needs to be reset manually by the super user via SSH access or remote command execution from an MC (file <code>/var/phion/preserve/bsms/cmdcter</code> needs to be reset to a value of <b>0</b> ).

**List 3-16** Administrative Settings - SMS Control - section Command Codes

Parameter	Description
	<p>The four commands listed below can be triggered remotely by SMS. Each command is associated with a password. Insert the password into the field right of the the parameter label and retype it in the <b>Confirm</b> field. The commands are only accepted when the sender ACL matches, the maximum successive command counter has not yet been reached, and both, keyword and password match. Simply send an SMS to your interface with a single line containing space separated keyword and associated password. The system will always attempt to send a confirmation SMS.</p> <p><b>Note:</b> The keyword needs to start with a lower case letter.</p>
<b>Reboot</b>	Send <b>reboot</b> in a SMS followed by this string to enforce a box reboot.
<b>Restart phion Services</b>	Send <b>restart</b> in a SMS followed by this string to enforce a restart of the phion subsystem.
<b>Reconnect Network</b>	Send <b>reconnect</b> in a SMS followed by this string to enforce a restart of the network subsystem.
<b>Rebuild Mgmt Tunnel</b>	Send <b>rebuild</b> in a SMS followed by this string to enforce a restart of the MGMT tunnel.

## 2.2.3.8 SCEP

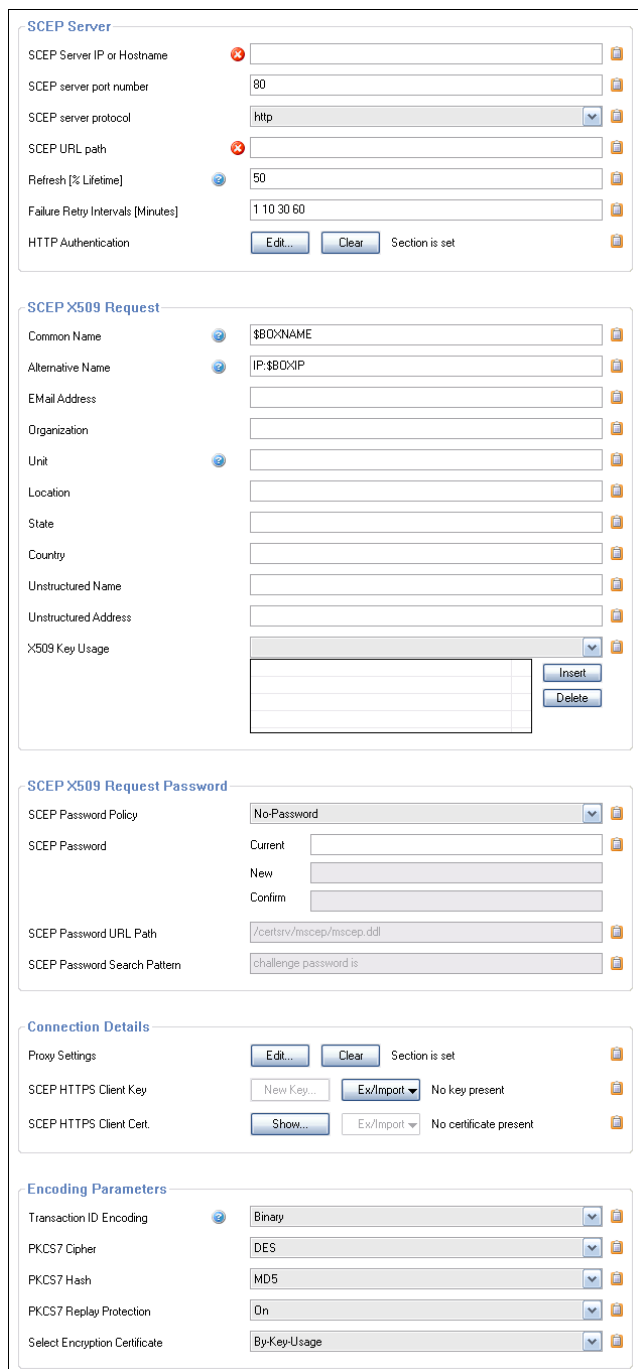
### Note:

See **Appendix - 1.3** How to set up for SCEP, page 526 for more detailed information.

**List 3-17** Administrative Settings - SCEP - section BOX SCEP Settings

Parameter	Description
<b>Enable SCEP</b>	Setting to <b>yes</b> (default: <b>no</b> ) activates SCEP and enables the corresponding configuration parameters below.
<b>SCEP Settings</b>	Choose <b>Set...</b> or <b>Edit...</b> to set the SCEP parameters.

**Fig. 3-20** Administrative Settings - SCEP



The screenshot displays the SCEP configuration interface, organized into several sections:

- SCEP Server:** Includes fields for SCEP Server IP or Hostname, SCEP server port number (90), SCEP server protocol (http), SCEP URL path, Refresh [% Lifetime] (50), Failure Retry Intervals (Minutes) (1 10 30 60), and HTTP Authentication (Edit... Clear Section is set).
- SCEP X509 Request:** Includes fields for Common Name (\$BOXNAME), Alternative Name (IP:\$BOXIP), EMail Address, Organization, Unit, Location, State, Country, Unstructured Name, Unstructured Address, and X509 Key Usage (Insert Delete).
- SCEP X509 Request Password:** Includes SCEP Password Policy (No-Password), SCEP Password (Current, New, Confirm), SCEP Password URL Path (/certsrv/mscep/mscep.dll), and SCEP Password Search Pattern (challenge password is).
- Connection Details:** Includes Proxy Settings (Edit... Clear Section is set), SCEP HTTPS Client Key (New Key... Ex/Import No key present), and SCEP HTTPS Client Cert. (Show... Ex/Import No certificate present).
- Encoding Parameters:** Includes Transaction ID Encoding (Binary), PKCS7 Cipher (DES), PKCS7 Hash (MD5), PKCS7 Replay Protection (On), and Select Encryption Certificate (By-Key-Usage).

**List 3-18** Administrative Settings - SCEP - SCEP Settings - section SCEP Server

Parameter	Description
<b>SCEP Server IP or Hostname</b>	The IP address or hostname of the SCEP server where the SCEP requests will be sent to. If a DNS hostname is used, make sure the DNS resolver of the gateway has been configured and is able to resolve it.
<b>SCEP server port number</b>	The TCP port number where the SCEP server listens to requests. The default value is 80, which generally suites for the HTTP protocol (see below).
<b>SCEP server protocol</b>	Choose between <i>http</i> or <i>https</i>
<b>SCEP URL path</b>	The complete URL path on the SCEP server which must be used to send the requests.
<b>Refresh [% Lifetime]</b>	The certificate will be refreshed after this percent of the certificate lifetime is reached (between 10 % and 90 %).
<b>Failure Retry Intervals [Minutes]</b>	The number of minutes to wait until the next retry.
<b>HTTP Authentication</b>	Choose <i>Set...</i> or <i>Edit...</i> to set the HTTP authentication. Parameter description see list 3-19.

**List 3-19** Administrative Settings - SCEP - SCEP Settings - section SCEP Server - section SCEP HTTP Server Authentication

Parameter	Description
<b>Authentication Type</b>	Choose between <ul style="list-style-type: none"> <li>➤ <i>None</i></li> <li>➤ <i>Basic-Authentication</i></li> <li>➤ <i>NTLM-Authentication</i></li> </ul>
<b>User Name</b>	Defines the user's name.
<b>Password</b>	Enter the (new) password and confirm it by re-entering into the confirm field (existing entries require the current password to unlock the fields <i>Password</i> and <i>Confirm</i> ).
<b>Domain</b>	Set the domain

**List 3-20** Administrative Settings - SCEP - SCEP Settings - section SCEP X509 Request

Parameter	Description
<b>Common Name</b>	The common name of the certificate. Default is <b>\$BOXNAME</b> . This value will be replaced with the real hostname of the box when the request is created.
<b>Alternative Name</b>	The alternative name of the certificate. Default is <b>IP:\$BOXIP</b> . This value will be replaced with the real IP address of the box when the request is created.
<b>E-Mail Address Organization</b>	Optional additional X.509 fields to include into the certificate request.
<b>Unit</b>	
<b>Location</b>	
<b>State</b>	
<b>Country</b>	
<b>Unstructured Name</b>	
<b>Unstructured Address</b>	
<b>X509 Key Usage</b>	Specific key usage. Leave empty for general purpose key usage. Key pairs may be intended for particular purposes, such as encryption only, or signing only. The usage of any associated certificate can be restricted by adding key usage and extended key usage attributes to the PKCS#10.

**List 3-21** Administrative Settings - SCEP - SCEP Settings - section SCEP X509 Request Password

Parameter	Description
<b>SCEP Password Policy</b>	<ul style="list-style-type: none"> <li>➤ <b>No-Password</b> No challenge password will be included in the certificate request.</li> <li>➤ <b>Password-from-Configuration</b> The challenge password is statically configured on the MC and will be included in the certificate request.</li> <li>➤ <b>Enter-Password-at-Box</b> The challenge password will be prompted at the box when the certificate request is created.</li> <li>➤ <b>Get-Password-From-Website</b> The challenge password is fetched from a web site (typically the CA itself)</li> </ul>
<b>SCEP Password</b>	Static challenge password, needed when the SCEP password policy option is set to <b>Password-from-Configuration</b> .
<b>SCEP Password URL Path</b>	The path and text to look for on the CAs website when the SCEP password policy option is set to <b>Get-Password-From-Website</b> .
<b>SCEP Password Search Pattern</b>	

**List 3-22** Administrative Settings - SCEP - SCEP Settings - section Connection Details

Parameter	Description
<b>Proxy Settings</b>	Choose <i>Set...</i> or <i>Edit...</i> to enter the configuration. Parameter description see table 3-23.
<b>SCEP HTTPS Client Key</b>	Click <i>Ex/Import</i> to import a key
<b>SCEP HTTPS Client Cert.</b>	Click <i>Show...</i> to view the certificate or click <i>Ex/Import</i> to import a certificate.

**List 3-23** Administrative Settings - SCEP - SCEP Settings - section Connection Details - section SCEP HTTP Proxy Settings

Parameter	Description
<b>Proxy IP Address</b>	The IP address of the proxy server.
<b>Proxy Port Number</b>	The TCP port number on which the proxy server listens for requests.
<b>Proxy Authentication Type</b>	The type of authentication used at the proxy server. <ul style="list-style-type: none"> <li>➤ <i>None</i></li> <li>➤ <i>Basic-Authentication</i></li> <li>➤ <i>NTLM-Authentication</i></li> </ul>
<b>Proxy User Name</b>	The credentials to use for authentication at the proxy server when the authentication type is not set to <i>None</i> .
<b>Proxy Password</b>	
<b>Proxy Domain</b>	The domain name to use when <i>NTLM-Authentication</i> is used.

**List 3-24** Administrative Settings - SCEP - SCEP Settings - section Encoding Parameters

Parameter	Description
<b>Transaction ID Encoding</b>	The transaction ID field can be sent in a binary or base64 encoded. Some SCEP servers support both. Although some certificate authorities support the binary format, problems can occur when using it. Falling back to the text format might help in this case.
<b>PKCS7 Cipher</b>	These are the encryption settings used when communicating with the CA. Must be set accordingly to the CA settings.
<b>PKCS7 Hash</b>	
<b>PKCS7 Replay Protection</b>	
<b>Select Encryption Certificate</b>	Choose between <ul style="list-style-type: none"> <li>➤ <i>By-Key-Usage</i></li> <li>➤ <i>Use-Any</i></li> </ul>

## 2.2.4 Identity

Password and username have to be supplied over an SSL-encrypted connection in most cases to be granted administrative access to a box. Before supplying your credentials to the server, for example the phion system, you may want to verify its identity.

To enable this verification the server authenticates itself to the client via a x.509-compatible digital certificate. Precisely speaking it is the public RSA key contained in this certificate that is used to establish the SSL connection in the first place. In order for this to work the administration console needs to associate a public RSA key with a particular phion box and network address. The management console will prompt for a decision how to proceed every time when access to a new box is requested or when the key of a box has changed.

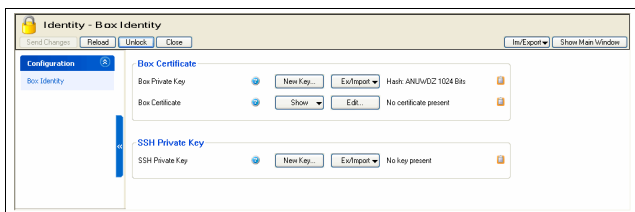
The same applies to accessing to the box via the SSH version 2 protocol. The box will try to prove its identity by means of a public 1024-bit DSA host key.

Only on first connection to a SSH server you will have to trust that the server is the one it claims to be. To avoid further moments of uncertainty a dialogue will then allow for creation of the box's private SSH DS. In this way the associated public key by which the SSH server can be identified is extracted.

The configuration dialogue **Identity** serves two major purposes. First it allows you to issue the contents of the certificate which the box uses to advertise its legitimacy to the world. Second it allows you to trigger the generation of a new private RSA box key or a new private SSH DSA key.

Open the network configuration by clicking twice on **Identity**.

Fig. 3-21 Box Identity



List 3-25 Identity - section Box Certificate

Parameter	Description
<b>Box Private Key</b>	The current base-64 encoded 1024-bit long RSA key of the box. The corresponding public RSA key is part of the box certificate. <b>Note:</b> Every time the key is regenerated the digital identity of the box changes.
<b>Box Certificate</b>	Digital x.509v3 compatible box certificate.

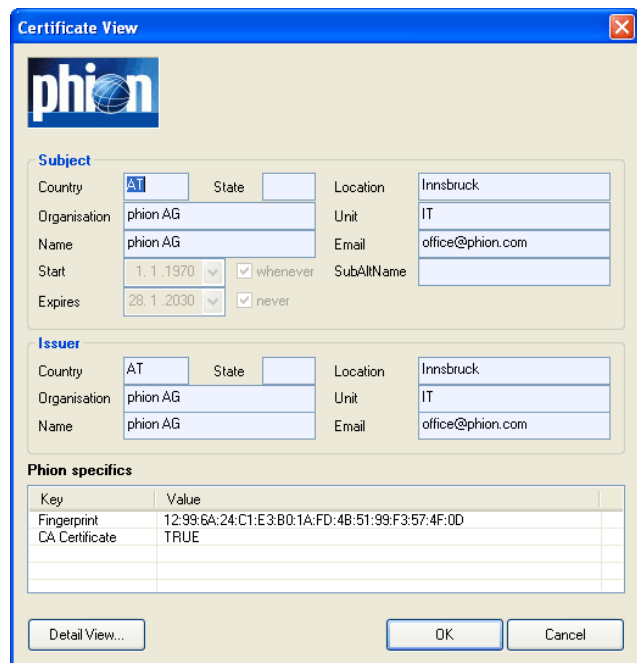
List 3-26 Identity - section SSH Private Key

Parameter	Description
<b>SSH Private Key</b>	Click on <b>New Key</b> to generate a new base-64 encoded 1024-bit long DSA private host key for use by the SSH daemon of the box. You may wish to locally store the corresponding public DSA key (Settings) in order to establish an a priori trust-relationship for SSH access. A key may be identified by its hash with high probability.

phion boxes make use of x.509 conform digital certificates. For a single box without supervision of a phion trust centre the certificate is basically identical to a mere RSA public key. It may be viewed as a neat way of storing information regarding the organisational affiliation of the box. As the certificate contains the public RSA key of the box it is rebuilt every time the key is changed. Editing the certificate on the other hand does not mean that the key is updated.

In order to edit the certificate simply click on the **Edit ...** button.

Fig. 3-22 Certificate window




For better understanding the actual structure of an x.509 conform digital certificate figure 3-23 contains a human readable textual representation of a x.509 digital certificate as used by phion systems to authenticate themselves.

The key elements are issuer and subject (which are identical in case of an unsigned or self-signed certificate), RSA public key (1024 bits), and a signature of the certificate's contents. The latter is created with the private part of the issuer's RSA key and may be verified using the corresponding public counterpart. Evidently, in case of a self-signed certificate there is no point in checking the signature and thus initially a human decision as to whether or not trusting a box is required. In case you run the box in conjunction with a phion cluster administration server the cluster server will take on the role of a trust centre originating certificates. Then it would suffice to check whether or not the certificate produced by the box has





List 3-27 Network - Management Network - section Device Name

Parameter	Description
<b>Hostname</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>The maximum length of this parameter is 25 characters. This is the box hostname without domain suffix.</p> <p><b>Note:</b> Entering a box hostname is obligatory (indicated by the icon ). The hostname is inserted into the file <code>/etc/hosts</code>.</p>

List 3-28 Network - Management Network - section Management Network

Parameter	Description				
<b>Management IP (MIP)</b>	<p>The principal IP address of the box. phion systems do not have dedicated administrative interfaces but rather use administrative IP addresses. The existence of this IP is required for access to the box via SSH as well as to the phion system via the administration console.</p> <p><b>Note:</b> Access to the <b>MIP</b> may be limited through specification in an ACL (at kernel level).</p>				
<b>Associated Netmask</b>	<p>The mask (or extent in bits) of the network the <b>MIP</b> is embedded in. You may choose the netmask from a pull-down menu with 8 bits being the default.</p> <p><b>Note:</b> A netmask smaller than 2 bits does not really make sense.</p>				
<b>Interface Name</b>	<p>For convenience a small pull-down menu containing the interfaces <code>eth0</code>, <code>eth1</code>, <code>tr0</code>, and <code>tr1</code> is present. Select the check box labelled <b>Other</b> to declare another interface. Always remember that your choice is limited to interfaces on NICs for which you have requested driver support.</p>				
<b>Responds to Ping</b>	<p>Governs whether ICMP echo requests will be replied to or not for this address. The default setting is <b>no</b>.</p>				
<b>Bind NTPd</b>	<p>Value <b>yes</b> causes NTPd to bind to this address. The default setting is <b>no</b>.</p> <p><b>Note:</b> NTPd has to be activated separately (see 2.2.3.5 TIME/NTP Tab, page 56).</p>				
<b>Interface Realm</b>	<p>This parameter determines what kind of IP address is to be counted by the firewall for traffic on this interface (<b>Licensing</b> - 6.5 Policy No. 5: General Case, page 510). The interface can be classified to one of the following:</p> <p><b>unspec</b> <b>internal</b> (default) <b>dmz</b> <b>external</b></p>				
<b>MTU</b>	<p>Here the MTU (Maximum Transmission Unit) can be set. Packets above this value are being sent fragmented.</p> <p><b>Note:</b> MTUs may also be set for NICs (list 3-29, page 63), virtual LANs (list 3-30, page 65), additional networks (Networks, page 61) and standard routing (2.2.5.5 Network Routes, page 68). The unwritten rule is that the maximum accepted MTU of the next hop will be used.</p>				
<b>Advertise Route</b>	<p>If set to <b>yes</b> (default: <b>no</b>) all routes will be advertised via Routing Protocols, provided an OSPF or RIP router service is active on the gateway.</p>				
<b>Additional IP Addresses</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Optionally you may specify additional addresses to be active within the primary box network. In general there is no need to make use of this option. Special circumstances may arise when doing so becomes desirable.</p> <p><b>Note:</b> We consider this an advanced option which is prone to cause unexpected behaviour when misused. Thus make sure you understand the implications of the individual options selected for the introduced additional IPs entirely.</p> <table border="1" data-bbox="207 2049 678 2136"> <thead> <tr> <th>IP Address</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td></td> <td>The address must be valid and within the associated network. It will be introduced as a stand alone IP with mask 0.</td> </tr> </tbody> </table>	IP Address	Description		The address must be valid and within the associated network. It will be introduced as a stand alone IP with mask 0.
IP Address	Description				
	The address must be valid and within the associated network. It will be introduced as a stand alone IP with mask 0.				

List 3-28 Network - Management Network - section Management Network

Parameter	Description
<b>Responds to Ping</b>	<p>Governs whether ICMP echo requests will be replied to. The default setting is <b>no</b>.</p>
<b>Management IP</b>	<p>To have box services bound to this IP chose <b>yes</b> (default: <b>no</b>). If yes is selected the <b>Additional IP</b> becomes <b>Management IP</b> supplementary to the <b>Main Box IP</b>.</p>
<b>Bind NTPd</b>	<p>Value <b>yes</b> causes NTPd to bind to this address. The default setting is <b>no</b>.</p> <p><b>Note:</b> NTPd has to be activated separately. (see Administrative Settings, page 53).</p>

### Section **Additional Local Networks**

This section is used to specify additional network addresses of the box besides those in the primary box network. Transit networks, external networks, networks describing demilitarised zones (DMZ) or secure server networks (SSN) could be accounted for by such a section. IP addresses utilised in a private uplink network between HA partners have to be inserted here as well (see 5.2.4.1 Monitoring Setup, page 117).

In general, it is not advantageous to have additional box IP addresses beyond the one required to administer the box. As an alternative strategy you could use a combination of pending direct routes and server IP addresses to grant the box access to additional networks.

phion recommends this latter approach as it leads to increased system security, especially when connecting a system to an untrusted network.

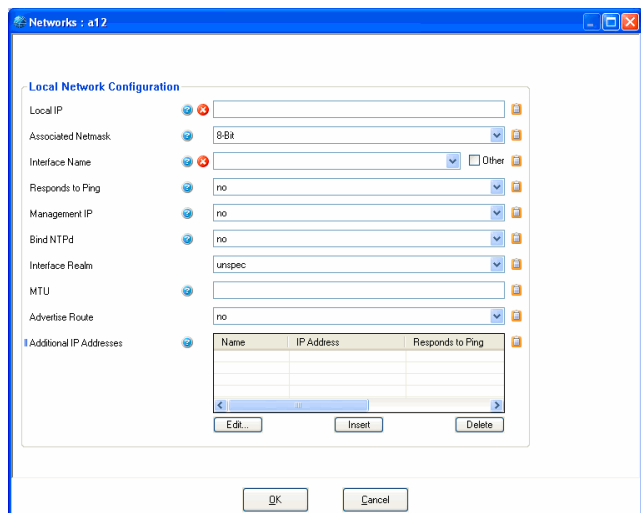
#### **Note:**

phion refers to a direct route as pending if it cannot be activated without the presence of a dynamically activated IP address (for example a server IP) (see Network Routes, page 68).

Like the primary box network, each additional network contains a subsection allowing the introduction of further isolated additional IPs within the network (see Networks, page 61).

To open the configuration dialogue, click the **Insert** button.

Fig. 3-25 Additional Local Networks configuration





### 2.2.5.2 Interfaces

List 3-29 Box Network - section Network Interface Configuration

Parameter	Description	
<b>Appliance Model</b>	<p>This pull-down menu contains all available pre-configured appliances. Selecting the corresponding appliance sets the <b>Visible Interface Name</b> to the name that is engraved on the front of the appliance.</p> <p><b>Note:</b> Each appliance model forces its typical corresponding set of interface names (naming eth&lt;n&gt;, port&lt;n&gt;, LAN&lt;n&gt;, ...). This directly influences values shown below in parameter group <b>Physical Interfaces</b> (page 64).</p> <p><b>Note:</b> Selecting the entry <b>USER</b> enables the section called <b>Port Labelling</b>.</p>	
<b>Port Labelling</b>	<b>Internal Interface Name</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p>
	<b>Visible Interface Name</b>	<p>This configuration section allows defining alternative <b>Visible Interface Names</b> for each interface with a maximum of 5 alphanumeric characters. However, only eth interfaces may be renamed. Interfaces like tap, ppp*, dhcp, loopback are pre-defined and cannot be modified.</p> <p><b>Note:</b> The interface names that are defined within this section should also be used for configuration purpose to avoid "messy" configurations.</p> <p><b>Note:</b> Please consider that interfaces, which have been renamed cannot be dynamically updated in the parameter group <b>Physical Interfaces</b>.</p>
<b>Network Interface Cards</b>	<b>NIC Type</b>	<p>Type of Network Interface Card; information required for logical consistency checks. In conjunction with the specified number of interfaces it becomes possible to check whether a particular interface may be referenced in some of the other sections. Available NICs are: <b>Ethernet</b></p>
	<b>Driver Type</b>	<p>Informs the system as whether the driver support is module or kernel based. Default is <b>Loadable_Module</b>. If module based driver support is not available select <b>Compiled_In</b>. This will automatically deactivate several consistency checking routines.</p> <p><b>Note:</b> When selecting <b>Compiled_In</b> please check whether the system's current kernel provides the required support. phion considers this an advanced option whose utilisation requires a profound understanding of the phion adapted Linux OS.</p>
	<b>Activate Driver</b>	<p>With this option the driver can be activated/deactivated (default: <b>yes</b>).</p>
	<b>Driver Module Name</b>	<p>You have to instruct the system which driver to use for any given kind of interface card. The selection offered corresponds to those cards recommended by phion. Consult the list of supported NICs if you wish to use another card. In this case you will have to select the checkbox labelled <b>Other</b> and enter the module name manually.</p> <p><b>Attention:</b> If you are using a Marvel network adapter that requires the module sk98lin_cb.o, pay attention that interface naming has to begin with eth1. Interface eth0 is NOT supported</p>
	<b>Network Interface Cards</b>	<p>Type of Network Interface Card; information required for logical consistency checks. In conjunction with the specified number of interfaces it becomes possible to check whether a particular interface may be referenced in some of the other sections. Available NICs are: <b>Ethernet</b></p>

List 3-29 Box Network - section Network Interface Configuration

Parameter	Description	
<b>Network Interface Cards</b>	<b>Driver Options</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Used only in conjunction with module based driver support. Refer to the list of supported NICs for more information on this topic. Options are typically used to set the ring speed for token ring interfaces or to bypass media type auto negotiation for ethernet interfaces. Note that several interface specific option strings may be specified, formatted as <b>key=value1 ... valueN</b>, with N being the number of interfaces.</p>
	<b>Number of Interfaces</b>	<p>The number of interfaces (integer) of the NIC or NICs that may be in simultaneous use.</p> <p><b>Note:</b> The <b>Number of Interfaces</b> indicates the number of ports and <b>NOT</b> the number of cards of the particular type, for example one dual-port NIC counts as 2 interfaces, but 1 combo-type card with support for three different connectors (for example BNC, AUI, RJ45) counts as 1, because only one connection is active at one time.</p> <p>You may set the number to zero. In this case the respective module will not be loaded. If more than seven cards (ports) are present, select the checkbox <b>Other</b> and enter the number of cards manually.</p>
	<b>Fallback Enabled</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>With this parameter it is possible to activate an alternative NIC driver that is defined via the entries <b>Fallback Module Name</b> and <b>Fallback Driver Options</b>, both mentioned below. This may be helpful during/after updating sequences. If the primary driver does not work, this fallback driver is used. In case the fallback driver as well does not work both drivers are loaded.</p>
	<b>Fallback Module Name</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. See <b>Driver Module Name</b>, page 63</p>
	<b>Fallback Driver Options</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. See <b>Driver Module Name</b>, page 63</p>
	<b>Ethernet MTU</b>	<p>When using an ethernet NIC (<b>NIC Type</b>, page 64), it is possible to set the MTU size (Maximum Transmission Unit) through this field. Packets exceeding this value will be sent fragmented.</p> <p><b>Note:</b> The MTU specified in this place is used as default value for all existing interfaces. It can be adapted individually per interface using parameter <b>MTU</b> in parameter group <b>Physical Interfaces</b> below (list 3-29).</p> <p><b>Note:</b> MTUs may also be set for virtual LANs (2.2.5.3 Virtual LANs, page 65), box network (2.2.5.1 Networks, page 61), additional networks (Section Additional Local Networks, page 62) and standard routing (Section Main Routing Table, page 68). The rule of thumb is that the maximum accepted MTU of the next hop will be used.</p> <p><b>Note:Example 1:</b> If you have a NIC with MTU size 1500 and a Standard Route with MTU size 2000, the valid MTU size will be 1500. <b>Example 2:</b> If you have a NIC with MTU size 2000 and a Standard Route with MTU size 1500, the valid MTU size will be 1500.</p>
	<b>Network Interface Cards</b>	<p>Type of Network Interface Card; information required for logical consistency checks. In conjunction with the specified number of interfaces it becomes possible to check whether a particular interface may be referenced in some of the other sections. Available NICs are: <b>Ethernet</b></p>

List 3-29 Box Network - section Network Interface Configuration

Parameter	Description	
<b>Interface Usage</b>	The <b>Interface Usage</b> parameter is a read only field. It displays the effective network configuration status and is set to <b>OK</b> , if configuration is in a clean state and all configured interfaces work properly. Otherwise, a warning is displayed.	
<b>Interface Computation</b>	The parameter <b>Interface Computation</b> steers the dynamical updating of values in parameter group <b>Physical Interfaces</b> . If set to <b>yes</b> (default) the view is updated each time the network configuration is changed. If set to <b>no</b> , the view remains at the formerly known values.	
<b>Physical Interfaces</b>	<b>MTU</b>	In general, the <b>MTU</b> size configured in the Box Network - section Network Interface Configuration is valid for all existing interfaces by default. You may use the <b>MTU</b> field in this place to customise the MTU setting to individual values per interface.
	<b>Availability</b>	If nothing else has been configured, all recognised interfaces are generally <b>available</b> by default. Interfaces may be claimed for exclusive use by <b>xDSL</b> ( <b>Connection Type: PPOE</b> ) and <b>DHCP Links</b> (2.2.5.6 xDSL/ISDN/DHCP, page 70). When an interface has been claimed as <b>Modem Interface</b> or <b>DHCP Interface</b> , its usage is set to status <b>reserved</b> . If an interface is claimed by multiple services concurrently, its usage status is set to <b>overbooked</b> . <b>Note:</b> Interfaces marked as overbooked cannot work properly. They will not be available for any of the configured services.
	<b>References</b>	An interface which has not been claimed by a service exclusively is flagged with <b>none</b> . Interfaces claimed by <b>xDSL</b> or <b>DHCP Links</b> are flagged with <b>xdsl</b> or <b>dhcp</b> respectively, followed by the link name as specified in the xDSL/DHCP configuration area when creating the link (for example <b>xdsl::xDSLLinkName</b> ).
	<b>Name of NIC</b>	This is the network card <b>Interface Name</b> as specified when inserted into Interfaces section (see page 63).
	<b>NIC Type</b>	This is the Network Interface Card type as specified when inserted into the <b>Interfaces</b> section (page 63).
	<b>Used Driver</b>	This is the module driver name as defined in parameter <b>Driver Module Name</b> in 2.2.5.1 Networks, page 61.
	<b>Enable Auto negotiation</b>	If the driver, that has been defined through the <b>Driver Module Name</b> (see page 63), does not support the driver options below, this parameter may be set to <b>No</b> in order to enable them. Speed and duplex mode options, which cannot be steered through the NIC driver, can by this means be set manually to a static value through the underlying utility <code>ethtool</code> . Note that this option has been introduced in netfence 3.6.3 because of known issues regarding the <b>Intel e100</b> driver, and that in systems earlier than netfence 3.6.3 <code>ethtool</code> has to be applied manually at the command line interface. Refer to the support section of the phion homepage for details on the usage of <code>ethtool</code> on netfence systems.
	<b>Forced Speed (Mbps)</b>	This is the NICs static network speed ( <b>10/100/1000 Mbps</b> ).
	<b>Duplex Mode</b>	This is the NICs static duplex mode ( <b>half/full</b> ).

List 3-29 Box Network - section Network Interface Configuration

Parameter	Description
<b>Ethernet Trunks</b>	<p><b>Name</b></p> <p><b>Note:</b> Following parameters are only available in <b>Advanced View</b> mode.</p> <p>The name of the trunk is a read-only field (after introduction). It may contain up to 8 characters (digits, "-", the 26 characters from the english alphabet).</p>
	<p><b>Virtual Interface</b></p> <p>The name the trunking interface is referred to. Legitimate names are <b>bond0</b> and <b>bond1</b>. When using a single trunk select <b>bond0</b> as the name of the master interface. In the case of two trunks make sure that the first trunk uses <b>bond0</b> and the second trunk uses <b>bond1</b>. Any other combination will cause the configuration to be rejected.</p>
	<p><b>Trunked Interfaces</b></p> <p>Select at least one ethernet interface (eth0, ...,eth7) from the list. Note that any meaningful configuration should rely on at least two (different) ethernet interfaces. Keep in mind that these interfaces are reserved for exclusive use by the trunking interface. Do not explicitly reference the selected slave interfaces anywhere else in the configuration. Use button <b>Insert ...</b> to apply the values to the list.</p>
	<p><b>Operation Mode</b></p> <p>The following trunking modes are available:</p> <ul style="list-style-type: none"> <li>➤ In mode <b>Fallback</b> (active backup policy) at least two interfaces are required with only a single slave interface being active at any one time. A prolonged failure of the link check on the active interface will trigger the activation of a backup slave interface.</li> <li>➤ In mode <b>Bundle</b> (round-robin policy) as many configured slave interfaces as possible are activated. The kernel will distribute network traffic sent to the master interface to all slave interfaces involved. In a similar fashion inbound traffic to any of the slave interfaces is directed to the master interface.</li> <li>➤ In mode <b>Broadcast</b> everything is transmitted on all slave interfaces.</li> <li>➤ In mode <b>XOR</b> the same slaves are selected for each destination MAC address.</li> <li>➤ Mode <b>LinkAggregation</b> If this option is selected parameter <b>LACPDU Packet Rate</b> becomes configurable.</li> </ul>
<b>Link Check Mode</b>	<p>Here the checking method can be defined. The following options are available:</p> <ul style="list-style-type: none"> <li>➤ <b>Compatibility</b> (default)</li> <li>➤ <b>Efficiency</b></li> </ul>
<b>Link Check (ms)</b>	<p>The bonding driver can regularly check all its slaves' links by checking the MII status registers. <b>Link Check</b> takes an integer that specifies the check interval in milliseconds.</p> <p><b>Note:</b> phion recommends to leave this parameter at its default setting, 100 ms. Thus an inactive or dead link will be detected at the most 100 ms after it has gone down.</p>
<b>Activation Lag (ms)</b>	<p>The time it takes before a backup slave interface is activated. Use this if it is desirable not to activate a backup interface immediately after a link has gone down. It has to be an integer multiple of the <b>Link Check</b> interval.</p>
<b>Deactivation Lag (ms)</b>	<p>Time in milliseconds by which the moment when a link will be completely disabled is delayed. It has to be an integer multiple of the <b>Link Check</b> interval.</p>
<b>LACPDU Packet Rate</b>	<p>The default is <b>Slow</b> meaning that a request is sent to the switch every 30 seconds, if set to <b>Fast</b> it will happen once every second. This parameter is configurable when parameter <b>Operation Mode</b> is set to <b>LinkAggregation</b>.</p>

List 3-29 Box Network - section Network Interface Configuration

Parameter	Description
<b>Interface Name</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>This is the name of the interface. Its labelling is triggered through <b>Appliance Model</b> selection (list 3-29, page 63).</p>

### 2.2.5.3 Virtual LANs

**Note:**  
Configuration of this section is only of avail in combination with a properly configured 802.1q capable switch.

With a Virtual LAN, several LANs on one network interface (but only one MAC address) can be simulated. The interface will behave as if it were several interfaces; the switch will behave as if it were multiple switches.

Virtual LANs are needed if too few slots for PCI interfaces exist on the machine. By using virtual LANs it would be possible to run a firewall with only one network interface.

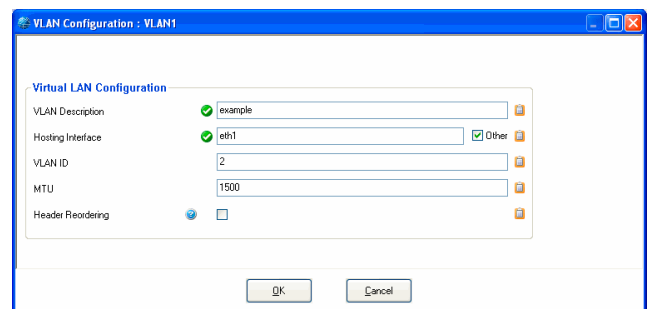
**Note:**  
On netfence gateways, only the following NICs supported by the listed drivers are capable of VLAN technology. Furthermore, phion recommends the usage of Intel NICs.

Table 3-7 NICs supporting VLAN technology

Supported NIC	Module
Intel 100 MBit Driver by Intel	e100.o
Intel 100 MBit Driver by Intel (certified by Compaq)	e100compaq.o
Intel 100 MBit Driver	eeepro100.o
Intel 1000 MBit Driver by Intel	e1000.o
Intel 1000 MBit Driver by Intel (certified by Compaq)	e1000compaq.o
Broadcom 1000 MBit Driver by Broadcom	bcm57xx.o
Broadcom 1000 MBit Driver	tg3.o

To open the VLAN configuration dialogue, click the **Insert** button:

Fig. 3-26 Virtual LAN configuration



List 3-30 Network - Virtual LANs Configuration - section Virtual LAN Configuration

Parameter	Description
<b>Name</b>	This is the name of the virtual LAN.
<b>VLAN Description</b>	Provide the VLAN with a significant description (optional).
<b>Hosting Interface</b>	Physical interface on which the virtual LAN should live (for example <b>eth0</b> ).
<b>VLAN ID</b>	This ID has to be the same as on the switch (for example <b>5</b> ).
<b>Note:</b>	In network configuration dialogues, a VLAN interface may be addressed with its Supporting Interface name and VLAN ID, separated by a point (for example <b>eth0.5</b> ).

**List 3-30** Network - Virtual LANs Configuration - section Virtual LAN Configuration

Parameter	Description
<b>MTU</b>	The <b>Maximum Transmission Unit</b> defines up to what size packets are sent directly. Packet sizes over this value are sent fragmented.  <b>Note:</b> MTUs may also be set for NICs (2.2.5.1 Networks, page 61), box network (list 3-29, page 63), additional networks (Section Additional Local Networks, page 62) and standard routing (Section Main Routing Table, page 68). The rule of thumb is that only MTUs smaller than the one of the supporting interface make sense.
<b>Header Reordering</b>	Ticking this checkbox causes tag reordering in the Ethernet header of VLAN tagged packets so that the VLAN interface appears as common Ethernet interface. Header reordering might become necessary in rare cases if external software components connecting to the VLAN interface experience communication problems.  <b>Note:</b> Header reordering is disabled by default. Do <b>NOT</b> change the default setting without explicit need.

**Note:**

The label of a network interface is put together by interface name, VLAN-ID and server name, separated from one another by punctuation marks. The label construct looks alike the following: `interfacename.vlanid:servername` (for example **eth0.99:foo**).

A label, including punctuation marks, must not be longer than 15 characters.

### Configuring and activating VLANs

Proceed as follows to configure and activate a virtual LAN in the network configuration:

#### Step 1 Create the virtual interface in the VLANS tab

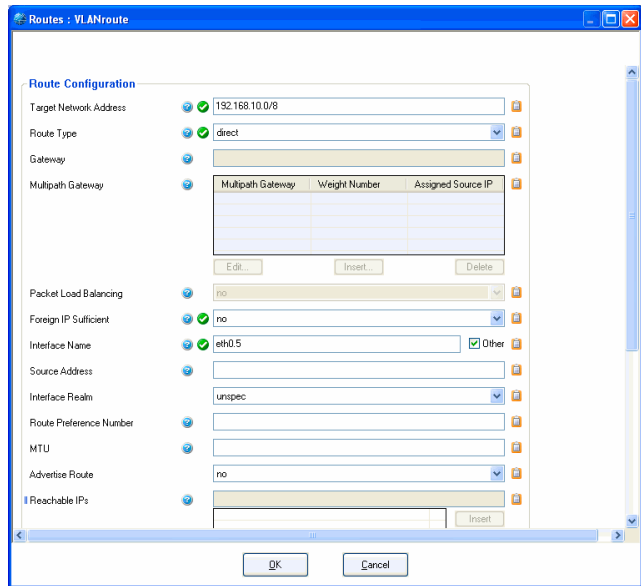
- Browse to **Config > Box > Network > Virtual LANs**.
- Specify the **Hosting Interface**. Therefore, either select the interface from the pull-down menu or select checkbox **Other** and enter the name of the interface the VLAN should live on manually (for example eth0).
- Specify the **VLAN ID** (for example 5).
- Optionally, adapt the **MTU** size.

#### Step 2 Create a direct route for the VLAN

- Browse to **Config > Box > Network > Network Routes**.
- Insert a route into the **Section Main Routing Table** field.
- Specify the address of the VLAN in the **Target Network Address** field (for example 192.168.8.10).
- Set the **Route Type** field to **direct**.
- Insert the name of the virtual interface into the **Interface Name** field. Therefore, select checkbox **Other** and enter the interface name manually (for example eth0.5).

- Specify a value for parameter **Foreign IP Sufficient** (page 69).

**Fig. 3-27** Direct route configuration for Virtual LAN



#### Step 3 Confirm the changes

- Click the **Send Changes** and **Activate** buttons to confirm your configuration changes.

#### Step 4 Activate the new network configuration

- Browse to **Control > Box** tab.
- Click the **Activate New** button and choose **Failsafe** to activate the new network configuration.
- This action will introduce the VLAN interface and a pending direct route in the **Control > Box** tab (**Control Centre** - 2.2.8.1 Handling of Routes by the Control Daemon, page 33).

#### Step 5 Activate the VLAN

Depending on the intended use, introduce the VLANs IP address either in:

- the Networks configuration area as **Section Additional Local Networks** (**Box > Network > Networks**, page 62).
- the Server configuration area as **Server Address** (see 3. Configuring a New Server, page 94 - 3.2.1 General, page 95).

As soon as the VLANs IP address has been introduced, the inserted direct route will be activated.

### 2.2.5.4 Management Access

**Note:**

This section is only available on MC-administered boxes and phion M-series boxes. Configuration is recommended for systems that are managed over the Internet.

**List 3-31** Management Access - section Remote Management Tunnel

Parameter	Description
<b>Enable Tunnel</b>	Setting to <b>yes</b> (default: <b>no</b> ) activates remote control options and enables the corresponding configuration parameters below.
<b>Virtual IP (VIP)</b>	The Virtual IP (VIP) is used for management access to the netfence system. When specified, all communication between management centre (MC) and box is processed through the VIP. The VIP may as well be addressed as Box Login address by client workstations administering the systems. Therefore, the VIP must be defined uniquely and it must reside in a <b>Box VIP Network Range (phion management centre - 6.3.10 Global Settings - Box VIP Network Ranges, page 415)</b> .
<b>Tunnel Details</b>	Choose <b>Set...</b> to set the <b>Tunnel Details</b> . Description see list 3-33, page 67

**Note:**

This parameter group is only available in **Advanced View** mode.

**List 3-32** Management Access - section Serial Console

Parameter	Description
	<b>Note:</b> See also 2.2.3.3 DNS, page 55.  To open the configuration dialogue, click the <b>Show...</b> button. To delete current settings, click the <b>Clear</b> button.
<b>PPP Remote IP</b>	This is the IP address connecting via the serial IP.
<b>PPP Local IP</b>	This is the Box Management IP. If this field is empty, the Box IP itself will be used.
<b>Require PAP</b>	With this option active the connecting client is required to authenticate itself to the netfence gateway [possible users: <code>root</code> or service user (phion)].

Tunnel Details - MC-managed box

**List 3-33** Remote Management Access - Tunnel Details - section Management Tunnel Configuration (MC-managed box)

Parameter	Description
<b>Used VPN Protocol</b>	Choose the appropriate protocol ➤ <b>VPN2</b> (default) or ➤ <b>legacy</b>
<b>VPN Point of Entry</b>	For establishing the remote management tunnel the box VPN client uses the Point of Entry IP as a destination IP. Thus the Point of Entry must be reachable by routing to successfully establish a remote management tunnel. In most cases the Point of Entry will be an external IP address (e.g. from an external firewall at the headquarters which redirects the VPN port to the MC server IP).  <b>Note:</b> Keep in mind that when the remote management tunnel is established through a Proxy server, the <b>VPN Point of Entry IP</b> inherits the Proxy server's port information. To achieve correct mapping, a rule that translates port addresses in connection requests to the <b>VPN Port</b> (see below) has to be created in the forwarding firewall of the gateway presenting the VPN Point of Entry. For translation of port addresses, use action type <b>Redirect</b> .
<b>VPN Port</b>	The VPN Port defines the destination port used by the box VPN client to establish a remote management tunnel (default: <b>692</b> ).
<b>Type of Proxy</b>	This option allows configuring the server type, in case the management setup provides management tunnel establishment through a Proxy server. By default (setting: <b>none</b> ), it is assumed that no Proxy server is used. Other Proxy server types are <b>secure-http</b> , <b>socks5</b> and <b>socks4</b> .
<b>Transport Protocol</b>	Choose <b>TCP</b> or <b>UDP</b>
<b>VPN Local IP</b>	If a special source IP is required (e.g. for policy routing purposes) the VPN local IP can be specified here. If this field is empty a source IP according to the routing table is used.
<b>VPN Interface</b>	Defines the interface that is to be used for VPN connections (default: <b>tap3</b> ).

**List 3-33** Remote Management Access - Tunnel Details - section Management Tunnel Configuration (MC-managed box)

Parameter	Description
<b>Proxy Server IP</b>	In case the management setup provides a Proxy server, specify its IP address in this field.
<b>Proxy Server Port</b>	Enter the proxy server port here.
<b>Proxy User</b>	If using secure-http enter a user name for authentication on the proxy here.
<b>Proxy Password</b>	Enter the proxy user's password here.
<b>Target Networks</b>	Enter the destination addresses that should be reached by the local box via the tunnel.  <b>Attention:</b> Minimum requirement: IP address of the management centre.
<b>Reachable IPs</b>	To check the availability of the remote management tunnel the box periodically sends ICMP echo request packets to the configured Reachable IPs. By default the Server IP of the management centre is used as reachable IP. If the destination host does not respond the box VPN client assumes that the remote management tunnel is broken and tries to re-establish the tunnel.

**List 3-34** Remote Management Access - Tunnel Details - section Connection Monitoring

Parameter	Description
<b>No. of ICMP Probes</b>	Number of ICMP echo packages that are sent via the VPN tunnel (default: <b>2</b> ).
<b>Waiting Period [s/probe]</b>	Number of seconds per probe while answering of the ping is awaited (e.g. probes=3 and waiting period=2 results in 3x2 s waiting time; default: <b>1</b> ).
<b>Run Probes Every [s]</b>	This parameter defines the time period in seconds for ICMP probes (default: <b>15</b> ).
<b>Failure Standoff [s]</b>	If no connection is possible, this time period is waited prior to a retry (default: <b>45</b> ).
<b>Alarm Period [s]</b>	If this time limit is exceeded without establishing a connection successfully, an alarm is set off (default: <b>120</b> ).

Tunnel Details - M-series

**Note:**

Dialogue **Tunnel Details** for generic VPN server for self-managed M-series appliances is different to the one for MC-managed boxes. See the following parameter list.

**List 3-35** Remote Management Access - Tunnel Details - section Management Tunnel Configuration - M-series (vpnc3)

Parameter	Description
<b>Used VPN Protocol</b>	For M-series appliances it is <b>VPN2</b> .
<b>VPN Server Key</b>	Public key from partner certificate (Server Protocol Key)
<b>VPN Server</b>	IP of the passive tunnel partner (VPN server bind IP)
<b>VPN Port</b>	see Tunnel Details - MC-managed box, list 3-33
<b>Remote Networks</b>	Enter the destination addresses that should be reached by the local box via the tunnel.
<b>Type of Proxy</b>	see list 3-33
<b>Transport Protocol</b>	see list 3-33
<b>VPN Local IP</b>	see list 3-33
<b>VPN Interface</b>	see list 3-33
<b>Proxy Server IP</b>	see list 3-33
<b>Proxy Server Port</b>	see list 3-33
<b>Proxy User</b>	see list 3-33
<b>Proxy Password</b>	see list 3-33
<b>Reachable IPs</b>	see list 3-33



### 2.2.5.5 Network Routes

#### Section *Main Routing Table*

Before discussing this section in detail a short digression is required to explain the way in which routing is handled by phion boxes.

We distinguish between two basic types of routes:

- direct routes
- gateway routes

The latter comprises all routes which utilise a next hop address. By default each introduced network (primary network as well as all additional networks) automatically effects a corresponding direct route.

For example, if you have configured a network 10.0.0.8/8 on interface eth0 then the corresponding route will imply that network 10.0.0.0 with mask 255.255.255.0 (and broadcast 10.0.0.255) can be reached directly via interface eth0. Furthermore the box would use address 10.0.0.8 as its source address to which replies should be sent.

We thus realise that an active direct route is fully determined by four key parameters:

- Target network
- Target netmask
- Interface
- Source address

Direct routes state how addresses in directly attached networks may be reached. Each network (**BOX NETWORK** and each of the optional **Additional Local Networks**) corresponds to exactly one direct route.

What about stand alone direct routes?

Assume you know that network 10.255.0.0/8 may also be reached directly via interface eth0 but you do not wish to introduce this network on your box.

Since you have not introduced a network the issue arises as to which source address should the direct route adopt? The operating system would automatically assign an address from an already existing network on the same interface. If several networks already exist you even have a choice of source address. The route dialogue then allows you to explicitly specify the desired source. Picking the right source address may be crucial under certain circumstances, as it can be the key factor whether traffic is routed back to the box or not.

In case no network has been introduced on an interface the Linux operating system would not allow you to introduce a direct route, since no valid source address is available.

One of the advanced features of phion boxes is that you may still configure so-called **pending direct routes**, which will be hidden from the operating system until an appropriate source address becomes available. In the context of firewalling this would allow you to configure a routing setup, which only becomes active when the firewall is active. The advantage of this is that the box as such will

never be directly accessible as a target for malicious activity.

Gateway routes now specify through which host within a directly attached network a particular remote network may be reached.

#### **Note:**

Direct routes are a necessary prerequisite for the successful introduction of gateway routes since in the first place you must be able to contact the next hop address.

We therefore realise that an active gateway route is determined by five key parameters:

- Target network
- Target netmask
- Next hop address
- Interface
- Source address

As far as its configuration is concerned only the first three parameters are mandatory, as interface and source address are inherited from the direct route leading up to the next hop or gateway address.

One of the advanced features of phion boxes is that you may configure so-called **pending gateway routes**. Their next hop addresses are only reachable via a pending direct route. They will be hidden from the operating system until the underlying required direct route becomes available. Yet once configured the status of both, pending direct routes and pending gateway routes, will always be visible from the control window.

To develop a better understanding consider the following example:

Box "Sega" is a border firewall using three ethernet interfaces:  
 eth0: 10.0.0.8/8 internal network  
 eth1: 192.168.0.1/8 DMZ  
 eth2: external connection

Assume that the box has been assigned a single internationally valid IP address 1.2.3.4 within the provider's network 1.2.4.0/5. Its default gateway has address 1.2.3.1.

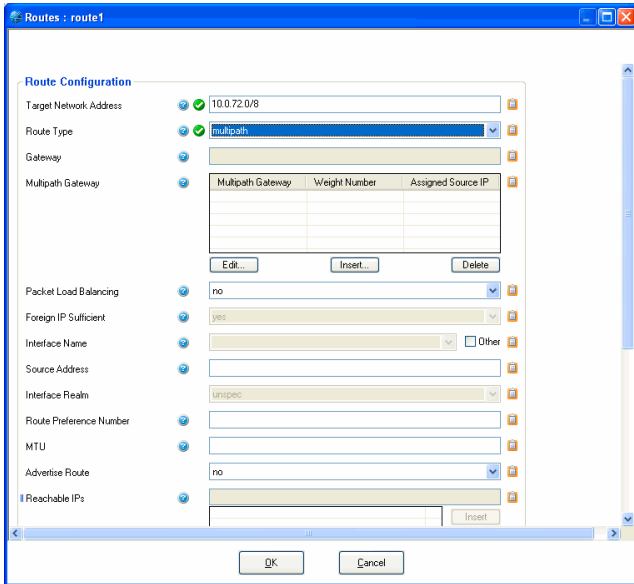
We would now configure a pending direct route into the provider's net:  
 1.2.3.0/5 via dev eth2  
 and a corresponding pending gateway route (which means the default route)  
 0.0.0.0/32 via 1.2.3.1

At boot time none of these would be activated. If we assign the firewall module address 1.2.3.4 as one of its addresses, both routes will be activated by the control daemon as soon as the firewall module is activated. If the firewall is blocked both routes will be deactivated again and the box is no longer accessible from the Internet.



To open the configuration dialogue, click the *Insert* button.

Fig. 3-28 Main Routing configuration



List 3-36 Network - section Main Routing Table

Parameter	Description						
<b>Target Network Address</b>	Network base address and netmask of the target network.						
<b>Route Type</b>	Type of route. Set to <i>direct</i> for a direct route. For a gateway route choose <i>gateway</i> . For usage of multiple gateways choose <i>multipath</i> . If using <i>multipath</i> further values under <i>Multipath Gateway</i> (see below) have to be set.						
<b>Gateway</b>	This field is only available with route type <i>gateway</i> and contains the address of the next hop or gateway. The gateway must be reachable by a direct route. This means the gateway address must be within the bounds of one of the target networks of the box direct routes. <b>Note:</b> The control daemon will disable the route for as long as the gateway is not reachable.						
<b>Multipath Gateway</b>	This field is only available with route type <i>multipath</i> . <table border="1" style="width: 100%;"> <tr> <td><b>Multipath Gateway</b></td> <td>Next hop IP address of the multipath route.</td> </tr> <tr> <td><b>Weight Number</b></td> <td>Weight number of path (valid range from 0 -10). Lower preference number means higher preference.</td> </tr> <tr> <td><b>Assigned Source IP</b></td> <td>Source address of traffic associated with the given multipath gateway.</td> </tr> </table> <b>Note:</b> If one of the gateways is no longer available, the metric is shifted automatically. For further information and configuration examples with <i>route type multipath</i> see <b>Firewall - 2.2.6.2 netfence Multipath Routing</b> , page 147.	<b>Multipath Gateway</b>	Next hop IP address of the multipath route.	<b>Weight Number</b>	Weight number of path (valid range from 0 -10). Lower preference number means higher preference.	<b>Assigned Source IP</b>	Source address of traffic associated with the given multipath gateway.
<b>Multipath Gateway</b>	Next hop IP address of the multipath route.						
<b>Weight Number</b>	Weight number of path (valid range from 0 -10). Lower preference number means higher preference.						
<b>Assigned Source IP</b>	Source address of traffic associated with the given multipath gateway.						
<b>Packet Load Balancing</b>	Set to <i>yes</i> to activate packet based load balancing over multiple next hops.						
<b>Foreign IP Sufficient</b>	Set to <i>yes</i> (default) to bring up a pending route when any IP becomes available on the interface, even if it does not belong to the target network. Set to <i>no</i> to activate a pending direct route only if a local IP belonging to the target network is or becomes available. <b>Note:</b> The control daemon will always try to select the best match by definition.						
<b>Interface Name</b>	You need to specify an existing interface (list 3-29, page 63). When having VLANs, it is mandatory to add the VLAN ID (for example <code>eth0.5</code> ; 2.2.5.3 Virtual LANs, page 65).						
<b>Source Address</b>	Optional entry allowing you to specify the used source address manually. This address must have been configured in one of the preceding two sections.						

List 3-36 Network - section Main Routing Table

Parameter	Description
<b>Interface Realm</b>	This parameter determines what kind of IP address is to be counted by the firewall for traffic on this interface ( <b>Licensing - 6.5 Policy No. 5: General Case</b> , page 510). - Only available with <i>Route Type direct</i> . The interface can be classified to one of the following: <i>unspec</i> (default), <i>internal</i> , <i>dmz</i> , <i>external</i> .
<b>Route Preference Number</b>	Direct routes do not generally have to be equipped with preference numbers. An exception worth mentioning can be regarded as given if several routes to the same target network exist. Preference numbers may then be assigned to each direct route. Flag the preferred route with a lower preference number. In case the gateway becomes unreachable the route with the higher preference number will be used as a backup option.
<b>MTU</b>	Here the MTU (Maximum Transmission Unit) can be set. Packets over this value are sent fragmented. <b>Note:</b> MTUs may also be set for NICs (2.2.5.2 Interfaces, page 63), virtual LANs (list 3-30, page 65), box network (2.2.5.1 Networks, page 61) and additional local networks (Section Additional Local Networks, page 62). The rule of thumb is that the maximum accepted MTU of the next hop will be used.
<b>Advertise Route</b>	If set to <i>yes</i> (default: <i>no</i> ) all routes will be advertised via Routing Protocols, provided an OSPF or RIP router service is active on the gateway.
<b>Reachable IPs</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Insert the IP addresses of hosts into this field that should be reachable via this route.
<b>Re-Reachable Command</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Insert commands that should be run into this field when formerly unreachable IPs become accessible again.
<b>Unreachable Command</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Here insert commands that should be run when neither gateway nor IP addresses that have been defined as <i>Reachable IPs</i> (see above) are accessible.

**Section Policy Based Routing**

As stated at the end of the preceding section policy routing is a way to implement more complex routing scenarios. The implementation provided by your phion system only uses a subset of the functional scope of policy routing. We base the decision as to whether or not a certain routing table is consulted solely on the source address used to establish a connection.

Since the firewall configuration (on a per rule basis) allows you to specify the address with which an allowed connection is established, policy routing represents an extremely powerful instrument to manage firewalling in topologically complex environments. Virtual private networks (VPN) and IP tunnels in general will routinely have to make use of some sort of policy routing.

Policy routing is all about rules and routing tables. A rule assigns an IP address range (source addresses) to a named routing table. Rules are organised in an ordered list, which means each rule is associated with a preference number. A routing decision by the operating system now involves a walk through of the rule set, starting from the rule with lowest preference number, until a match based on source address is attained. In this case the routing table the rule points to is consulted. If a matching route to the destination address is found in the particular table it will be applied. Otherwise the remaining rules are consulted until a match is found or if there are no more rules. In the latter case the destination is said to be unreachable.

When introducing a new policy routing section you create a table and at least one rule at the very same time. More precisely, the name of the table you create is the name of the section; for every source (IP/mask pair) you specify you will create a rule (all with the same preference) pointing to this table.

On every phion system at least the following routing rules are always present:

**Table 3-8** phion routing rules

Rule	Source	Table
0	0.0.0.0/32	local
1	VIP	vpn2mc
2	VIP	vpn2inet (prohibit)
3	0.0.0.0/32	vpnlocal
10000	0.0.0.0/32	main
32767	0.0.0.0/32	default

Table **local** will contain all routing information related to local addresses, directly attached networks (direct routes), and broadcast addresses. All routes introduced under **Section Main Routing Table** wind up in table **main** unless their target network is 0.0.0.0/32 in which case they are placed into table default.

Table **vpn2mc** is defined but empty unless the box comes available via a VPN tunnel.

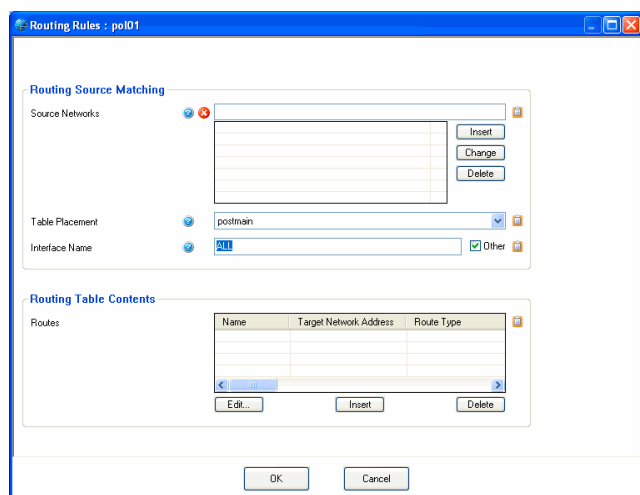
Table **vpn2inet** is used for blocking additional route look up.

Consequently, it will usually make a marked difference whether or not a rule is inserted before or after the one pointing to table main (preference 10000). We thus have made provisions to specify on a per table basis, if the table is inserted before or after table main. Thus the administrator will now have to worry about preference numbers which are automatically generated in descending order from 9999 for premain placement or in ascending order from 10001 for postmain placement, respectively.

The one thing the administrator will have to worry about is that there is no overlap between source addresses belonging to different rules and therefore tables.

To open the configuration dialogue, click the **Insert** button.

**Fig. 3-29** Policy Routing configuration



**List 3-37** Network Routes - Policy Routing - section Policy Source Matching

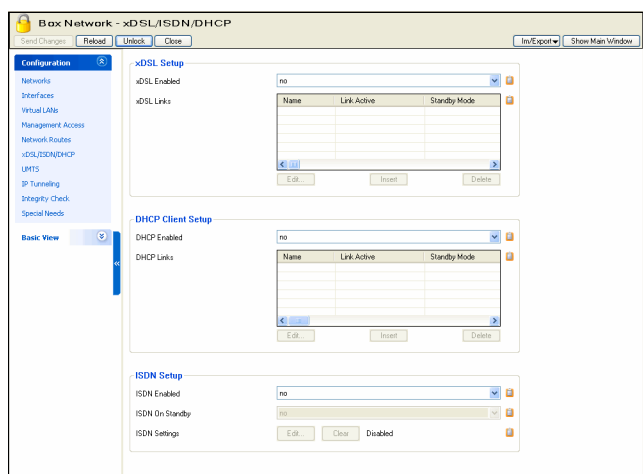
Parameter	Description
<b>Source Networks</b>	Array of source networks or single hosts for which this policy routing table is looked up. IP/mask notation is expected. For a single host you will have to supply <b>0</b> as its netmask. ( <b>Getting Started - 5.</b> phion Notation, page 25)
<b>Table Placement</b>	Governs placement of the table. You have a choice between the default <b>postmain</b> and the advanced option <b>premain</b> . only in rare instances you should need to introduce a table that is positioned before the main table. You would use this option if you would wish to create exemptions from the general routing framework (gateway routes) of table main for certain source addresses. <b>Note:</b> Direct routes refer to routes to directly attached networks. Direct routes based on tunnel interfaces do clearly not fall into this category. In any case direct routes automatically go into table local and are thus omnipresent. A <b>postmain</b> placement makes sense if you wish to implement an alternative default route for certain source addresses. In the majority of all cases you will probably want to use postmain.
<b>Interface Name</b>	Introduces policy tables which are based on both source networks and input interface.

**List 3-38** Network Routes - Policy Routing - section Policy Table Contents

Parameter	Description
<b>Routes</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Subsection containing the routing content of this table. phion supports gateway routes only since direct routes are already contained in table main. In appearance the corresponding dialogue is essentially the same as the one for gateway routes within list 3-36, page 69, with all direct route specific options removed. The parameter <b>Route Type</b> contains the additional entry <b>throw</b> . This route type is special as a match is not treated as a termination of the route lookup. Instead only the route lookup in the current table is terminated and the lookup continues with the remainder of the routing structure.

## 2.2.5.6 xDSL/ISDN/DHCP

**Fig. 3-30** xDSL/ISDN/DHCP configuration



### Section xDSL Setup

The configuration allows for the integration of up to four asymmetric digital subscriber lines (xDSL). xDSL (in its many variants ADSL, SDSL ...) has become popular as a low cost medium performance alternative to leased lines. Standard Linux implementations rely on the use of a combination of PPP (point-to-point protocol) and PPTP (point-to-point tunnelling protocol) or PPPOE

(point-to-point protocol over ethernet). In order to bring up the xDSL link you will have to identify yourself to the xDSL provider by supplying a special username and password combination.

xDSL links are special as they involve a dynamic component. The IP address assigned to you by your xDSL provider will change every time the link is brought up. Consequently, an xDSL link to the internet would not be convenient to grant others access to parts of your network.

**Note:**

Alternatively, you might try to coax your provider into assigning you your own fixed IP address.

Moreover, telecom providers are known to be in the habit of disconnecting your xDSL modem from the network after a given period of time.

For this reason phion xDSL link management automatically introduces and deactivates routes, rules, and tables required by the xDSL link. It continuously monitors the link status and the reachability of certain configurable addresses. If required the link will be brought down and subsequently re-established. This ensures that if there is a way to have the link up it will be up.

By selecting **yes** for the entry **xDSL Enabled** the other configuration areas for xDSL connections will be activated.

The entry **Standby Mode** allows combining HA setups to achieve high available xDSL connections. Setting this parameter to **yes** implements two different working steps:

- The involved routes are set to pending state, and it is not checked whether they are established.

- The configuration is completely run through but the connection is not yet established. Connecting is handled via a server-side script that is used for starting and stopping the connection with corresponding command lines:

```
connection start:
/etc/phion/dynconf/network/openxDSL start
<name>
connection stop:
/etc/phion/dynconf/network/openxDSL stop
<name>
```

This way it is guaranteed that as soon as the server is up, the connection is established automatically, whereas when the server is to be deactivated, the connection is stopped automatically. By doing so, it is possible to implement HA setups with broadband links.

**Attention:**

To avoid routing conflicts in multi-provider environments, be aware that every provider usually assigns the same gateway to a dynamically assigned IP address. Do not configure multiple xDSL links managed by the same provider, unless you are sure that the assigned addresses stem from distinctive IP pools and use clearly distinguishable gateways.

To open the configuration dialogue, set **xDSL Enabled** to **yes** and then click the **Insert** button.

List 3-39 Network - xDSL configuration - section Link Properties

Parameter	Description
<b>Name</b>	This is the name of the xDSL link. <b>Note:</b> Only ciphers and characters from the Latin character set excluding special characters are allowed in the link name
<b>Link Active</b>	If set to <b>yes</b> the link is taken into account for link management, otherwise it is ignored.
<b>Standby Mode</b>	If set to <b>no</b> (default) the link is supposed to be activated and monitored as a consequence of a network activation. If set to <b>yes</b> , its activation and subsequent monitoring needs to be triggered externally. Note that for a PPP multi-link bundle the setting of the respective primary link is adopted for all links.
<b>Enable PPP Multilink</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. If set to <b>yes</b> the two entries below are activated and the link will become part of a PPP multilink bundle (note that the ISP providing the links needs to explicitly support this feature).
<b>Primary Link</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Selects the primary link of a PPP multilink bundle. A link becomes primary when its own name is selected here.
<b>Endpoint Descriptor</b>	Optional entry that may be used to describe the local system in a unique fashion. It sets the endpoint discriminator sent by the local machine to the peer during multilink negotiation to this value. The default is to use the MAC address of the first ethernet interface on the system, if any, otherwise the IPv4 address corresponding to the host-name, if any, provided it is not in the multicast or locally-assigned IP address ranges, or the localhost address. The endpoint discriminator can be the string null or of the form type: value, where type is a decimal number or one of the strings local, IP, MAC, magic, or phone. The value is an IP address in dotted-decimal notation for the IP type, or a string of bytes in hexadecimal, separated by periods or colons for the other types. For the MAC type, the value may also be the name of an ethernet or similar network.
<b>Synchronous PPP</b>	If set to <b>yes</b> PPP and the transport protocol daemons - as determined by the parameter below - will initiate a connection in synchronous mode.  This is usually of higher performance but requires appropriate support by the opposite server end.
<b>Connection Type</b>	Specifies the transport protocol for the PPP protocol. Note that in case of PPP multilink bundles all links must use the same connection types.

List 3-40 Network - xDSL configuration - section PPTP Connection Details

Parameter	Description
<b>Modem IP</b>	Address of the xDSL modem or PPTP server to which a PPTP connection is supposed to be established.
<b>Local IP Selection</b>	This parameter offers the following options: ➤ <b>Static</b> Static is the standard one, where the local address is specified ➤ <b>DHCP</b> DHCP is the old get address from DHCP option ➤ <b>Dynamic</b> Dynamic is the option, it means that the device will pick the one address that is provided by routing to reach the PPTP server. This address is then reported to the firewall engine for GRE registration.
<b>Required DHCP Link</b>	This field is only active with <b>Local IP via DHCP</b> set to <b>yes</b> . Name of the DHCP section this xDSL link relies upon for providing a routing path to the configured <b>Modem IP</b> address.

List 3-40 Network - xDSL configuration - section PPTP Connection Details

Parameter	Description
<b>Local IP</b>	Only needed with PPTP selected. Determines the <b>Local IP</b> address, which is used to establish a connection with the <b>Modem IP</b> address. The local address must be an already configured local IP address. The specified address is used for local GRE protocol registration with the local firewall. <b>Note:</b> This option and the Local IP via DHCP option are mutually exclusive.
<b>Gateway to Modem IP</b>	Optional entry that may be used to handle scenarios where the xDSL Modem or PPTP server are not directly attached to the gateway. Note that this option and the Local IP via DHCP option are mutually exclusive. <b>Note:</b> A gateway route will automatically be created for PPTP.
<b>Max MTU/MRU Size</b>	default: 1492 Possible values from 60 to 1492.

List 3-41 Network - xDSL configuration - section PPPOE Connection Details

Parameter	Description
<b>Modem Interface</b>	Name of the ethernet interface to which the xDSL modem or PPPOE server is attached. In the latter case use of a crossover cable is required.
<b>Max. Segment Size</b>	Specifies the maximum segment size for the encapsulated traffic. The default value is 1412 bytes.

List 3-42 Network - xDSL configuration - section Authentication

Parameter	Description								
<b>Authentication Method</b>	Select the method for authentication here. Authentication protocols can be set to <b>PAP</b> (default), <b>CHAP</b> or <b>PAP_or_CHAP</b> .								
<b>User Access ID</b>	Principal account name (PPP user name) assigned to you by your provider.								
<b>User Access Sub-ID</b>	PPPOE-only option. Some providers (for example Deutsche Telekom) assign this sub-ID, which is separated from the User Access ID by a hash sign '#'. Note that the hash sign must not be typed in.								
<b>Access Password</b>	PPP password assigned to you by your ISP.								
<b>Provider Name</b>	PPPOE-only option. Some providers assign user access IDs, which contain a provider name separated from the actual User Access ID (and optional Sub-ID) by an '@' symbol. Note that the '@' must not be typed in. It will be automatically generated (for example username#subid@provider).								
<b>Access Concentrator</b>	PPPOE-only option. The name of the Access Concentrator (pppoe Server) entered here has to be specified by the provider. This is an optional value. Use only if required.								
<b>Service Name</b>	Set to <b>yes</b> if you wish to use the DNS server(s) assigned by your provider.								
<b>Use Provider DNS</b>	Set to <b>yes</b> (default: <b>no</b> ) if you wish to use the DNS server(s) assigned by your provider.								
<b>Use Dynamic DNS</b>	Setting to <b>yes</b> (default: <b>no</b> ) activates Dynamic DNS and enables <b>Dynamic DNS Params</b> configuration. <b>Note:</b> To use this feature it is necessary to register with www.dyndns.org. Check with your provider whether usage of dynamic DNS is advisable when using a static address or an address that rarely changes. Note that when using static or rarely changing addresses dynamic DNS might not be appropriate as the address needs to change once a month.								
<b>Dynamic DNS Params</b>	Click the <b>Set ...</b> button to access the <b>Dynamic DNS Params</b> configuration section: <table border="1" data-bbox="212 1854 687 2112"> <tbody> <tr> <td><b>Service Type</b></td> <td>default: <b>DynamicDNS</b></td> </tr> <tr> <td><b>Dyndns Name</b></td> <td>Here the dyndns name that was registered at dyndns.org has to be entered.</td> </tr> <tr> <td><b>Secure Update</b></td> <td>This parameter defines whether HTTP (<b>no</b>) or HTTPS (default: <b>yes</b>) is used for updating.</td> </tr> <tr> <td><b>User Access ID</b></td> <td>User ID for accessing the server as defined during registration at dyndns.org.</td> </tr> </tbody> </table>	<b>Service Type</b>	default: <b>DynamicDNS</b>	<b>Dyndns Name</b>	Here the dyndns name that was registered at dyndns.org has to be entered.	<b>Secure Update</b>	This parameter defines whether HTTP ( <b>no</b> ) or HTTPS (default: <b>yes</b> ) is used for updating.	<b>User Access ID</b>	User ID for accessing the server as defined during registration at dyndns.org.
<b>Service Type</b>	default: <b>DynamicDNS</b>								
<b>Dyndns Name</b>	Here the dyndns name that was registered at dyndns.org has to be entered.								
<b>Secure Update</b>	This parameter defines whether HTTP ( <b>no</b> ) or HTTPS (default: <b>yes</b> ) is used for updating.								
<b>User Access ID</b>	User ID for accessing the server as defined during registration at dyndns.org.								

List 3-42 Network - xDSL configuration - section Authentication

Parameter	Description
<b>Access Password</b>	Password for accessing the server as defined during registration at dyndns.org.
<b>Wildcard Support</b>	Setting this parameter to <b>yes</b> (as it is per default) allows the resolution to sub-hostnames (regardless of the domain, the IP address pointed to is the same).
<b>MX Record</b>	This parameter specifies the mail handler ( <b>Mail eXchanger</b> ) for the given domain. MXs are used for directing mail to other servers than the one the hostname points to.
<b>Backup MX</b>	Setting this parameter to <b>yes</b> triggers that the configured <b>MX Record</b> works as a backup mail server. The registered <b>Dyndns Name</b> will be used as primary mail server. Setting the parameter to <b>no</b> induces that only the <b>MX Record</b> is used. <b>Note:</b> It is not recommended to use the MX parameters offered. If you have to, please consult <a href="http://www.dyndns.org">www.dyndns.org</a> for detailed information.
<b>Retry Time [mins]</b>	Standoff time in minutes until a new update try is started if the preceding one has failed.

List 3-43 Network - xDSL configuration - section Routing

Parameter	Description
	<b>Note:</b> For PPP multilink bundles the routing settings of the primary link are adopted for the bundled link. Routing settings of other non-primary link members are tacitly ignored.
<b>Own Routing Table</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  If set to <b>no</b> (default) routes will only be inserted into tables main or default. If set to <b>yes</b> policy routing will be used. With policy routing activated a new table named adsN (where N is the positional index of the section in the list of xDSL sections) is introduced to the main routing table. Routes are inserted into this table only unless <b>Clone Routes</b> (see below) is set to <b>yes</b> . All routes involving the xDSL link make use of this policy routing table. <b>Note:</b> If this parameter is set to <b>yes</b> , the only available <b>Monitoring Method</b> will be <b>LCP</b> .
<b>Use Assigned IP</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  When set to <b>yes</b> the IP address dynamically assigned by your Internet provider is used as source network for policy routing. Initially, until the ISP has successfully assigned an address, the rule will have 0.0.0.0 as a source address. The field is only active when <b>Own Routing Table</b> is used.
<b>Source Networks</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  Array of source networks or single hosts that will point to the policy routing table adsN. IP/mask notation is expected. For a single host supply "0" as its netmask. ( <b>Getting Started</b> - 5. phion Notation, page 25)
<b>Create Default Route</b>	If set to <b>yes</b> (default: <b>no</b> ) the default route assigned by the provider is automatically introduced. <b>Attention:</b> When set to yes in an environment where multiple dynamic links are available, configuring a <b>Route Preference Number</b> (see below) is mandatory
<b>Target Networks</b>	Target networks that are supposed to be reachable through this link.



**List 3-43** Network - xDSL configuration - section Routing

Parameter	Description
<b>Advertise Route</b>	If set to <b>yes</b> (default: <b>no</b> ) all routes will be advertised via Routing Protocols, provided an OSPF or RIP router service is active on the gateway.
<b>Interface Realm</b>	This parameter determines what kind of IP address is to be counted by the firewall for traffic on this interface ( <b>Licensing</b> - 6.5 Policy No. 5: General Case, page 510). The interface can be classified to one of the following: <b>unspec</b> <b>internal</b> <b>dmz</b> <b>external</b> (default)
<b>Route Preference Number</b>	Preference number or metric assigned to the routes to the specified target networks. You will need to set this parameter to a value larger than 0 if you wish to use your xDSL uplink as a backup connection (provider-failover) to the internet, for example.
<b>Clone Routes</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. <b>Note:</b> If set to <b>yes</b> all routes will be cloned from the table adslN to tables main or default (depending on the route target). This parameter is aiming at setups where application based selection (explicit binding in a firewall rule) of a traffic path is supposed to coexist with link failover (proxy dynamic).
<b>GRE with Assigned IP</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Set this parameter to <b>Yes</b> to register the assigned IP for IP protocol 47.

**List 3-44** Network - xDSL configuration - section Connection Monitoring

Parameter	Description
	For configuration details, see 2.2.5.8 Connection Monitoring of Dynamic Links, page 78.

**Section DHCP Client Setup**

The configuration allows the integration of a single cable connection (broadband or general assignment of addresses via a DHCP server). Cable connections are a very popular medium performance alternative to leased lines.

Cable connections are special in so far as they involve a dynamic component. The IP address is assigned via DHCP and will change from time to time. The phion implementation will only accept IP and gateway addresses from the DHCP server. All other assigned parameters or any static routes are silently dropped.

Since certain pieces of information are unknown at configuration time, the system will only request filling in the interface that will serve for link establishment as well as some routing information. An associated phion cable link management will automatically monitor the link and introduce routes, rules, and tables as soon as the missing information becomes available or changes. The system continuously monitors the link status and the reachability of a set of user-defined addresses. If required the link will be brought down and up again. This ensures that if there is a way to have the link up, it will be up.

By selecting **yes** for the entry **DHCP Enabled** the configuration areas for DHCP connections are activated.

The entry **Standby Mode** allows having high available DHCP/cable connections. Setting this parameter to **yes** implements two different working steps:

- The affected routes are set to pending state and it is not checked whether they are established.

- The configuration is completely run through but the connection is not yet established. Connecting is handled via a server-side script that is used for starting and stopping the connection with corresponding command lines:  

```
connection start: /etc/phion/dynconf/network/dhcrestart
connection stop: /etc/phion/bin/wipecable
```

 This way it is guaranteed that as soon as the server is up, the connection is established automatically, whereas when the server is shut down the connection is stopped automatically.

To open the configuration dialogue, set **DHCP Enabled** to **yes** and then click the **Insert** button.

**List 3-45** Networks - DHCP configuration

Parameter	Description
<b>Name</b>	This is the name of the DHCP link. <b>Note:</b> Only numbers and characters from the Latin character set excluding special characters are allowed in the link name.
<b>Link Active</b>	If set to <b>yes</b> the link is taken into account for link management, otherwise it is ignored.
<b>Standby Mode</b>	If set to <b>no</b> (default) the link is supposed to be activated and monitored as a consequence of a network activation. If set to <b>yes</b> , its activation and subsequent monitoring needs to be triggered externally.
<b>DHCP Connect Timeout</b>	Timeout for connection attempts [s] from configured <b>DHCP Links</b> to unreachable interfaces or networks.

**List 3-46** Networks - DHCP configuration - section Connection Details

Parameter	Description
<b>DHCP Interface</b>	Name of the ethernet interface connected to the cable modem. This interface is reserved for exclusive use by the cable link. No further IP addresses or networks may reside on it. The interface is renamed to <b>dhcp</b> and will accordingly be displayed in the control window.
<b>devmtu</b>	MTU setting of the selected DHCP interface.

**List 3-47** Networks - DHCP configuration - section DNS

Parameter	Description										
<b>Use Provider DNS</b>	Set to <b>yes</b> (default: <b>no</b> ) if you wish to use the DNS server(s) assigned by your provider.										
<b>Use Dynamic DNS</b>	Setting to <b>yes</b> (default: <b>no</b> ) activates Dynamic DNS and enables Dynamic DNS Params configuration. <b>Note:</b> To use this feature it is necessary to register with www.dyndns.org. Check with your provider whether usage of dynamic DNS is advisable when using a static address or an address that rarely changes. Note that when using static or rarely changing addresses dynamic DNS might not be appropriate as the address needs to change once a month.										
<b>Dynamic DNS Params</b>	This button provides the following parameters: <table border="1" data-bbox="1061 1697 1540 2101"> <tbody> <tr> <td><b>Dyndns Name</b></td> <td>Here the dyndns name that was registered at dyndns.org has to be entered.</td> </tr> <tr> <td><b>Secure Update</b></td> <td>This parameter defines whether HTTP (no) or HTTPs (default: yes) is used for updating.</td> </tr> <tr> <td><b>User Access ID</b></td> <td>User ID for accessing the server as defined during registration at dyndns.org.</td> </tr> <tr> <td><b>Access Password</b></td> <td>Password for accessing the server as defined during registration at dyndns.org.</td> </tr> <tr> <td><b>Wildcard Support</b></td> <td>Setting this parameter to <b>yes</b> (as it is per default) allows the resolution to sub-hostnames (regardless of the domain, the IP address pointed to is the same).</td> </tr> </tbody> </table>	<b>Dyndns Name</b>	Here the dyndns name that was registered at dyndns.org has to be entered.	<b>Secure Update</b>	This parameter defines whether HTTP (no) or HTTPs (default: yes) is used for updating.	<b>User Access ID</b>	User ID for accessing the server as defined during registration at dyndns.org.	<b>Access Password</b>	Password for accessing the server as defined during registration at dyndns.org.	<b>Wildcard Support</b>	Setting this parameter to <b>yes</b> (as it is per default) allows the resolution to sub-hostnames (regardless of the domain, the IP address pointed to is the same).
<b>Dyndns Name</b>	Here the dyndns name that was registered at dyndns.org has to be entered.										
<b>Secure Update</b>	This parameter defines whether HTTP (no) or HTTPs (default: yes) is used for updating.										
<b>User Access ID</b>	User ID for accessing the server as defined during registration at dyndns.org.										
<b>Access Password</b>	Password for accessing the server as defined during registration at dyndns.org.										
<b>Wildcard Support</b>	Setting this parameter to <b>yes</b> (as it is per default) allows the resolution to sub-hostnames (regardless of the domain, the IP address pointed to is the same).										

List 3-47 Networks - DHCP configuration - section DNS

Parameter	Description
<b>MX Record</b>	This parameter specifies the mail handler (Mail eXchanger) for the given domain. MXs are used for directing mail to other servers than the one the hostname points to.
<b>Backup MX</b>	Setting this parameter to yes triggers that the configured MX Record works as a backup mail server. The registered DynDNS Name will be used as primary mail server. Setting the parameter to no induces that only the MX Record is used. <b>Note:</b> It is not recommended to use the MX parameters offered. If you have to, please consult <a href="http://www.dyndns.org">www.dyndns.org</a> for detailed information.
<b>Retry Time [mins]</b>	Standoff time in minutes until a new update try is started if the preceding one has failed.

List 3-48 Networks - DHCP configuration - section Routing

Parameter	Description
<b>Own Routing Table</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  If set to <b>yes</b> policy routing will be activated. In the current context this means that a new table named <b>dhcp</b> is introduced after the main routing table. All routes involving the cable link (via interface dhcp) use these policy routes. <b>Note:</b> If this parameter is set to <b>yes</b> , the only available <b>Monitoring Method</b> will be <b>LCP</b> .
<b>Use Assigned IP</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  When set to yes the IP address dynamically assigned by your Internet provider is used as source network for policy routing. Initially, until the ISP has successfully assigned an address, the rule will have 0.0.0.0 as a source address. The field is only active when Own Routing Table is used.
<b>Source Networks</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  Array of source networks or single hosts which point to the policy routing table DHCP. IP/mask notation is expected. For a single host you supply "0" as its netmask. ( <b>Getting Started</b> - 5. phion Notation, page 25)
<b>Create Default Route</b>	If set to <b>yes</b> (default) the default route assigned by the provider is automatically introduced. <b>Attention:</b> When set to yes in an environment where multiple dynamic links are available, configuring a <b>Route Preference Number</b> (see below) is mandatory
<b>Target Networks</b>	Target networks that are supposed to be reachable through this link.
<b>Advertise Route</b>	If set to yes (default: no) all routes will be advertised via Routing Protocols, provided an OSPF or RIP router service is active on the gateway.
<b>Interface Realm</b>	This parameter determines what kind of IP address is to be counted by the firewall for traffic on this interface ( <b>Licensing</b> - 6.5 Policy No. 5: General Case, page 510). The interface can be classified to one of the following: <b>unspec</b> <b>internal</b> <b>dmz</b> <b>external</b> (default)
<b>Route Preference Number</b>	Preference number or metric assigned to the routes to the specified target networks. You will need to set this parameter to a value larger than 0 if you wish to use your low-cost cable uplink as a backup connection (provider-failover) to the internet, for example.

List 3-48 Networks - DHCP configuration - section Routing

Parameter	Description
<b>Clone Routes</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. <b>Note:</b> If set to <b>yes</b> all routes will be cloned from the table dhcp to tables main or default (depending on the route target). This parameter is aiming at setups where application based selection (explicit binding in a firewall rule) of a traffic path is supposed to coexist with link failover (proxy dynamic).
<b>GRE with Assigned IP</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  Set this parameter to <b>Yes</b> to register the assigned IP for IP protocol 47.

List 3-49 Networks - DHCP configuration - section Connection Monitoring

Parameter	Description
	For configuration details, see 2.2.5.8 Connection Monitoring of Dynamic Links, page 78.

### Section **ISDN Setup**

With this section it is possible to integrate a ISDN connection.

By selecting **yes** for the entry **ISDN Enabled** the configuration areas for ISDN connections are activated.

The entry **ISDN on Standby** allows having high available ISDN connections. Setting this parameter to **yes** implements two different working steps:

➤ The affected routes are set to pending state. It is not checked whether they are established.

➤ The configuration is completely run through but the connection is not yet established. Connecting is handled via a server-side script that is used for starting and stopping the connection with corresponding command lines:

```
connection start: /etc/phion/dynconf/network/isdnrestart
connection stop: /etc/phion/bin/wipeisdn
```

This way it is guaranteed that as soon as the server is up, the connection is established automatically, whereas when the server is shut down the connection is stopped automatically.

To open the configuration dialogue, click the **ISDN Settings > Set ...** button.

List 3-50 Networks - ISDN configuration - section Connection Details

Parameter	Description
<b>Provider Phone Number</b>	Insert the phone number here that has been assigned to you by your provider for connection establishment.
<b>Dial Out Prefix</b>	If needed, insert a dial out prefix here (optional).
<b>ISDN MSN</b>	Compared to a normal telephone connection an ISDN connection can have more than one phone number - each of these numbers is called MSN ( <b>M</b> ultiple <b>S</b> ubscriber <b>N</b> umber). If your provider has supplied you with a MSN number fill it into this field.
<b>ISDN Modem Card</b>	Select the name of the ISDN card you are using. <b>Note:</b> Please contact phion if you are using an unsupported ISDN card, which is not in the list.
<b>Encapsulation Mode</b>	The following modes are available: ➤ <b>SyncPPP</b> (default) bit oriented transfer protocol ➤ <b>RawIP</b> no PPP; IP addresses will have to be specified manually (attention: static)



**List 3-50** Networks - ISDN configuration - section Connection Details

Parameter	Description
<b>Dial Mode</b>	<p>Dialling can be handled in two ways:</p> <ul style="list-style-type: none"> <li>➤ <b>Dial-On-Demand</b> The ISDN subsystem connects itself to the provider only when there is traffic on the line. The connection is detached after an adjustable <b>Idle Hangup Time</b>. The advantage of automatic dialling is that on leased lines it may save money. The disadvantage on the other hand is that users connecting to systems externally (system administrators for example) cannot rely on the line being up all the time. <p><b>Note:</b> Do not use <b>Dial-On-Demand</b> mode on boxes managed by a management centre. Box management requires the link to be up incessantly.</p> <li>➤ <b>Always-On</b> The connection is initiated at startup of the box and is kept open all the time.</li> </li></ul>
<b>Idle Hangup Time</b>	When the <b>Dial Mode</b> is set to <b>Dial-On-Demand</b> , this field is used to specify after how many seconds the line will be disconnected when being idle.
<b>Use Channel Bonding</b>	<p>If set to <b>yes</b> (default: <b>no</b>) the ISDN subsystem will open a second ISDN channel to the provider when the first line is saturated, therefore doubling the bandwidth. After some time, when the traffic falls below a certain rate, the second line will be closed again.</p> <p><b>Note:</b> Your provider has to support channel bonding (=mppp).</p>
<b>Channel Bonding Settings</b>	<p>Use this section to adjust the way in on-demand bandwidth allocation works.</p> <ul style="list-style-type: none"> <li>➤ <b>Transfer Rate Limit [Bytes/s]</b> Limit for bringing up/down the slave channel depending. See Slave Channel Policy for bringing down the slave. Values range from 4000 Bytes/s to 7999 Bytes/s.</li> <li>➤ <b>Slave Channel Policy</b> Stay up policy for the slave channel, choose between <b>Stay Only Up While Transfer Limit Exceeded</b> and <b>Stay Permanently Up Till Hangup Timeout Reached</b></li> <li>➤ <b>Minimum Slave Uptime [s]</b> Minimum time the slave channel - once brought up - will unconditionally stay up. Values range from 1 s to 3600 s.</li> </ul>
<b>Dial Allowed From/Dial Allowed Until</b>	Use these lists to specify a time interval within which an ISDN dial-in is permissible. One interval valid for all days of the week may be specified. Temporal granularity is limited to 30 minutes.
<b>Dynamic Address Assignment</b>	When set to <b>yes</b> (default) the IP address/mask pair and the gateway address will be provided by the ISP dynamically. In case you are equipped with a static addresses, set the value to <b>no</b> and fill in a <b>Static IP/Mask</b> and <b>Static Gateway IP</b> below.
<b>Static IP/Mask</b>	If available define a static IP address/mask here.
<b>Static Gateway IP</b>	If a static IP/Mask is used define the gateway IP address here.

**List 3-51** Networks - ISDN configuration - section Compression

Parameter	Description
	In general you can leave the all compression settings <b>off</b> , which is the default. The ippp daemon will negotiate these settings in accordance with the PPP partners capabilities anyway.
<b>VJ TCP Header</b>	Negotiation of Van Jacobson style TCP/IP header compression.
<b>VJ Connection-ID</b>	When set to <b>off</b> the connection-ID compression in Van Jacobson style TCP/IP header is disabled. ipppd will neither omit the connection-ID byte from Van Jacobson compressed TCP/IP headers, nor ask the peer to do so.
<b>Address Control</b>	Address/Control compression.
<b>Protocol Field</b>	Protocol field compression.
<b>BSD</b>	BSD-Compress scheme.
<b>CCP Control Protocol</b>	Point to point compression protocol. Build upon the LCP protocol ( <b>Link Control Protocol</b> ).

**List 3-52** Networks - ISDN configuration - section Authentication

Parameter	Description
<b>User Access ID</b>	Insert the user ID here that has been assigned to you by your ISP.

**List 3-52** Networks - ISDN configuration - section Authentication

Parameter	Description
<b>User Access Sub-ID</b>	Insert an optional SUB-ID here if it has been assigned to you by your ISP. The User SUB-ID complements the User Access ID separated from it by a hash (#). Insert the SUB-ID without the hash as it will automatically be prefixed to it.
<b>Access Password</b>	Insert the password here that has been assigned to you by your ISP.
<b>Provider Name</b>	If required insert the name of your ISP here, which is supposed to be appended to your <b>User Access ID</b> .
<b>Authentication Method</b>	Select the method for authentication here. Authentication protocols can be set to <b>NONE</b> , <b>PAP</b> , <b>CHAP</b> or <b>PAP_or_CHAP</b> .
<b>Use Provider DNS</b>	Set to yes (default: no) if you wish to use the DNS server(s) assigned by your provider.
<b>Use Dynamic DNS</b>	Setting to yes (default: no) activates Dynamic DNS and enables Dynamic DNS Params configuration.
	<b>Note:</b> To use this feature it is necessary to register with www.dyndns.org. Check with your provider whether usage of dynamic DNS is advisable when using a static address or an address that rarely changes. Note that when using static or rarely changing addresses dynamic DNS might not be appropriate as the address needs to change once a month.
<b>Dynamic DNS Params</b>	Click the <b>Set ...</b> button to access the <b>Dynamic DNS Params</b> configuration section:
<b>Service Type</b>	default: <b>DynamicDNS</b>
<b>Dyndns Name</b>	Here the dyndns name that was registered at dyndns.org has to be entered.
<b>Secure Update</b>	This parameter defines whether HTTP (no) or HTTPs (default: yes) is used for updating.
<b>User Access ID</b>	User ID for accessing the server as defined during registration at dyndns.org.
<b>Access Password</b>	Password for accessing the server as defined during registration at dyndns.org.
<b>Wildcard Support</b>	Setting this parameter to yes (as it is per default) allows the resolution to sub-hostnames (regardless of the domain, the IP address pointed to is the same).
<b>MX Record</b>	This parameter specifies the mail handler (Mail eXchanger) for the given domain. MXs are used for directing mail to other servers than the one the hostname points to.
<b>Backup MX</b>	Setting this parameter to yes triggers that the configured MX Record works as a backup mail server. The registered Dyndns Name will be used as primary mail server. Setting the parameter to no induces that only the MX Record is used.
	<b>Note:</b> It is not recommended to use the MX parameters offered. If you have to, please consult www.dyndns.org for detailed information.
<b>Retry Time [mins]</b>	Standoff time in minutes until a new update try is started if the preceding one has failed.

**List 3-53** Networks - ISDN configuration - section Routing

Parameter	Description
	Normally routing is configured by the ISDN subsystem itself. You only have to supply the <b>Target Networks</b> . If your default route should be set dynamically when the ISDN connection is established, then you can add the entry 0.0.0.0/32 into the <b>Target Networks</b> field. Setting an own routing table is useful when you want to route single IP addresses or networks over the ISDN interface. The dialogue <b>Route Preference Number</b> lets you configure backup routes that can be activated when another connection type (for example xDSL, DHCP) fails.

List 3-53 Networks - ISDN configuration - section Routing

Parameter	Description
<b>Own Routing Table</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Specify the networks which should be routed by the ISDN interface. Set this value to <b>yes</b> to use own routing tables and subsequently define <b>Source Networks</b> below. If set to <b>no</b> all traffic to the target networks will be routed by this interface.</p> <p><b>Note:</b> If this parameter is set to <b>yes</b>, the only available <b>Monitoring Method</b> will be <b>LCP</b>.</p>
<b>Use Assigned IP</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>When set to <b>yes</b> the IP address dynamically assigned by your Internet provider is used as source network for policy routing. Initially, until the ISP has successfully assigned an address, the rule will have 0.0.0.0 as a source address. The field is only active when Own Routing Table is used.</p>
<b>Source Networks</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Add networks here that should be routed by the ISDN interface. IP/mask notation is expected (<b>Getting Started</b> - 5. phion Notation, page 25). For a single host use "0" as its netmask - for example 192.168.0.55/0.</p>
<b>Create Default Route</b>	<p>If set to <b>yes</b> (default) the default route assigned by the provider is automatically introduced.</p> <p><b>Attention:</b> When set to <b>yes</b> in an environment where multiple dynamic links are available, configuring a Route Preference Number (see below) is mandatory.</p>
<b>Target Networks</b>	Target networks that are supposed to be reachable through the ISDN interface. Note that this information is obligatory.
<b>Advertise Route</b>	If set to <b>yes</b> (default: <b>no</b> ) all routes will be advertised via Routing Protocols, provided an OSPF or RIP router service is active on the gateway.
<b>Interface Realm</b>	<p>This parameter determines what kind of IP address is to be counted by the firewall for traffic on this interface (<b>Licensing</b> - 6.5 Policy No. 5: General Case, page 510). The interface can be classified to one of the following:</p> <ul style="list-style-type: none"> <li>➤ <b>unspec</b></li> <li>➤ <b>internal</b></li> <li>➤ <b>dmz</b></li> <li>➤ <b>external</b> (default)</li> </ul>
<b>Route Preference Number</b>	You may specify a preference number to use the ISDN link in a multi-provider environment.
<b>Clone Routes</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>If set to <b>yes</b> the dynamic routes will be cloned to tables main or default (depending on the route target).</p> <p>This parameter is aiming at setups where application based selection (explicit binding in a firewall rule) of a traffic path is supposed to coexist with link failover (proxy dynamic).</p>
<b>GRE with Assigned IP</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Set this parameter to <b>Yes</b> to register the assigned IP for IP protocol 47.</p>

List 3-54 Networks - ISDN configuration - section Connection Monitoring

Parameter	Description
	For configuration details, see 2.2.5.8 Connection Monitoring of Dynamic Links, page 78.

## 2.2.5.7 UMTS

UMTS (Universal Mobile Telecommunications System) defines a mobile communication standard using the 3G specification in Europe. One UMTS card may be included into the network configuration of a netfence gateway.

List 3-55 Networks - UMTS configuration - section UMTS (3G) Setup

Parameter	Description
<b>UMTS Enabled</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables support for one UMTS card.
<b>Standby Mode</b>	If set to <b>no</b> (default) the link is supposed to be activated and monitored as a result of network activation. If set to <b>yes</b> its activation and subsequent monitoring needs to be triggered externally.
<b>Register in Standby</b>	This option allows for the registration of the card in the provider network even when <b>Standby Mode</b> is selected. This allows for a faster dial-in process when the link is fully activated.
	<p><b>Note:</b> Setting <b>Inbound SMS Handling</b> (see below) to <b>yes</b> will also lead to an immediate registration in the network.</p>

List 3-56 Networks - UMTS configuration - section UMTS Connection Details

Parameter	Description
<b>UMTS Modem Card</b>	Configure your UMTS card here.
	<p><b>Note:</b> Please consult the Hardware Compatibility List (HCL) available in Myphion area on <a href="http://www.phion.com">www.phion.com</a> for supported UMTS cards.</p>
<b>Modem Interface</b>	This parameter specifies the terminal interface associated with the UMTS Card. Typically, this is <b>noz0</b> for the card Option Globetrotter 3G+ - NZ and <b>ttyUSBO</b> for the other cards. Select checkbox <b>Other</b> to define another value.
<b>Active 2nd Channel</b>	Select <b>Yes</b> when you want to use the second modem channel.
	<p><b>Note:</b> For compatibility reason, please consult the Hardware Compatibility List (HCL) in Myphion area at <a href="http://www.phion.com">www.phion.com</a>. The entry in the HCL is called <b>SMS option</b>.</p>
<b>Radio Preference</b>	Choose the way how the modem connects to the radio network:
	<ul style="list-style-type: none"> <li>➤ <b>-- Not Applicable --</b></li> <li>➤ <b>GPRS/EDGE Preferred</b></li> <li>➤ <b>3G/UMTS Preferred</b></li> <li>➤ <b>GPRS/EDGE Only</b></li> <li>➤ <b>3G/UMTS Only</b></li> </ul>
<b>Inbound SMS Handling</b>	When set to <b>yes</b> (default: <b>no</b> ) the modem card will be polled at regular intervals for inbound SMS messages.
	Depending on the settings in the <b>SMS Control</b> tab (see 2.2.3.7 SMS Control, page 57), the SMS is either deleted right away or further processed. The respective log output goes into the log file <b>Auth &gt; SMS</b> .
<b>Speed [baud]</b>	This is the UMTS card's connection speed. Select a predefined default value from the pull-down menu or select the checkbox <b>Other</b> to define an individual value.
<b>Connect Timeout</b>	This value defines the period of time (in seconds) until a connection attempt is expected to have succeeded.
<b>Register Timeout</b>	The register timeout is the time in seconds that the box will wait for the network registration to be completed before actually dialling out.
	<p><b>Note:</b> Registration in standby will exactly avoid this waiting period thus speeding up the dial-out.</p> <p><b>Note:</b> The waiting period only applies to the first dial-out after a network configuration activation, restart, or boot. Subsequent dial-out will take place without a prior registration.</p>
<b>SIM PIN</b>	This is the SIM card's Personal Identification Number (PIN) usually consisting of four digits.
<b>APN Name</b>	Insert the <b>Access Point Name</b> (APN) for GPRS into this field.

**List 3-56** Networks - UMTS configuration - section UMTS Connection Details

Parameter	Description				
<b>PDP Context</b>	Click the <b>Set ...</b> button to access PDP Context configuration. This section allows for a more fine grained specification of the Packet Data Protocol (PDP) that is used for accessing the provider network.  <table border="1"> <tr> <td><b>Context Identifier</b></td> <td>Specify the numeric "Context Identifier" (CID).</td> </tr> <tr> <td><b>PDP Type</b></td> <td>Specify the PDP Type (<b>IP</b> or <b>PPP</b>).</td> </tr> </table> Usually the default values of <b>1</b> and <b>IP</b> , respectively, will suffice. If unsure, enquire with your provider.	<b>Context Identifier</b>	Specify the numeric "Context Identifier" (CID).	<b>PDP Type</b>	Specify the PDP Type ( <b>IP</b> or <b>PPP</b> ).
<b>Context Identifier</b>	Specify the numeric "Context Identifier" (CID).				
<b>PDP Type</b>	Specify the PDP Type ( <b>IP</b> or <b>PPP</b> ).				
<b>Phone Number</b>	This is the number the modem has to dial.  <b>Note:</b> The dialled number always needs to end with a hash (#), but this hash must not be inserted into this field.  <b>Note:</b> The last digit in the phone number is used to set the <b>Context Identifier</b> (see above). Note that when your provider does not assign you a number ending with "1", you will have to adapt the setting in the <b>PDP Context</b> section accordingly.				
<b>Allw Compression</b>	If set to <b>yes</b> the netfence box will agree to negotiate compression settings with the dial-in server. If set to <b>no</b> (default) compression is disabled.				

**List 3-57** Networks - UMTS configuration - section Authentication

Parameter	Description
<b>Authentication Method</b>	Select the method for authentication here. Authentication protocols can be set to <b>PAP</b> , <b>CHAP</b> (default) or <b>PAP_or_CHAP</b> .
<b>User Access ID</b>	This is the principal account name (PPP user name) assigned by the provider.
<b>Access Password</b>	This is the PPP password assigned by the ISP.
<b>Use Provider DNS</b>	Set to <b>yes</b> if you wish to use the DNS server(s) assigned by your provider.
<b>Use Dynamic DNS</b>	This parameter activates (default setting: <b>no</b> ) Dynamic DNS and enables the configuration of Dynamic DNS Params.  <b>Note:</b> To use this feature it is necessary to register with <a href="http://www.dyndns.org">www.dyndns.org</a> . Check with your provider whether usage of dynamic DNS is advisable when using a static address or an address that rarely changes. Note that when using static or rarely changing addresses dynamic DNS might not be appropriate as the address needs to change once a month.

**List 3-57** Networks - UMTS configuration - section Authentication

Parameter	Description																		
<b>Dynamic DNS Params</b>	Click the <b>Set</b> button to access the <b>Dynamic DNS Params</b> configuration section:  <table border="1"> <tr> <td><b>Service Type</b></td> <td>default: <b>DynamicDNS</b></td> </tr> <tr> <td><b>Dyndns Name</b></td> <td>Here the dyndns name that was registered at dyndns.org has to be entered.</td> </tr> <tr> <td><b>Secure Update</b></td> <td>This parameter defines whether HTTP (<b>no</b>) or HTTPs (default: <b>yes</b>) is used for updating.</td> </tr> <tr> <td><b>User Access ID</b></td> <td>User ID for accessing the server as defined during registration at dyndns.org.</td> </tr> <tr> <td><b>Access Password</b></td> <td>Password for accessing the server as defined during registration at dyndns.org.</td> </tr> <tr> <td><b>Wildcard Support</b></td> <td>Setting this parameter to <b>yes</b> (as it is per default) allows the resolution to sub-hostnames (regardless of the domain, the IP address pointed to is the same).</td> </tr> <tr> <td><b>MX Record</b></td> <td>This parameter specifies the mail handler (<b>Mail eXchanger</b>) for the given domain. MXs are used for directing mail to other servers than the one the hostname points to.</td> </tr> <tr> <td><b>Backup MX</b></td> <td>Setting this parameter to <b>yes</b> triggers that the configured <b>MX Record</b> works as a backup mail server. The registered <b>Dyndns Name</b> will be used as primary mail server. Setting the parameter to <b>no</b> induces that only the <b>MX Record</b> is used.   <b>Note:</b>            It is not recommended to use the MX parameters offered. If you have to, please consult <a href="http://www.dyndns.org">www.dyndns.org</a> for detailed information.         </td> </tr> <tr> <td><b>Retry Time [mins]</b></td> <td>Standoff time in minutes until a new update try is started if the preceding one has failed.</td> </tr> </table>	<b>Service Type</b>	default: <b>DynamicDNS</b>	<b>Dyndns Name</b>	Here the dyndns name that was registered at dyndns.org has to be entered.	<b>Secure Update</b>	This parameter defines whether HTTP ( <b>no</b> ) or HTTPs (default: <b>yes</b> ) is used for updating.	<b>User Access ID</b>	User ID for accessing the server as defined during registration at dyndns.org.	<b>Access Password</b>	Password for accessing the server as defined during registration at dyndns.org.	<b>Wildcard Support</b>	Setting this parameter to <b>yes</b> (as it is per default) allows the resolution to sub-hostnames (regardless of the domain, the IP address pointed to is the same).	<b>MX Record</b>	This parameter specifies the mail handler ( <b>Mail eXchanger</b> ) for the given domain. MXs are used for directing mail to other servers than the one the hostname points to.	<b>Backup MX</b>	Setting this parameter to <b>yes</b> triggers that the configured <b>MX Record</b> works as a backup mail server. The registered <b>Dyndns Name</b> will be used as primary mail server. Setting the parameter to <b>no</b> induces that only the <b>MX Record</b> is used.  <b>Note:</b> It is not recommended to use the MX parameters offered. If you have to, please consult <a href="http://www.dyndns.org">www.dyndns.org</a> for detailed information.	<b>Retry Time [mins]</b>	Standoff time in minutes until a new update try is started if the preceding one has failed.
<b>Service Type</b>	default: <b>DynamicDNS</b>																		
<b>Dyndns Name</b>	Here the dyndns name that was registered at dyndns.org has to be entered.																		
<b>Secure Update</b>	This parameter defines whether HTTP ( <b>no</b> ) or HTTPs (default: <b>yes</b> ) is used for updating.																		
<b>User Access ID</b>	User ID for accessing the server as defined during registration at dyndns.org.																		
<b>Access Password</b>	Password for accessing the server as defined during registration at dyndns.org.																		
<b>Wildcard Support</b>	Setting this parameter to <b>yes</b> (as it is per default) allows the resolution to sub-hostnames (regardless of the domain, the IP address pointed to is the same).																		
<b>MX Record</b>	This parameter specifies the mail handler ( <b>Mail eXchanger</b> ) for the given domain. MXs are used for directing mail to other servers than the one the hostname points to.																		
<b>Backup MX</b>	Setting this parameter to <b>yes</b> triggers that the configured <b>MX Record</b> works as a backup mail server. The registered <b>Dyndns Name</b> will be used as primary mail server. Setting the parameter to <b>no</b> induces that only the <b>MX Record</b> is used.  <b>Note:</b> It is not recommended to use the MX parameters offered. If you have to, please consult <a href="http://www.dyndns.org">www.dyndns.org</a> for detailed information.																		
<b>Retry Time [mins]</b>	Standoff time in minutes until a new update try is started if the preceding one has failed.																		

**List 3-58** Networks - UMTS configuration - section Routing

Parameter	Description
<b>Own Routing Table</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  If set to <b>no</b> (default) routes will only be inserted into tables main or default. If set to <b>yes</b> policy routing will be used. With policy routing activated a new table named <b>umts1</b> is introduced to the main routing table. Routes are inserted into this table only unless Clone Routes (see below) is set to <b>yes</b> . All routes involving the UMTS link make use of this policy routing table.  <b>Note:</b> If this parameter is set to <b>yes</b> , the only available <b>Monitoring Method</b> will be <b>LCP</b> .
<b>Use Assigned IP</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  When set to <b>yes</b> the IP address dynamically assigned by your Internet provider is used as source network for policy routing. Initially, until the ISP has successfully assigned an address, the rule will have 0.0.0.0 as a source address. The field is only active when <b>Own Routing Table</b> is used.
<b>Source Networks</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  Array of source networks or single hosts that will point to the policy routing table <b>umts1</b> . IP/mask notation is expected. For a single host supply "0" as its netmask. ( <b>Getting Started</b> - 5. phion Notation, page 25)
<b>Create Default Route</b>	If set to <b>yes</b> (default) the default route assigned by the provider is automatically introduced.  <b>Attention:</b> When set to <b>yes</b> in an environment where multiple dynamic links are available, configuring a Route Preference Number (see below) is mandatory.

List 3-58 Networks - UMTS configuration - section Routing

Parameter	Description
<b>Target Networks</b>	Target networks that are supposed to be reachable through this link.
<b>Remote Peer IP</b>	Use this override mechanism if your provider does not assign a remote gateway IP.
<b>Advertise Route</b>	If set to <b>yes</b> (default: <b>no</b> ) all routes will be advertised via Routing Protocols, provided an OSPF or RIP router service is active on the gateway.
<b>Interface Realm</b>	This parameter determines what kind of IP address is to be counted by the firewall for traffic on this interface ( <b>Licensing</b> - 6.5 Policy No. 5: General Case, page 510). The interface can be classified to one of the following: <ul style="list-style-type: none"> <li>➤ <b>unspec</b></li> <li>➤ <b>internal</b></li> <li>➤ <b>dmz</b></li> <li>➤ <b>external</b> (default)</li> </ul>
<b>Route Preference Number</b>	Preference number or metric assigned to the routes to the specified target networks. You will need to set this parameter to a value larger than 0 if you wish to use your UMTS uplink as a backup connection (provider-failover) to the internet, for example.
<b>Clone Routes</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. <b>Note:</b> If set to <b>yes</b> all routes will be cloned from the table umts1 to tables main or default (depending on the route target). This parameter is aiming at setups where application based selection (explicit binding in a firewall rule) of a traffic path is supposed to coexist with link failover (proxy dynamic).
<b>GRE with Assigned IP</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Set this parameter to <b>Yes</b> to register the assigned IP for IP protocol 47.

List 3-59 Networks - UMTS configuration - section Connection Monitoring

Parameter	Description
	For configuration details, see 2.2.5.8 Connection Monitoring of Dynamic Links.

### 2.2.5.8 Connection Monitoring of Dynamic Links

Connection monitoring options allow specifying a list of IP addresses that must be reachable through the dynamical xDSL, DHCP, ISDN or UMTS link. If these addresses are not pingable the network subsystem will be restarted and error messages will be reported in the log file.

#### Note:

For PPP multilink bundles in xDSL configurations the connection monitoring settings of the primary link are adopted for the bundled link. Monitoring settings of other non-primary link members are tacitly ignored.

List 3-60 Connection monitoring of dynamic links - section Connection Monitoring

Parameter	Description
<b>Log Level</b>	Set to <b>debug</b> (default: <b>standard</b> ) in case you encounter configuration problems and temporarily need verbose log files.

List 3-60 Connection monitoring of dynamic links - section Connection Monitoring

Parameter	Description
<b>Monitoring Method</b>	Selects the method adopted for link quality assessment. <ul style="list-style-type: none"> <li>➤ By selecting <b>ICMP</b> the reachable IP addresses (set in parameter <b>Reachable IPs</b>) are probed first. If there is no response the gateways are probed.</li> <li>➤ If the Internet provider does not allow pings, the monitoring method has to be set to <b>LCP</b>. The Dial-In daemon is then probed directly.</li> <li>➤ By selecting <b>StrictLCP</b> absolutely no ICMP probing occurs.</li> </ul> <b>Note:</b> <b>ICMP</b> is not available when parameter <b>Own Routing Table</b> is set to <b>yes</b> . <b>Note:</b> <b>LCP</b> checks are automatically performed by the pppd according to the LCP parameterisation below. <b>Note:</b> The DHCP link monitoring method is ICMP by default and therefore not customisable. <b>Note:</b> Regardless of the monitoring method which is set, the monitoring of the gateway-IP is not affected (for example: if LCP for monitoring method is chosen it does not prevent the gateway-IP from being pinged).
<b>Reachable IPs</b>	Probing target IP addresses that are pinged in order to see whether the link is still functioning or not. At least one single IP address that is meant to be accessible only via the xDSL link has to be specified. Each of the specified IPs is pinged every 20 seconds (2 ICMP packets each). If none of the IPs responds the remote end of the PPP-connection to the ISP is checked. In case of no response the link is dismantled and it is attempted to re-establish it.
<b>LCP Check Interval</b>	Time between two successive LCP echo checks.
<b>No. of LCP Checks</b>	Number of successive failed LCP echo checks before the PPP connection is terminated by the local pppd.
<b>No. of ICMP Probes</b>	Number of ICMP echo requests sent to each probing target IP address (maximum value: 9, default: 2).
<b>Waiting Period [s/probe]</b>	Number of seconds per probe that a reply is waited for.
<b>Check Interval [s]</b>	The time between two successive link state assessments.
<b>Failure Standoff[s]</b>	The time to wait immediately after a failed link establishment before trying to connect again. The idea here is that blunt retrying usually does not improve the situation but rather leads to vast amounts of unwanted log output.

#### Note:

For further information on monitoring mechanisms refer to 2.2.5.12 Further Reading: Probing Policies and Mechanisms, page 80.

### 2.2.5.9 IP Tunnelling

#### IP Tunnelling

#### Note:

The following parameters are only available in **Advanced View** mode.

This section allows the introduction of simple point-to-point tunnels using generic routing or plain IP in IP encapsulation.

#### Note:

If you wish to establish a secure tunnel between two firewalls you should rather make use of a VPN tunnel.

The box-based tunnels you may configure here do neither offer peer authentication nor encryption support. Especially in conjunction with high availability (HA)

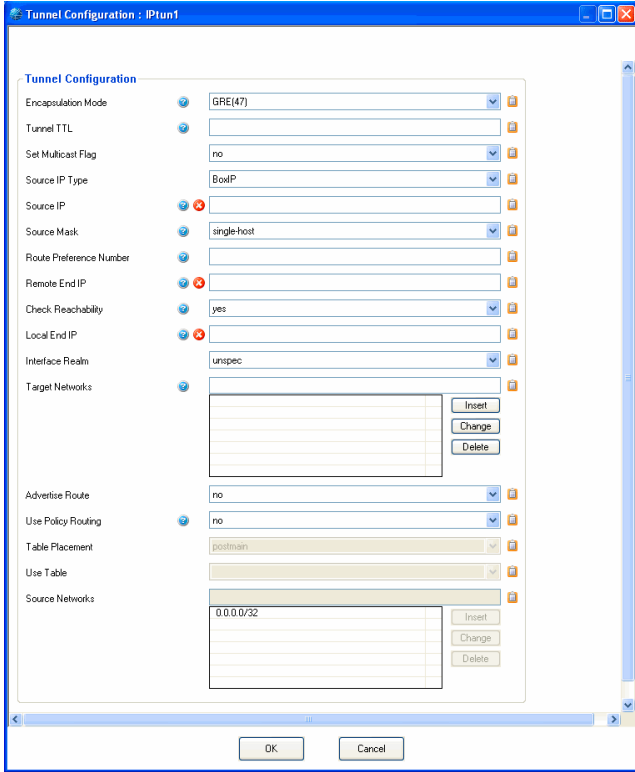


systems a VPN tunnel will offer significant benefits as it is attached to a server and not to a box.

Moreover, if you wish to establish a tunnel hub (which means a box sustaining many tunnels, each with a different peer) a VPN server will turn out to be a much better choice.

To open the configuration dialogue, click the *Insert* button.

Fig. 3-31 IP Tunnels configuration



List 3-61 Networks - IP Tunnels configuration - section Tunnel Configuration

Parameter	Description
<b>Encapsulation Mode</b>	Choose the type of encapsulation. Default setting is <b>GRE(47)</b> (Generic Routing Encapsulation). Alternatively there is support for plain IP in IP encapsulation ( <b>IPinIP(4)</b> ).
<b>Tunnel TTL</b>	This optional parameter allows setting the TTL for encapsulated tunnel traffic. Leaving this field blank corresponds to the hitherto standard behaviour of TTL inherit and Nopmtudisc (no path MTU discovery).
<b>Set Multicast Flag</b>	If set to <b>yes</b> (default: <b>no</b> ) the multicast flag will be set for the tunnel interface.
<b>Source IP Type</b>	Select the type of source IP here. Available values are ServerIP and BoxIP (default). If ServerIP is selected no source IP has to be specified as the IP will be provided by a server. If BoxIP is selected a local source IP address has to be specified (see below). <b>Note:</b> In absence of a local source IP the box itself cannot use the tunnel for local traffic.
<b>Source IP</b>	Specify a routable source address if the box itself is meant to use the tunnel. The IP is activated on the tunnel interface.
<b>Source Mask</b>	Enter the source IPs' netmask here. A non-zero mask specifies a local network.

List 3-61 Networks - IP Tunnels configuration - section Tunnel Configuration

Parameter	Description
<b>Route Preference Number</b>	Preference number of this route. Use only when two routes to the same target exist. Assigning a route preference number only makes sense under the following premises. You do not wish to use policy routing for tunnelling thus the respective tunnel routes go either into table main or default (in the case the target needs to be network 0.0.0.0/32). You wish to use policy routing but plan to assign the routes to an already existing table. In both cases the preference will only have an effect if there exists another route to one of the specified target networks. As mentioned in the preceding section it is not sensible to introduce redundant routes to a target net with a direct route being the preferred path.
<b>Remote End IP</b>	IP address of the remote tunnel end. Guarantee, that the routing setup allows accessing this address from the local tunnel end, which means with source address as specified in <b>Local End IP</b> .
<b>Check Reachability</b>	If set to <b>yes</b> (as it is by default) a check is performed whether the remote tunnel end is directly reachable from the local end IP. If this check fails the tunnel is not introduced, if verification is active already a <b>Send Changes</b> will fail. Setting this parameter to <b>no</b> disables this check. Select <b>no</b> when the remote tunnel end is only accessible via a VPN route.
<b>Local End IP</b>	IP address of local tunnel end. <b>Note:</b> This address must already exist. In particular it must correspond to one of the addresses introduced in a network related section.
<b>Interface Realm</b>	This parameter determines what kind of IP address is to be counted by the firewall for traffic on this interface ( <b>Licensing</b> - 6.5 Policy No. 5: General Case, page 510). The interface can be classified to one of the following: <b>unspec</b> (default) <b>internal</b> <b>dmz</b> <b>external</b>
<b>Target Networks</b>	Array of IP/mask pairs that are meant to be accessible through the tunnel. They are thus target networks of routes that rely on the existence of the tunnel interface. Each specified target will rely on a corresponding direct route.
<b>Advertise Route</b>	If set to <b>yes</b> (default: <b>no</b> ) all routes will be advertised via Routing Protocols, provided an OSPF or RIP router service is active on the gateway.
<b>Use Policy Routing</b>	Select <b>yes</b> to activate a source filter for the tunnel routes. If set to <b>yes</b> the three policy routing related entries below will be activated.
<b>Table Placement</b>	Controls placement of the table. Choose between the default setting <b>postmain</b> , and the advanced options <b>premain</b> and <b>existing</b> . The latter allows referencing an already existing table. The rule preference of this table will be inherited.
<b>Use Table</b>	<b>Note:</b> Only enabled when <b>Table Placement</b> has been set to <b>existing</b> . Allows you to specify an existing policy routing table to which the tunnel routes are added. For each source network defined an appropriate rule pointing to this very table (with the table's original preference) is also appended. Do not use the tables local, main or default in this parameter.
<b>Source Networks</b>	Array of source networks or single hosts for which a yet to be defined policy routing table is looked up. <b>Note:</b> By default the name of the table would be identical to the name of the tunnel section entry. You may however assign the routes to another already existing table. IP/mask notation is expected. For a single host you will have to supply "0" as its netmask. ( <b>Getting Started</b> - 5. phion Notation, page 25)

### 2.2.5.10 Integrity Check

The Integrity check performs a logical test on the network configuration.

List 3-62 Integrity Check configuration - section Integrity Check Settings

Parameter	Description
<b>Consistency Verification</b>	(default: <i>Always</i> ) <i>Box-Only</i> <i>Never</i>
<b>Include Server IPs</b>	(default: <i>yes</i> ) <i>no</i>

### 2.2.5.11 Special Needs

**Note:**

The following parameters are only available in **Advanced View** mode.

#### Section *User Scripts*

The **Special Needs** section is provided to satisfy rare network-related demands that are difficult to cover with standardised configuration settings. This part of the configuration clearly addresses the well-versed system administrator. Section instances of this type allow specifying bash2-conform user-defined commands. The integration of these command sections into the graphical user interface has several significant advantages. There is no need to alter any of the standard utilities required to bring up the networking subsystem thus software updates are not an issue. Modifications to the way in which networking is brought up are kept track of and may not easily be forgotten.

At the very same time such a user-interface has the potential to wreak havoc on your system as all commands are run with super user privileges. Therefore use only with due care.

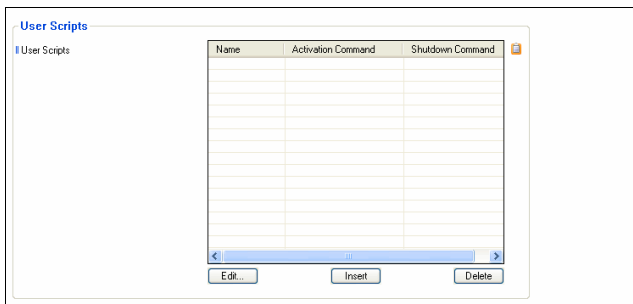
**Note:**

phion recommends to input only commands that have previously been tested on the command line and which are guaranteed to produce the desired results.

Please do not use this as a personal playground.

To open the configuration dialogue, click the **Insert** button:

Fig. 3-32 Special Needs configuration



For example, we have labelled the section **spec**. The activation command resets the maximum transmission unit of tokenring interface tr0 to 1400 bytes (the default value is 2000 bytes). The shutdown command has intentionally been left blank.

Note that the full path must be given (for example /usr/bin/, /sbin/, ...)

In the section instance list the presence of a command will only be indicated by a string reading either `-set-` or `-not set-`. This is due to the potentially significant length of the individual commands.

### 2.2.5.12 Further Reading: Probing Policies and Mechanisms

#### ➤ **Monitoring Method: ICMP**

Before probing actually commences the existence of a meaningful address assignment on the associated ppp-interface (ppp1-4) is checked for. If no meaningful assignment is found the link is deemed dead and no further probing is required.

Only if the address assignment appears correct the actual probing takes place. If ICMP has been chosen as monitoring method the configured reachable IPs are probed first. If at least one reachable IP has been specified and an echo reply is received, then the link is deemed functional.

In case no reachable IPs have been specified (which is not smart) or none of the addresses specified have replied, the probing continues with the gateway address assigned by the ISP.

If then this gateway address replies to an ICMP echo request the link is deemed functional.

If the gateway address does not reply then the link is deemed inoperative and is shut down.

#### ➤ **Monitoring Method: LCP**

For probing policy LCP the ICMP ISP gateway check (which is performed as final step with ICMP selected as monitoring method) is also carried out but its result is interpreted in a different way. If the gateway does not respond no further check is attempted and the current probing failure is ignored. However, if the gateway responds further regular probing is carried out. Should one of these then fail in the future the link will be deemed inoperative and will be shut down.

#### ➤ **Monitoring Engine Changes**

The executable used to start and monitor all ADSL connections is now called `/epb/openxDSL`.

The executable **openxDSL** has three distinctively different operation modes. These are called **daemon**, **signal**, and **worker**.

List 3-63 The monitoring executable openxDSL and its commands

Command	Operation Mode	Description
<code>/epb/openxDSL</code>	daemon	All configured links in non-standby mode are activated and monitored. The executable becomes a daemon and detaches from the controlling terminal. The daemon starts a separate worker process for each xDSL link or link bundle.
<code>/epb/openxDSL void</code>	deamon	Same as above but runs in foreground, which means the daemon does not detach.
<code>/epb/openxDSL stop</code> <code>/start/restart</code>	signal	Instructs a running daemon process to stop (= block), start or restart all running worker processes (links or bundled links).



**List 3-63** The monitoring executable openxDSL and its commands

Command	Operation Mode	Description
/epb/openxDSL stop /start/restart <names>	signal	Same as above but only stops/starts/restarts the links associated with the supplied section names.  <b>Note:</b> Names of non-primary multilink members are no valid arguments. You may only stop, start or restart the link as a whole. Use the name or the primary link member to do so.
/epb/xDSL[1-4] -> /epb/openxDSL	worker	When invoked as xDSL[n] the same executable openxDSL behaves differently, for example as a worker starting up a particular link or link bundle. The integer n denotes the list position of the link in the list of xDSL section entries. Note that this index also determines the used ppp[n]-interface.

Beyond this an auxiliary cleanup utility called /epb/wipexDSL is provided.

A process list output for a link bundle with two pptp connections maintained by an xDSL- worker:

**Fig. 3-33** Process list output for a link bundle

```
|--openxDSL (29801) --sleep (30144)
|   `--xDSL (29829) --sleep (30137)
|
|--xDSL (29876) ---xDSL (29881) ---pppd_xDSL.0 (29882) ---pptp_xDSL.0 (29883) [link handler]
|
| `--xDSL (30089) ---xDSL (30094) ---pppd_xDSL.1 (30097) ---pptp_xDSL.1 (30098) link handler]
|
|--pptp_xDSL.0 (29885) [pptp call manager for primary link ]
```

Note that each worker forks at least one link handler (with identical name) which in turn starts a pppd daemon. The individual pppd-processes and their forked pptp or pppoe transport handlers have distinct names which allow tracing them back to the worker and link handler.

**➤ File Locations**

The xDSL implementation writes all volatile temporary data (pid-files, state-files ...) into

/var/phion/run/boxnet/xDSL. Data-files required at runtime which only change as a consequence of a full network configuration activation are written into /var/phion/config/boxnet/xDSL. The idea behind this separation is to easily facilitate the migration to a flash-RAM-based appliance platform, where /var/phion/run may be linked against a directory in a RAM-disk.

**Fig. 3-34** Listing of /var/phion/run/boxnet/xDSL

```
prw-r--r-- 1 root root 0 Aug 24 16:26 fifo_xDSL.0
prw-r--r-- 1 root root 0 Aug 24 16:05 fifo_xDSL.1
lrwxrwxrwx 1 root root 14 Aug 19 11:48 pppd_xDSL.0 -> /usr/sbin/pppd
lrwxrwxrwx 1 root root 14 Aug 19 11:48 pptp_xDSL.0 -> /usr/sbin/pptp
-rw-r--r-- 1 root root 4 Aug 24 16:26 xDSL.0.state
-rw-r--r-- 1 root root 4 Aug 24 16:24 xDSL.1.state
lrwxrwxrwx 1 root root 38 Aug 10 13:23 xDSL_master -> /var/phion/run/boxnet/xDSL/xDSL.0.pid
```

**Fig. 3-35** Listing of /var/phion/config/boxnet/xDSL

```
-rwx----- 1 root root 1230 Aug 23 10:31 ip-up.xDSL
lrwxrwxrwx 1 root root 44 Aug 23 10:31 xDSL -> /var/phion/config/boxnet/xDSL/xDSL_PPTP_ppp1
-rw----- 1 root root 0 Aug 23 10:31 xDSL_reachips
-rw----- 1 root root 0 Aug 23 10:31 xDSL_reachips.last
-rw----- 1 root root 100 Aug 23 10:31 xDSL.opconf
-rw----- 1 root root 100 Aug 23 10:31 xDSL.opconf.now
-rw----- 1 root root 504 Aug 24 16:23 xDSL_PPTP_ppp1
```

## 2.2.6 Traffic Shaping

**Note:**  
Hardware based on i386 compatible CPUs does not provide the functions required for traffic shaping. Thus traffic shaping does not work on i386 kernels. Enter `rpm -q kernel --qf %{ARCH}\\n` on the command line to find out which kernel is present.

### 2.2.6.1 Enterprise Shaping

This design satisfies the requirements necessary for executing any of the following application schemes:

- **Data Traffic Classification**  
Important traffic is distinguished from unimportant data traffic.
- **Prioritisation**  
Important traffic is given preferential treatment (either more bandwidth and/or lower latency).
- **Bandwidth Partition**  
Certain types of traffic are not allowed to exceed a bandwidth limit.
- **Network Overflow Protection**  
Prohibits protocols not having a flow control mechanism from congesting the network.
- **Dynamically Adjusted Shaping**  
Shaping is adjusted according to dynamic parameters like daytime or download volume.
- **Shaping of VPN Transports**  
Shaping may not only be used for physical network interfaces but also for VPN transports.

When implementing traffic shaping, one distinguishes between traffic classification and shaping enforcement: The results of traffic classification are used as input for shaping enforcement in order to implement a shaping policy.

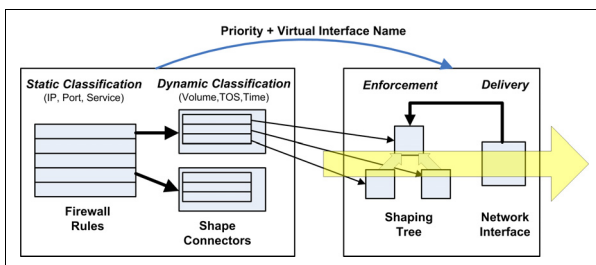
- **Static Classification**  
Network traffic may be classified according to configurable conditions. Since the **firewall rule set** is already used to classify network traffic regarding security, we also use the rule set to classify network traffic for traffic shaping. It is therefore possible to treat network traffic for certain services (for example http, ftp, ...) as well as traffic originating from certain IP source/destination addresses differently.
- **Dynamic Classification**  
Since the firewall rule set is only consulted during session initiation we call the above classification "static classification". Once the session is initiated the classification performed by the rule set does not change. In order to also handle dynamic parameters like daytime or download volume, which vary during the

session lifetime, we add an element called **shaping connector** to the concept. These shaping connectors (described in more detail later on) take the dynamic parameters of a network session into account and allow taking shaping decisions accordingly.

### ➤ Enforcement

Once traffic is classified, traffic shaping enforcement has to take place. The shaping enforcement is performed by processing network data before it is delivered to a network interface (**outbound shaping**) or after it is received by a network interface (**inbound shaping**). The enforcement is realised by delaying (queuing) or even discarding network traffic according to the present bandwidth utilisation status using the results of traffic classification. To implement this enforcement we make use of a tree of **virtual interfaces (virtual tree)**, which may be attached to network interfaces indicating that traffic shaping is intended.

Fig. 3-36 Enterprise Shaping - Enforcement



### ➤ Virtual Interface

The active element of traffic shaping is called the 'Virtual Interface'. As its name implies, the virtual interface involves a non-physical (abstract) network adapter. Data is transmitted over a virtual interface and, depending on the settings, is systematically transmitted onwards.

The most important characteristics of a virtual interface are:

- a limiting bandwidth and
- a priority weighting (high, medium or low).

The bandwidth limit specifies the maximum amount of data rate available for the virtual interface. If the virtual interface is congested (more data arrives than the bandwidth limit allows), the priority weighting determines how the available bandwidth will be partitioned according to individual priorities. Partitioning is never static. In other words, if all available traffic has a low priority, it will be assigned the whole bandwidth. The **Weighted Random Early Drop (WRED)** queue management algorithm is used for prioritisation.

### ➤ Virtual Tree

Virtual trees are constructed of a root virtual interface, which may be attached to a real network interface and an arbitrary number of sub nodes forming a tree. The output of any number of virtual interfaces can be fed into the input of a super ordinate virtual interface. Each and every virtual interface of a virtual tree can be configured individually. Virtual trees are built as templates and will only operatively perform traffic

shaping when they are referred to by a physical network interface.

This way the same virtual tree can be reused for several physical network interfaces. As a consequence of this re-usage, the limiting bandwidth rates are configured in relative numbers (percent), which become absolute values when assigning a physical network interface with absolute bandwidth values. When assigning virtual trees to physical network interfaces, it is possible to decide if inbound and/or outbound traffic should be performed by the traffic shaping mechanism. With the assignment the effective rates (in- and outbound) of the physical network interfaces are specified. Note that these rates do not have to be identical with the rate the interface is capable of, but should rather specify the expected effective bandwidth (for example 2 MBit Provider Line accessed over a 100Mbit Ethernet interface)

### ➤ Shaping connector

Virtual interfaces, their associated virtual trees, and the active elements of data flow modelling are based on the presupposition that the data has already been classified. This classification is the role of the **shaping connector**. As its name suggests, the shaping connector is responsible for the connection between the rule-based static classification (session) and traffic shaping. Not only do shaping connectors evaluate and prioritise traffic (high, medium or low), they also specify the name of the virtual interface into which the data is fed. Ultimately, the virtual interface is selected according to the session's routing information. This information is used to define the network interface or VPN transport, then determines whether a virtual tree exists for the designated virtual interface. The shaping connector has its own set of rules that accommodate the dynamic character. These rules are evaluated as soon as the session starts and are continually re-evaluated throughout the session's entire duration. The rules evaluate the following characteristics: an IP packet's TOS (type of service), current data volume for the associated session, and absolute time domain within the period of one week. The goal of these rules is to prioritise traffic and decide where the data should be sent to. Due to its dynamic character, completely different shaping schemes can be used over the course of one single session.

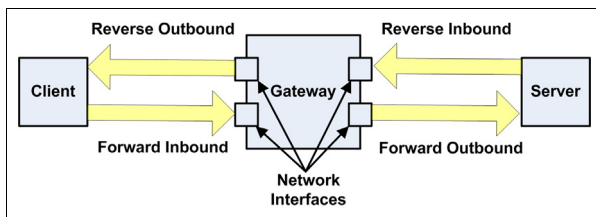
Since shaping connectors do not completely identify the virtual interface (they only specify the name of the linked network interface), it is possible to construct routing-dependent traffic shaping schemes (different shaping schemes for the Internet connection in normal and fallback (ISDN) operation).

### ➤ Firewall Rule Parameter

In order to use a shape connector it must be referred to in a firewall rule. When selecting shape connectors (formerly called "bands" for the old traffic shaping) one can distinguish between the forward and the reverse direction. The forward direction is defined by traffic generated by the session initiator (client) and the reverse direction by traffic generated by the responder (server). As shown in figure 3-37 we have four different

traffic types. For each type shaping may be enabled/disabled or configured differently.

**Fig. 3-37** Enterprise Shaping - Firewall Rule Parameter



The following steps should be taken to configure traffic shaping:

**Prerequisites (configurative)**

- Create a virtual tree template.
- Assign the template to a network interface and specify a maximum bandwidth for outbound and/or inbound traffic. Not specifying a bandwidth implies no in- or outbound shaping.
- Create one or more shaping connectors which point to virtual interface names according to the specified conditions.
- Refer to the shaping connector in firewall rule advanced settings for forward and/or reverse traffic.

**Operating sequence**

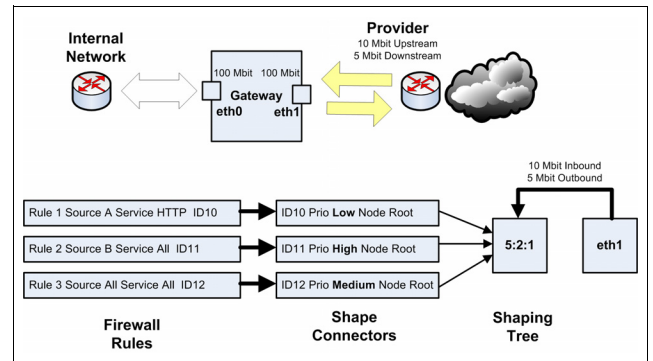
- The session is constructed according to a firewall rule and the configured rule shaping connectors (forward and reverse) are registered for the session.

Once this is completed, every packet is processed:

- The associated shaping connectors are determined according to packet direction (forward or reverse).
- The shaping connector rules, which are conditions on TOS, daytime and data volume, are evaluated, resulting in a **priority** and a **virtual interface name**.
- Packet routing is evaluated (**input** and **output interface** are determined).
- If the resulting interface (inbound shaping applies to input interfaces and outbound shaping applies to outbound interfaces) has a virtual tree attached, the result of the shaping connector rules is used to assign a virtual interface by name. In case no virtual interface with this name exists but the physical interface has a virtual tree assigned, the root node of the virtual tree is assigned by default.
- If a virtual interface is assigned, traffic is not delivered immediately but diverted to the assigned virtual interface first. It must traverse through the shaping tree (shaping enforcement), where it might be propagated, delayed, or even discarded depending on the available bandwidth and queues fill status.
- Traffic with no virtual interface assigned is processed immediately.

**Example 1:** Simple traffic prioritisation

**Fig. 3-38** Enterprise Shaping - Example 1: Simple traffic prioritisation



The following goals should be achieved:

- Traffic is classified according to the source IP and network service into three types, which should be prioritise with the ratio 5:2:1 (high:medium:low).

**Configuration for Example 1:**

A virtual tree consisting of a single virtual interface with a partition priority of 5:2:1. Three shaping connectors, where one results in a high, one in a medium and one in a low priority selection, all pointing to the root node (note: we have only one node to point to anyway). A firewall rule set that exists of three rules, each referring to one of the three shaping connectors. And finally a physical network device, where we expect network traffic to be delivered with the virtual tree attached to it.

For this simple setup we observe the following behaviour:

- The configured total in and outbound bandwidth is never exceeded.
- The three types (low, medium and high) of network traffic share the bandwidth. Should not all three types of traffic be in operation, the total bandwidth is divided amongst the available traffic according to the partition priority. If the preset bandwidth limit is not reached, traffic shaping does not take place and there is no prioritisation.

**Note:**

Prioritisation only occurs when the available bandwidth is insufficient.

Since all three types of traffic operate on the same limiting unit datagram delivery latency of a specific traffic type will highly depend on the amount of traffic of the other types, since they share the same datagram queue.

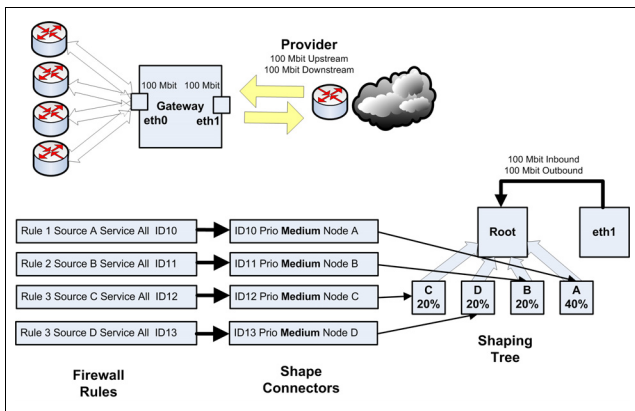
- The prescribed priority partition is an estimated ratio, which is more likely to be exact the more network traffic is sent (See note on TCP traffic, page 85).

**Example 2:** ISP customer bandwidth assignment

Assume an ISP with an internet access providing a total bandwidth of 100 Mbits. The bandwidth should be assigned to 4 customers, where one should get 40 Mbits and the other three 20 bits each. The assigned bandwidth of each

customer should not be exceeded even if the total bandwidth is not saturated.

**Fig. 3-39** Enterprise Shaping - Example 2: ISP customer bandwidth assignment



### Configuration for Example 2:

A virtual tree consisting of a virtual root interface and four subnodes (A-D) with a limiting bandwidth of 40 % (one) and 20 % (three). Four shaping connectors where each one results in medium priority selection (unimportant for this example) and points to each one of the sub nodes. A firewall rule set that exists of four rules each referring to one of the four shaping connectors. And finally a physical network device where we expect network traffic to be delivered with the virtual tree attached to it.

For this example we observe the following behaviour:

- The total bandwidth (sum over all customers) is never exceeded.
- The available per customer bandwidth is never exceeded. There is no bandwidth borrowing between customers (nodes).
- The setup can be extended by introducing more than one shaping connector per customer with varying priorities.

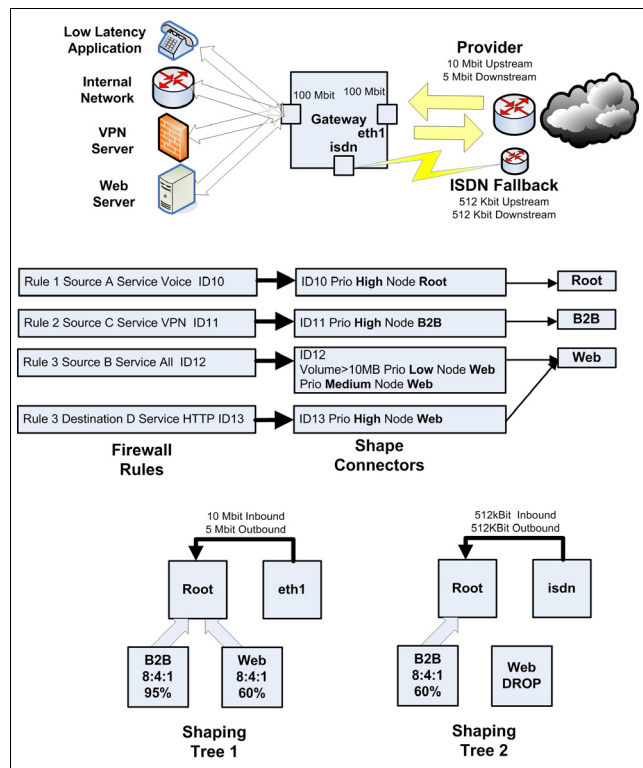
### Example 3: Advanced traffic shaping

The advanced traffic shaping example makes use of the prioritisation of example 1 and the bandwidth assignment of example 2. Furthermore, the dynamic parameters of the session download volume is taken into account in order to demonstrate the purpose of the shaping connector rules. The setup describes an internet gateway which services:

- An application which needs low delivery latency (for VoIP for example).
- Internet access from the internal network (mainly HTTP web traffic).
- VPN traffic over the internet.
- Web access from the internet (Web Shop).

- Multiprovider setup with a fallback ISDN line (bundled to 512 kbit). ISDN fallback is implemented with redundant network routes.

**Fig. 3-40** Enterprise Shaping - Example 3: Advanced traffic shaping



From this setup we expect the following:

- Low latency delivery for the VoIP application. This is achieved by feeding the VoIP traffic directly into the root node, whereas other traffic has to pass either the "B2B" or "Web" node first, where they are queued (delayed) if bandwidth saturation occurs. This way the VoIP traffic may even overtake the traffic waiting in the **Web** or **B2B** queues.
- A minimum of 40 % of the internet bandwidth for VPN traffic. By limiting the **Web** node to 60 % we guarantee that the **B2B** node will get at least 40 % of the available bandwidth (Assuming that the amount of VoIP traffic is negligible).
- High priority treatment for Web access from the internet (Web Shop).
- Medium priority treatment for Web access from the internal network to the internet.
- Low priority treatment for downloads from the internal network which are larger than 10 MB.
- For ISDN Fallback operation (Provider Failure) deliver only the VPN and the VoIP application traffic. This is achieved by setting the **Web** node for the ISDN tree to



operate in **Drop Mode**. This way the ISDN line is protected against unwanted web traffic.

**Note:**  
**TCP traffic**

The TCP protocol uses a flow control mechanism to throttle the rate at which it is sending data. Since traffic shaping interferes with the packet delivery (packet delaying or discarding) it will affect the TCP flow control mechanism. Ideally, the TCP flow control will reduce its flow rate to an amount where the shaping mechanism is no longer forced to discard packets. This is only possible if the traffic shaping mechanism can delay packets long enough that the TCP flow control "detects" a smaller bandwidth by measuring longer RTTs (round trip times). A longer delay involves larger queue sizes that should be considered when configuring virtual interface nodes. Also long delays result into larger latency values, which might be unwanted for other protocols. Therefore, in the case of mixed TCP and other protocol traffic, one might consider using separate traffic shaping nodes for TCP with different queue size settings.

It is also the TCP flow control mechanism which makes the priority weights approximate values. Assume we have 20 TCP sessions, where 10 are classified as high and 10 are classified as medium priority, all trying to get the maximum bandwidth possible. If we configured a ratio of 1:2 for the two priorities we will indeed observe this ratio when measuring the output for the two priorities. But if we change to setup to 1 high priority TCP session and 39 medium TCP sessions the result will change. In fact we will see that the single TCP session gets less bandwidth than we expected. The reason is simply that the flow control mechanism of the 39 TCP sessions generates more traffic while trying to find its optimum rate than the single high priority session. So if you know beforehand that you want to favour a small number of TCP sessions over a large number of unprivileged TCP sessions you should anticipate a larger ratio in order to get the wanted output ratio.

**Traffic Shaping Configuration:**

To configure virtual trees, go to the dialogue **Box > Traffic Shaping > Virtual Shaping Trees**, lower window:

**Fig. 3-41** Traffic Shaping Settings - Virtual Shaping Trees

Virtual Shaping Trees	Shaping Connectors	Legacy Shaping
Interface/VFN/Transport	Assigned Tree	Rate Outbound / Rate Inbound
eth1	normal	10 MB/s / 10 MB/s

Virtual Tree	Virtual Interface	Rate	Priority Weights	Priority Adjustment	Mode	Queue Size
normal	root	100%	4 : 2 : 1	0	shape	0
	internet	40%	4 : 2 : 1	0	shape	0
	vpn	100%	4 : 2 : 1	0	drop	0

Commands on the context menu:

**Table 3-9** Traffic Shaping Settings - Virtual Tree commands

Command	Description
Add new virtual tree	Create a new virtual tree.
Add new virtual interface	Create a new virtual interface for the selected virtual tree.
Copy virtual tree	Copy a selected virtual tree and give it another name.
Remove virtual tree	Delete a selected virtual tree

**Table 3-9** Traffic Shaping Settings - Virtual Tree commands

Command	Description
Remove virtual interface	Delete a selected virtual interface.

The dialogue box for creating a new virtual tree:

**Fig. 3-42** Traffic Shaping Settings - dialogue box Virtual Device

The dialog box 'Virtual Device' contains the following fields:

- Tree Name: normal
- Device Name: root
- Outbound (traffic being sent over the device):
  - Operation Mode: Shape
  - Assumed Rate: 100 Percent 100%
  - Priority Weights: H 4 M 2 L 1
  - Priority Adjustment: 0 Leave Priority Unchanged
  - Queue Size (Bytes): 0 (0 default)
- Inbound (traffic received by the device):
  - Operation Mode: As-Outbound
  - Assumed Rate: 100 Percent 100%
  - Priority Weights: H 4 M 2 L 1
  - Priority Adjustment: 0 Leave Priority Unchanged
  - Queue Size (ms): 0 (0 default)

**List 3-64** Traffic Shaping configuration

Parameter	Description
<b>Tree Name</b>	The name of the virtual tree.
<b>Device Name</b>	The name of the virtual interface.

**List 3-65** Traffic Shaping configuration - section Outbound (traffic sent over the device)

Parameter	Description
<b>Operation Mode</b>	Choose the operational mode for the root virtual interface from the following possibilities: <ul style="list-style-type: none"> <li>➤ <b>Shape</b> The virtual interface limits traffic according to the settings.</li> <li>➤ <b>Passthrough</b> Every packet received is immediately passed to the next tree node or to the associated network interface.</li> <li>➤ <b>Drop</b> Every packet received is immediately discarded.</li> </ul>
<b>Assumed Rate</b>	This is the limiting bandwidth for the virtual interface. The rate is specified relatively in percent and becomes an absolute value as soon as a physical interface is assigned to a virtual tree. <p><b>Note:</b> Do not produce very low values (lower than 64 kbit).</p> <p><b>Note:</b> The assignment uses effective interface rates rather than physical line speeds.</p> <p><b>Note:</b> When using decimals be sure to use a period (.) as separator.</p>
<b>Priority Weights</b>	The relative weight of the three priorities high (H), medium (M) or low (L). These weights specify the ratio of the traffic being propagated by a virtual node assuming that the input traffic is evenly distributed among the three priorities.
<b>Priority Adjustment</b>	When a datagram is passed to the next node in the tree its priority may be adjusted before processing is continued. This way packets may be treated with high priority in one node and with medium or even low priority in the next node.
<b>Queue Size (Bytes)</b>	Size of the virtual interface's internal queue (in bytes). If set at '0', a suitable value is calculated for the virtual interface rate. If not using the default value note that small queue sizes imply low latencies and large queue sizes imply better TCP handling.

**List 3-66** Traffic Shaping configuration - section Inbound (traffic received by device)

Parameter	Description
	The parameters may be configured explicitly (asymmetric case) for the inbound mode or, if selected, the inbound configuration parameters are taken from the outbound configuration (symmetric case).

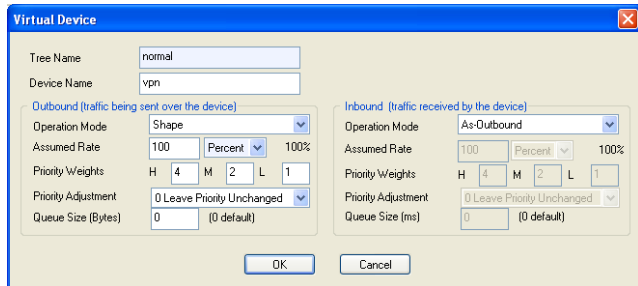
**List 3-66** Traffic Shaping configuration - section Inbound (traffic received by device)

Parameter	Description
<b>Operation Mode</b>	Choose the operational mode from the following possibilities: ↗ <b>As-Outbound</b> ↗ <b>Shape</b> . The virtual interface limits traffic according to the settings. ↗ <b>Passthrough</b> . Every packet received is immediately passed to the next tree node or to the associated network interface. ↗ <b>Drop</b> . Every packet received is immediately discarded.
<b>Assumed Rate</b>	See section <b>Outbound</b> .
<b>Priority Weights</b>	See section <b>Outbound</b> .
<b>Priority Adjustment</b>	See section <b>Outbound</b> .
<b>Queue Size (Bytes)</b>	See section <b>Outbound</b> .

A new virtual interface can be created on the subordinate level of an existing virtual interface. Choose an existing virtual interface (which means Virtual Tree Root Virtual Interface) and select **Add new virtual interface**.

The dialogue box for creating a new virtual interface:

**Fig. 3-43** Traffic Shaping Settings - dialogue box, new virtual interface



**Note:**

For Parameter description see list 3-64, page 85, list 3-65 and list 3-66.

To assign a virtual tree to a physical interface, go to the dialogue **Box > Traffic Shaping > Virtual Shaping Trees** and open the context menu.

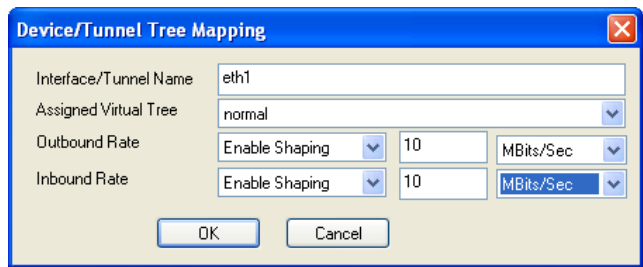
The following commands are available:

**Table 3-10** Traffic Shaping Settings - Interface commands

Command	Description
Add new interface/tunnel	Assign a virtual tree to a physical interface.
Edit/Show	Change an existing physical interface assignment.
Remove Interface/Tunnel	Delete an existing physical interface assignment.

To configure a physical interface assignment, use the following dialogue box:

**Fig. 3-44** Traffic Shaping Settings - dialogue box Device/Tunnel Tree Mapping

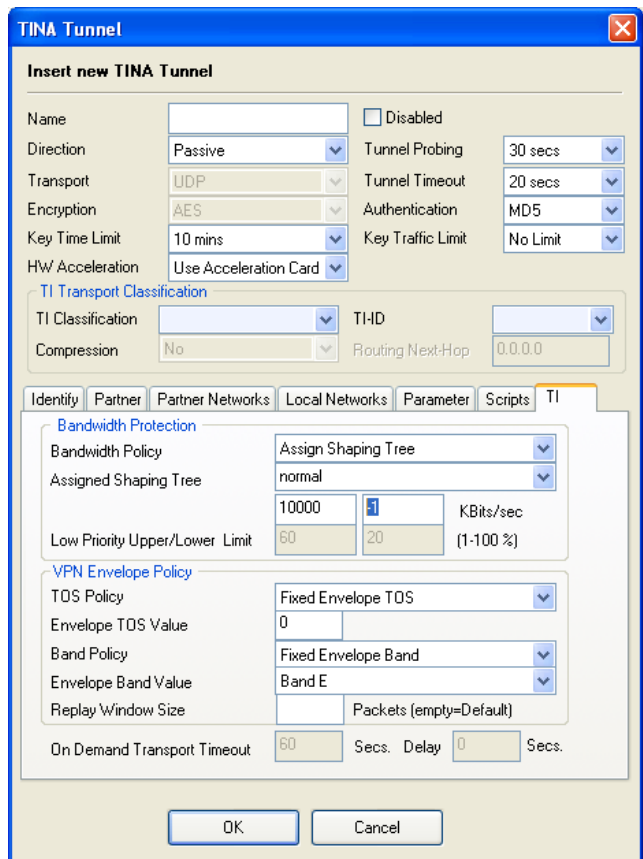


**List 3-67** Device/Tunnel Tree Mapping

Parameter	Description
<b>Interface / Tunnel Name</b>	Specify the name of the physical interface (for example eth1).
<b>Assigned Virtual Tree</b>	Specify the virtual tree which should be assigned to the network interface.
<b>Outbound Rate</b>	Specify the effective outbound rate of the physical interface. <b>Note:</b> This may differ from the rate the physical interface is capable. (Internet provider access using a 100 Mbit interface but only 10 Mbit are effectively available).
<b>Inbound Rate</b>	Specify the effective inbound rate of the physical interface.

For VPN transports, virtual trees are assigned in the TI settings of the VPN transport.

**Fig. 3-45** Traffic Shaping Settings - dialogue box TINA Tunnel



To carry out the assignment, choose the option **Assign Shaping Tree** found in the **Bandwidth Policy** parameter. The maximum bandwidth is defined using the following two fields:



- Maximum rate of outbound traffic [kbit/s]
- Maximum rate of inbound traffic [kbit/s]

AO (zero) rate indicates no shaping.  
 A inbound rate of -1 indicates outbound and inbound rate being the same.

To define and edit shaping connectors, choose dialogue **Box > Traffic Shaping > Shaping Connectors**, upper window.

**Fig. 3-46** Traffic Shaping Settings - Shaping Connectors

ID	Name	Priority	Virtual Interface	TOS	Traffic-Limit (KB)	Time-Period	Weekday/Hour
10	VPN	High	vpn				
11	internet	High	internet		2048		
		Low	internet				

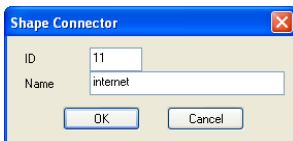
The following commands are available:

**Table 3-11** Traffic Shaping Settings - Shaping connector commands

Command	Description
Add new connector	Create a new shaping connector.
Remove connector	Delete an existing shaping connector and all its associated rules.
Append new connector rule	Add a new connector rule. The new rule will be appended at the bottom of the existing list of rules for the selected shaping connector.
Remove connector rule	Delete a connector rule from the list of rules for the selected shaping connector.
Move connector rule down	Move the selected connector rule back a position.
Move connector rule up	Move the selected connector rule forward a position.

To create or change a shaping connector, go to the following dialogue box:

**Fig. 3-47** Traffic Shaping Settings - dialogue box Shape connector

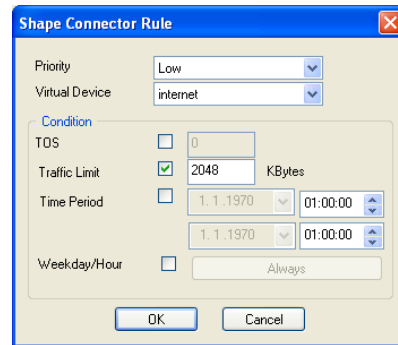


**List 3-68** Traffic Shaping configuration - Shaping connector

Parameter	Description
<b>ID</b>	The shaping connector's index number. For legacy purposes the index numbers 1 to 8 correspond to Band Sys and Band A-G as used for the old traffic shaping. This way existing firewall rules which use the old traffic shaping bands may be migrated to the new traffic shaping.
<b>Name</b>	Give the shaping connector a name.

To edit connector rules, use the following dialogue box:

**Fig. 3-48** Traffic Shaping Settings - dialogue box Shape Connector Rule



**List 3-69** Shape Connector Rule

Parameter	Description
<b>Priority</b>	Defines the data packet's priority (high, medium, low) should the rule apply. This is the priority at which the packet will eventually be fed into the virtual interface
<b>Virtual Device</b>	The name of the virtual interface into which the data packet will be fed, should this rule apply.

**List 3-70** Shape Connector Rule - section Condition

Parameter	Description
<b>TOS</b>	Indicates that the TOS in the IP header must match the specified value.
<b>Traffic Limit</b>	Indicates that network sessions must not exceed the specified amount of data being sent.
<b>Time Period</b>	Indicates an absolute time span during which this rule applies.
<b>Weekday/Hour</b>	Defines the hours of the week during which this rule applies.

**Realtime Information**

Realtime information of the traffic shaping mechanism is shown in the operative firewall GUI (Shaping). The provided information shows all physical interfaces or VPN transports with an assigned virtual tree. For each tree node traffic information is provided.

**Fig. 3-49** Realtime Information - Shaping

Interface	Dir	VirtualIF	Rate-Max	Rate-Sum	Rate-H	Rate-M	Rate-L	Sessions	Bytes	Packets	Drops	
eth0	Out	root	1.3 M	13.8 K	13.8 K	0	0	0 (1)	717.5 K	0	12.5 K	0
	Out	internet	512.0 K	13.8 K	13.8 K	0	0	1 (1)	717.5 K	0	12.5 K	0
eth0	Out	vpn	1.3 M	0	0	0	0	0 (0)	0	0	0	0
	In	root	1.3 M	496.5 K	496.5 K	0	0	0 (1)	26.5 M	0	18.2 K	0
eth0	In	internet	512.0 K	493.6 K	493.6 K	0	0	1 (1)	26.5 M	0	18.2 K	0
	In	vpn	1.3 M	0	0	0	0	0 (0)	0	0	0	0

The individual columns contain the following information.

**Table 3-12** Realtime Information - Shaping

Column	Description
<b>Interface</b>	The physical network interface or VPN transport
<b>Dir</b>	Shaping Direction (In ... Inbound ; Out ... Outbound)
<b>VirtualIF</b>	The name of the virtual interface. Here the hierarchy of the virtual tree is presented in a typical tree structure.
<b>Rate-Max</b>	The maximum bandwidth available for each virtual interface.
<b>Rate-Sum</b>	The actual utilised bandwidth of the virtual interface. (Sum over all priorities)
<b>Rate-H</b>	The actual traffic rate of the three priorities (high, medium, low)
<b>Rate-M</b>	
<b>Rate-L</b>	
<b>Sessions</b>	The number of active sessions operating on the virtual interface. The first number indicates the number of sessions directly fed into this virtual interface.
<b>Bytes</b>	Number of bytes propagated by the virtual interface.

**Table 3-12** Realtime Information - Shaping

Column	Description
Packets	Number of packets propagated by the virtual interface
Drops	Number of drops on the virtual interface due to shaping.

The following commands can be found in the context menu:

**Table 3-13** Realtime Information - Shaping commands

Command	Description
Reset Interface Statistics	Resets all the virtual trees statistics.
Show Interface Configuration	Provides information on the effective values operating on the virtual interface. Shows the actual maximum rate and selected values for the size of internal queues. This command is also accessible by double-clicking on one of the virtual interfaces.

### 2.2.6.2 Legacy Shaping

The traffic shaping file contains the configuration settings for bandwidth management. Shaping is performed by classifying the traffic into one of the 8 available shaping bands:

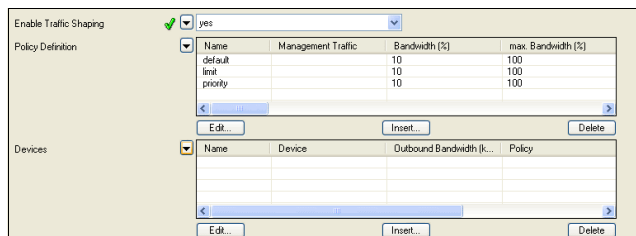
#### ➤ **Band A to G**

#### ➤ **System Traffic (Management Traffic)**

The firewall rules define to which band traffic is assigned. The classification of the traffic can be monitored in the **Status** tab of the firewall service..

#### **Attention:**

When planning the deployment of traffic shaping take the CPU resources of the traffic shaping equipment into consideration. Especially on low-end machines the shaping process on links with high utilisation can cause performance degradation, resulting in high CPU loads and reduced network connectivity. Depending on the system configuration, phion recommends a maximum interface shaping bandwidth of 10Mbits/s on systems with a CPU clock of 800MHz or lower.

**Fig. 3-50** Config Section - Traffic Shaping**List 3-71** Traffic Shaping configuration

Parameter	Description
<b>Enable Traffic Shaping</b>	This option can be used to quickly enable or disable the traffic shaping subsystem. For the convenience of the system administrator it is still possible to edit the traffic shaping configuration while the subsystem is disabled. The default setting is <b>no</b> .

**List 3-72** Traffic Shaping configuration - section Policy Definition

Parameter	Description
	This list contains the shaping policies that can be assigned to the shaping enabled interfaces. The policy defines how the different shaping bands are processed by the network queuing mechanism.

**List 3-72** Traffic Shaping configuration - section Policy Definition

Parameter	Description
<b>Management Traffic</b>	The management traffic is a class that is reserved for traffic, which is generated by the network management protocols of the netfence gateway. It can be used to ensure that a minimum of bandwidth is available for the management protocols. This bandwidth is not lost when it is not fully used up by the management protocols, but instead the other bands may use the otherwise idle link to extend their bandwidth. This "borrowing" of bandwidth can also be restricted by the <b>Max. Bandwidth</b> setting, which allows you to set a maximum bandwidth share for a single traffic band. Management traffic is different from the traffic from the other bands. Instead of getting a relative share from the total available bandwidth, the management band rates are calculated in absolute numbers. So a setting of 10 % bandwidth means that 10 % of the total interface bandwidth is reserved for management. The rest of the bandwidth, as well as the bandwidth that was not used up by management, is available to the A, B and C bands. If these bands do not exhaust the full capacity of the link, the rest can be used by the management traffic up to its "max. Bandwidth" setting, which is 100 % by default.
<b>Band A to G</b>	These seven bandwidth classes can be used to classify the network traffic of any given network individually. The classification can be done by the firewall rule set or manually in the "Status" tab of the firewall. The A-G traffic bands share their bandwidth in the relation of their bandwidth settings. A maximum setting may also be defined to limit the total traffic bandwidth of any band. The share that is not consumed by the A-G bands is available to the managed traffic until its maximum share limit is exhausted.
<b>Bandwidth (%)</b>	The bandwidth defines the share of the total traffic that is available to a band. When there is still bandwidth available after every band has claimed its share, then additional resources can be used until the link is fully utilised.
<b>Max. Bandwidth (%)</b>	The maximum bandwidth defines an upper limit of traffic bandwidth that may be used by a band. Any band is not allowed to exceed its limit.

**List 3-73** Traffic Shaping configuration - section Devices

Parameter	Description
	The interfaces that are going to be used by the traffic queuing must be listed here. The total bandwidth that is available for the inbound and outbound traffic has to be entered here.
<b>Device</b>	This is the network interface that should be used for application of the shaping policy. Only static interfaces may be used (eth0, tr1, ...). Network interfaces that establish the network connection dynamically (for example, ppp0) may not be entered here. In these cases the symbolic names <b>DYNAMIC_adsl</b> should be used for ADSL connections and <b>DYNAMIC_isdn</b> should be used for ISDN connections
<b>Outbound Bandwidth (kbit)</b>	The outbound bandwidth defines the maximum bandwidth in kbit that may be utilised by network traffic. This can also be used for setting a maximum egress traffic limit on the given interface.
<b>Policy</b>	The policy of the interface defines how the bands share the available network bandwidth.
<b>Enable Inbound Shaping</b>	If this option is set to <b>yes</b> the shaping mechanism is also applied to inbound traffic. The same traffic policy, which is used for outbound traffic, is then also used for inbound traffic.
<b>Inbound Bandwidth (kbit)</b>	The inbound bandwidth defines the maximum inbound bandwidth in kbit that may be utilised by network traffic. This can also be used for setting a maximum ingress traffic limit on the given interface. If this field is left blank, the same bandwidth setting is used that was defined in the entry <b>Outbound Bandwidth (in kbit)</b> .

### Calculation of Bandwidth Settings

The main purpose of traffic shaping is to confine the maximum available network bandwidth an application may utilise, in order to guarantee full functionality and availability of another application with higher priority. Moreover, traffic shaping can be used to limit the speed of network connections.

### Bandwidth Calculation

Regarding the interaction between traffic shaping parameters, the following applies:

➤ **Bandwidth percentage settings:**

In the configuration dialogue of the **Policy Definition**, bandwidth settings have to be configured only for effective bands. Settings of ineffective bands will be ignored until those bands are activated in a rule set.

➤ **Calculation of Traffic Shaping quotas:**

Two variants exist how Traffic Shaping quotas can be calculated (in the example, an interface bandwidth of 1 Mbit/s is assumed):

#### 1. Calculation by ratio

This calculation method is the easiest way to keep overview of the configured settings. In Variant 1 a defined absolute share is first assigned to Management Traffic, the remaining interface bandwidth is then assumed to match 100 %. In the example, 10 % of the total available interface bandwidth is assigned to Management Traffic. The settings of the other bands (excluding Management Traffic settings) are then configured to equal 100 %. The bandwidth calculation is thus based on a remaining total bandwidth of 900 kbit/s instead of 1 Mbit/s.

**Table 3-14** Bandwidth calculation by ratio

Band	Bandwidth Setting	Ratio	Available Interface Bandwidth
Management Traffic	10 / 100	10 % of total interface bandwidth 1 Mbit/s	100 kbit/s
Band A	40 / 100	40 % of total bandwidth remainder 900 kbit/s	360 kbit/s
Band B	60 / 100	60 % of total bandwidth remainder 900 kbit/s	540 kbit/s

#### 2. Calculation by total percentage

The settings in Variant 2 lead to the same result. The sum of all bandwidth settings is configured not to exceed 100 %. Keep in mind that the bandwidth setting for Management Traffic takes a special position, as it is calculated as absolute share from the total available interface bandwidth.

In the example, 10 % of the interface bandwidth are assigned to Management Traffic, 36 % and 54 % respectively are assigned to Bands A and B.

**Table 3-15** Bandwidth calculation by total percentage

Band	Bandwidth Setting	Ratio	Available Interface Bandwidth
Management Traffic	10 / 100	10 % of total interface bandwidth 1 Mbit/s	100 kbit/s
Band A	36 / 100	36 % of total bandwidth 1 Mbit/s	360 kbit/s
Band B	54 / 100	54 % of total bandwidth 1 Mbit/s	540 kbit/s

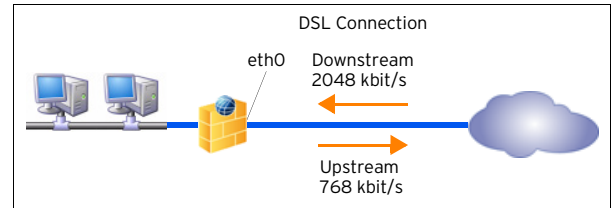
### Example Configurations for Traffic Shaping

The following traffic shaping scenarios are imaginable:

➤ **Example 1**

A company network is connected to the Internet with DSL through an exclusive interface (transfer rates 2048 kbit/s downstream, 768 kbit/s upstream). The aim is to guarantee bandwidth for Remote Desktop connections running beside other common Internet applications.

**Fig. 3-51** Traffic Shaping scenario 1 - Bandwidth configuration for inbound and outbound connections



**Note:**

In setups where only one traffic-shaping interface is involved, both, inbound and outbound bandwidth, have to be configured, as outbound traffic arrives at the gateway without prioritisation.

#### Step 1

Configure a Forwarding Firewall Rule Set allowing DSL connections from the company network to the Internet for common Internet applications. Assign a **Band** to the Rule Set in the **Parameter Section** of the Edit/Create Rule configuration window. By default **Band A** is preselected. If Traffic Shaping is not enabled, the Band selection is nothing more than an unused parameter in the configuration. As soon as Traffic Shaping is enabled, the selected Band comes into effect.

#### Step 2

Configure a Forwarding Firewall Rule Set allowing Remote Desktop connections over the DSL interface. Assign a **Band** to the Rule Set in the **Parameter Section** of the Edit/Create Rule configuration window. In the example, usage of **Band B** is assumed.

#### Step 3

On the box browse to **Config > Box > Traffic Shaping**. Enable **Traffic Shaping** by setting the parameter of the same name to **yes**.

#### Step 4

Define a shaping policy through parameter **Policy Definition**. The following policy would suit the needs:

**Table 3-16** Example 1 - Policy Definition configuration

Parameter	Description
Policy Name	dsconnection
Management Traffic	Ratio: bandwidth 0 % / maximum bandwidth 0 %
Band A	70 / 100
Band B	30 / 100
Band C - Band G	0 / 0

**Note:**

Settings for **Band C** to **Band G** may as well be left at the default setting 100 / 100. As long as the Bands are not allotted, the settings are ignored.

**Step 5**

Assign policy dslconnection to an interface through parameter **Devices**. The following configuration settings apply:

**Table 3-17** Example 1 - Interfaces configuration

Parameter	Description
Name	dslconnection
Outbound Bandwidth (kbit)	768 (upstream)
Interface	eth0
Policy	dslconnection
Enable Inbound Shaping	yes
Inbound Bandwidth (kbit)	2048 (downstream)

Through the configured settings, the following effective values apply:

**Band A: 70 / 100**

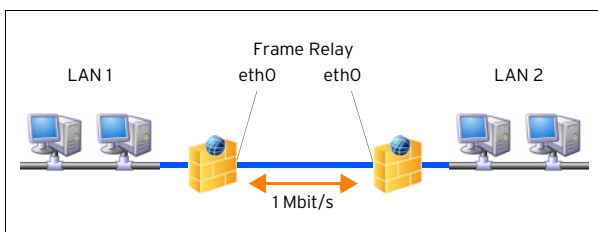
Band A may use 70 % out of available 2048 kbit/s downstream and 768 kbit/s upstream, that is 1433.6 kbit/s and 537.6 kbit/s, respectively. If Band B does not claim its share, it may use all available bandwidth up to 100 % of the total amount.

**Band B: 30 / 100**

Band B may use 30 % out of available 2048 kbit/s downstream and 768 kbit/s upstream, that is 614.4 kbit/s and 230.4 kbit/s, respectively. If Band A does not claim its share, it may use all available bandwidth up to 100 % of the total amount.

**Example 2**

A company network spans two locations, which continuously perform common tasks such as browsing the Internet, sharing files, utilising terminal sessions, and so on. The two locations are connected via Frame Relay supporting speeds up to 1 Mbit/s. The aim is to guarantee non disrupted e-mail traffic and constant room for management traffic.

**Fig. 3-52** Traffic Shaping scenario 2 - Prioritisation of applications**Step 1**

On netfence gateways 1 and 2 configure Forwarding Firewall Rule Sets allowing connections to the desired application such as Internet, file sharing, terminal sessions and so on. Assign the same **Band** to all these rule sets in the **Parameter Section** of the Edit/Create Rule configuration window. In the example, usage of **Band A** is assumed.

**Step 2**

On netfence gateways 1 and 2, configure a Forwarding Firewall Rule Sets controlling e-mail traffic between the company locations. Assign a **Band** to this rule set in the **Parameter Section** of the Edit/Create Rule configuration window. In the example, usage of **Band B** is assumed.

**Step 3**

On both boxes browse to **Config > Box > Traffic Shaping**.

Enable **Traffic Shaping** by setting the parameter of the same name to **yes**.

**Step 4**

On both boxes, define shaping policies through parameter **Policy Definition**. The following policy would suit the needs:

**Table 3-18** Example 2 - Policy Definition configuration

Parameter	Description
Policy Name	emailpriority
Management Traffic	Ratio: bandwidth 10 % / maximum bandwidth 100 %
Band A	40 / 100
Band B	60 / 100
Band C - Band G	0 / 0

**Step 5**

Assign policy emailpriority to an interface through parameter **Devices**. The following configuration settings apply:

**Table 3-19** Example 2 - Interfaces configuration

Parameter	Description
Name	emailpriority
Outbound Bandwidth (kbit)	1000
Interface	eth0 (On each box, select the interface, which connects the other location.)
Policy	emailpriority
Enable Inbound Shaping	no
Inbound Bandwidth (kbit)	-

Through the configured settings, the following effective values apply:

**Management Traffic: 10 / 100**

As the highest priority is always assigned to administration tasks, Management Traffic may at all times use 10 % of the interfaces bandwidth, that is 100 kbit/s. If not used by other bands it may use all available bandwidth up to 100 % of the total amount.

**Band A: 40 / 100**

As 10 % of all available bandwidth is allotted to Management Traffic, Band A may use 40 % out of still available 900 kbit/s, that is 360 kbit/s. If not used by other bands it may use all available bandwidth up to 100 % of the total amount, that is 1 Mbit/s. In this case, if Management Traffic does not claim its share, it may use its bandwidth as well.

**Band B: 60 / 100**

Band B may use 60 % out of still available 900 kbit/s, that is 540 kbit/s (see Band A for explanation). If not

used by other bands it may use all available bandwidth up to 100 % of the total amount.

## 2.2.7 Administrators

Multiple administrators with different rights managing the stand-alone netfence gateway can be managed with this configuration file.

To enter the admin configuration, simply double-click the config-tree entry **Administrators**, change to read-write mode by clicking **Lock**. Now click **Insert** to start the configuration sequence by entering the administrator login name.

**Note:**

Please consider that the login name may contain digits and Latin characters devoid of special characters only.

In order to modify an already existing profile, select it from the list and click the **Edit ...** button which opens the configuration dialogue.

To delete a profile, select it from the list, and click the **Delete** button.

List 3-74 Administrators configuration - section Account Description

Parameter	Description
<b>Disabled</b>	A newly configured profile is active by default (default: <b>No</b> ). Disable an administrator's profile by setting the value to <b>yes</b> . With disabled profile logging into the system is no longer possible. <b>Attention:</b> As soon as an administrator's profile is disabled, all processes owned by him are killed, and his home directory is removed.
<b>Full Name</b>	Enter a name here using Latin characters devoid of special characters. The entry is mandatory.

List 3-75 Administrators configuration - section Administrator Authorization

Parameter	Description
<b>Roles</b>	Six predefined roles exist which can be assigned to each additional administrator - Manager, Operator, Mail, Security, Audit, and Cleanup. For detailed information on permissions and restrictions associated with each role please check table 3-20, page 91.
<b>Shell Level</b>	This menu provides options to control the shell access of the administrator. The following entries are available: <b>No_Login</b> effects that the administrator cannot access the shell. <b>Standard_Login</b> allows access to the system on the OS layer via a default/standard user account (home directory: <code>user/phion/home/username</code> ). <b>Restricted_Login</b> permits system access via a restricted shell (rbash). As its name already implies, this type of shell has some limitations such as specifying commands containing slashes, changing directories by entering <code>cd, ...</code> A restricted login confines any saving action to the users home directory. <b>Attention:</b> Data saved to the home directory will be deleted as soon as the administrator with restricted access logs out again.

Table 3-20 Authorisations associated with administrator roles

Box menu	Software item	Manager	Operator	Mail	Security	Audit	Cleanup
<b>Antivir</b>		✓	-	-	✓	-	-
	Update Pattern	✓	-	-	✓	-	-
	Disable/Enable Pattern Update	✓	-	-	✓	-	-
<b>Config</b>		✓	-	-	✓	✓	-
	Create a DHA box	✓	-	-	-	-	-
	Create a PAR file	✓	-	-	-	-	-
	Create a repository	✓	-	-	-	-	-

List 3-76 Administrators configuration - section Administrator Authentication

Parameter	Description
<b>Authentication Level</b>	This menu allows specifying the type of required authentication. The available settings are <b>Key-OR-Password</b> , <b>Password</b> (default), <b>Key</b> and <b>Key-AND-Password</b> . Depending on the selection in this menu, the parameters described below will or will not be available.
<b>External Authentication</b>	Choose the authentication method for external authentication of an administrator. For further information on authentication schemes see 5.2.1 Authentication Service, page 111.
<b>External Login Name</b>	Specify an external login name for the administrator.
<b>Password</b>	Specify the administrator's password here. Confirm the password in the <b>Confirm</b> field.
<b>Next Forced Change [d]</b>	Here the validity period of the password (in days) is specified. As soon as this period expires, the administrator is forced to change the password.
<b>Warning Period [d]</b>	Here it is defined how many days prior to the password-expiration date a warning message is displayed to the administrator.
<b>Expiry Grace Period [d]</b>	Here it is defined for how many days the administrator may exceed the parameter <b>Next Forced Change [d]</b> .
<b>Change Mode</b>	Via the entries provided by this menu, it can be defined whether a password may be used again as it is (entry <b>allow_reuse_of_previous</b> , default) or if a different password is mandatory (entry <b>force_different_password</b> ).
<b>Public RSA Key</b>	As soon as the parameter <b>Authentication Level</b> contains a <b>Key</b> component, this parameter is mandatory. This menu is used for importing the Public RSA Key (required for successful certificate verification) either via a file, clipboard or from the certificate management.

List 3-77 Administrators configuration - section Administrator Access Control

Parameter	Description
<b>Peer IP Restriction</b>	Via this field it is possible to grant the administrator access to systems within her/his scope. Enter the required IP address into this field and click the <b>Insert ...</b> button to the right in order to add the address to the configuration. To modify an already existing entry, select it in the list, edit the entry and then click the <b>Change</b> button. To delete an entry, simply select it and click the <b>Delete</b> button.
<b>Login Event</b>	This menu specifies the way a login is recorded. The entry <b>Service_Default</b> (default) is a reference to the settings made within the <b>Access notification</b> (see Access Notification, page 105). The entry <b>Silent</b> suppresses event notification except login failure events, which always revert to <b>Service_Default</b> settings.



Table 3-20 Authorisations associated with administrator roles

Box menu	Software item	Manager	Operator	Mail	Security	Audit	Cleanup
	Create a server	✓	-	-	-	-	-
	Create a service	✓	-	-	-	-	-
	Kill configuration sessions	✓	-	-	-	-	-
	HA synchronisation	✓	-	-	✓	-	-
<b>Control</b>		✓	✓	-	✓	-	-
	Activate new network configuration	✓	✓	-	-	-	-
	Block a server	✓	✓	-	-	-	-
	Block a service	✓	✓	-	-	-	-
	Time control	✓	-	-	-	-	-
	Delete Wild Route	✓	✓	-	-	-	-
	Import license	✓	-	-	-	-	-
	Kill sessions	✓	✓	-	-	-	-
	Phion restart	✓	✓	-	-	-	-
	Reboot Box	✓	✓	-	-	-	-
	Remove license	✓	-	-	-	-	-
	Restart network configuration	✓	✓	-	-	-	-
	Show license	✓	✓	-	-	-	-
	Start a server	✓	✓	-	-	-	-
Stop a server	✓	✓	-	-	-	-	
<b>DHCP</b>		✓	✓	-	-	-	-
	GUI commands	✓	✓	-	-	-	-
<b>Events</b>		✓	✓	-	✓	✓	✓
	Confirm events	✓	✓	-	-	-	✓
	Delete events	✓	-	-	-	-	✓
	Mark events as read	✓	✓	-	-	-	✓
	Set events to silent	✓	✓	-	-	-	✓
Stop alarm	✓	✓	-	-	-	✓	
<b>Firewall</b>		✓	✓	-	✓	✓	-
	Access to trace tab	✓	-	-	✓	-	-
	Remove entries from cache	✓	-	-	✓	-	-
	Terminate connections	✓	✓	-	✓	-	-
	Create dynamic rules	✓	✓	-	✓	-	-
	Kill a process	✓	✓	-	✓	-	-
	Modify connections	✓	✓	-	✓	-	-
	Modify traces	✓	-	-	✓	-	-
Toggle traces	✓	-	-	✓	-	-	
View rules	✓	-	-	✓	-	-	
<b>Logs</b>		✓	-	-	✓	✓	✓
	Delete resource logs (box_)	✓	-	-	-	-	✓
	Delete service logs	✓	-	-	-	-	✓
	Read resource logs (box_)	✓	-	-	✓	✓	✓
Read service logs	✓	-	-	✓	✓	✓	
<b>Mail</b>		✓	-	✓	-	✓	-
	GUI commands	✓	-	✓	-	-	-
	View Stripped Attachments	✓	-	✓	-	✓	-
	Retrieve Stripped Attachments	✓	-	✓	-	-	-
	Delete Stripped Attachments	✓	-	✓	-	-	-
<b>Policy Service</b>		✓	-	-	✓	-	-
	Block Sync	✓	-	-	✓	-	-
<b>SSL-Proxy</b>		✓	-	-	✓	-	-
	Access Cache Management	✓	-	-	✓	-	-
	Ticket Management	✓	-	-	✓	-	-
	Cert Authorities Management	✓	-	-	✓	-	-
XML Services Management	✓	-	-	✓	-	-	
<b>Statistics</b>		✓	-	-	✓	✓	✓
	Delete resource logs (box_)	✓	-	-	-	-	✓
	Delete service logs	✓	-	-	-	-	✓
	Read resource logs (box_)	✓	-	-	✓	✓	✓
Read service logs	✓	-	-	✓	✓	✓	
<b>VPN</b>		✓	✓	-	✓	✓	-
	Disable VPN connections	✓	✓	-	✓	-	-
	Disconnect VPN connections	✓	✓	-	✓	-	-
	View Configuration	✓	-	-	✓	-	-



## 2.2.8 Box Licenses

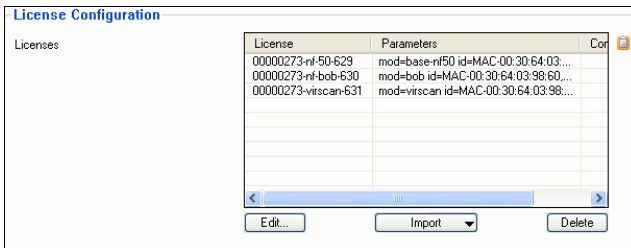
The configuration file **Box Licenses** is a container for all license data a system requires for non-demo mode operation. Purchased licenses may be imported from clipboard or directly from the license file. Licenses are immediately active on the system after activation change.

**Note:**

Importing licenses within the Box Licenses node has the same effect as making use of the license import facility of the control daemon. This means that licenses, which are imported or deleted from the box control licenses view, will be inserted into or removed from the configuration file **Box Licenses**. On a stand-alone system, both approaches may be used interchangeably.

To open the configuration file, double-click **Box Licenses**.

**Fig. 3-53** License Configuration



**List 3-78** Advanced Configuration - section License Configuration

Parameter	Description
<b>Licenses</b>	To import a phion license (.lic), click the <b>Import</b> button and depending on how the license file has been delivered, select a suitable context menu entry from the list.

## 3. Configuring a New Server

### 3.1 General

A server may be configured with one or multiple IPs. It can either run on a single box or, in case of a redundant or high availability (HA) setup, on two boxes.

A server name may contain a maximum of eight characters. It must not contain underscores and special characters except the minus sign.

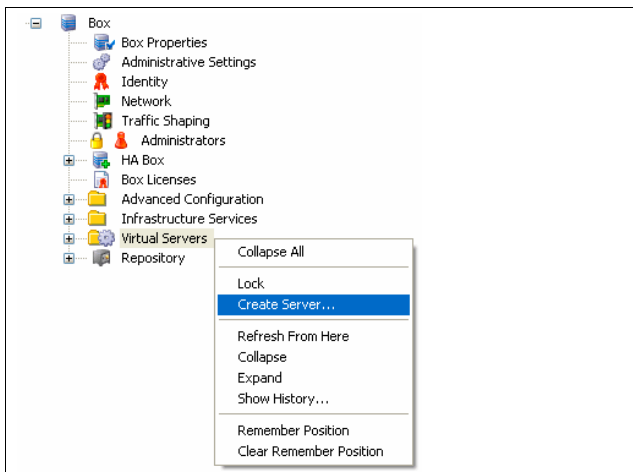
Gather information about the following before introducing a server:


- How will the server be named?
- Which IP addresses will it employ?

**The introduction of servers and services is the first action required after having installed a phion system.**

Unless doing so, the box will stay without special functions.

Fig. 3-54 Context-menu of the Servers directory




To enter the configuration dialogue right-click  **Virtual Servers** and select **Create Server ...** from the context menu.

**Note:**

Creating a new server is only available for netfence gateways on **standard-hardware** (parameter **Appliance Model**).

**Attention:**

To guarantee clearly arranged log files avoid naming a server **'box'**. Choose a significant name instead.

The data inserted into the server configuration dialogue is stored in the  **Server Properties** file, which is a standard component of each server branch of the tree.

**Note:**

Consult this instance to alter server/service configuration settings, such as IP addresses.

Because the configuration parameters in the **Server Properties** section slightly vary in detail, note that servers can be introduced on the following systems and places in the configuration tree:

- on single boxes (3.2 Server Configuration on Single Boxes, page 95)
- on management centres (**phion management centre** - 3.1 Configuring the Box, page 393)
- on MC-administered boxes (3.3 Server Configuration on MC-administered Boxes, page 96)

The deviances between the configuration details are based on the interconnection between service availability and the platform the netfence system is installed on (**Getting Started** - 2.5 phion Multi-Platform Product Support, page 16).

The opportunity to specify the **Product Type** when creating a server is given in order to avoid the possibility of creating services later on that will not be executable on the purchased system. The selection displayed in the product type field is determined and narrowed by the specifications appointed in the **Box Properties** (2.2.2 Box Properties, page 51).

Consider the following example for understanding:

You have installed a single box using the installation tool phion.i (**Getting Started** - 2.2 Creating a "standard" Kickstart Disk, page 10, and then Step 3 Defining Box Type settings) and have specified the following values for the box configuration:

Table 3-21 Example - Box configuration

Parameter	Value
<b>OS Platform</b>	netfence
<b>Product Type</b>	sectorwall
<b>Appliance Model</b>	standard-hardware

As you proceed with creating a server on this box you will notice that you have to choose sectorwall as **Product Type** again, because otherwise no box will be offered for selection in the **Active** and **Backup Box** fields.

Correspondingly, when administering multiple non-identical boxes on a management centre, the view in the boxes' fields will always be narrowed down to the systems suitable for server creation with the chosen product type.

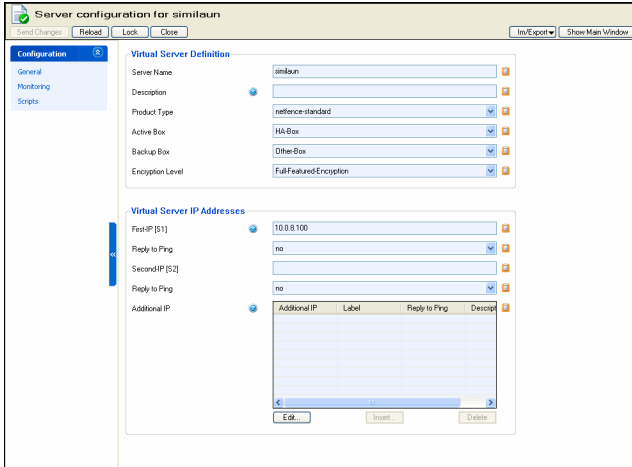
**Note:**

Note that servers cannot be moved to boxes set up using another product type.

## 3.2 Server Configuration on Single Boxes

### 3.2.1 General

Fig. 3-55 Server configuration (single box) - General



List 3-79 Server configuration - General settings on single boxes - section Virtual Server Definition

Parameter	Description
<b>Server Name</b>	The server name is created the moment the server is introduced and cannot be changed later on. The name may contain a maximum of eight characters (digits, "-", "_", and characters from the Latin character set excluding special characters).
<b>Description</b>	Provide a brief but significant description of your server here.
<b>Product Type</b>	Each product type allocates a specific range of services ( <b>Getting Started</b> - 2.5 phion Multi-Platform Product Support, page 16). The product type chosen in this place determines, which services will be available for creation. Choose the product type matching the box(es) you are creating the server for.
<b>Active Box</b>	The box on which the service is meant to run has to be specified as <b>Active Box</b> . In high availability (HA)-setups, two boxes can run active servers alternating to achieve a load-balanced system ( <b>High Availability</b> , page 375). When creating a server on a single box, the box itself has to be specified as active box. In HA-setups, where the configuration is always done on the primary box, the HA-partner has to be specified as active box if it should run the server actively. <b>Note:</b> When creating a server for the first time, the Active Box field cannot be edited. Nevertheless, the server will be allocated to it.
<b>Backup Box</b>	In HA-setups ( <b>High Availability</b> , page 375) this field expects definition of the HA-partner.
<b>Encryption Level</b>	Set the encryption level to <b>Full-Featured-Encryption</b> when installing a fully licensed system. Otherwise, select <b>Export-Restricted-Encryption</b> when installing a DEMO mode or export-restricted gateway.

List 3-80 Server configuration - General settings on single boxes - section Virtual Server IP Addresses

Parameter	Description
<b>First-IP [S1]</b>	This address is the primary address of the server. The IP entered here usually reflects the internal side, which means the primary box network.
<b>Reply to Ping</b>	Controls whether the primary address of the server will respond to an ICMP echo request (default: <b>no</b> ).
<b>Second-IP [S2]</b>	This address is the secondary address of the server.
<b>Reply to Ping</b>	Controls whether the secondary address of the server will respond to an ICMP echo request (default: <b>no</b> ).

List 3-80 Server configuration - General settings on single boxes - section Virtual Server IP Addresses

Parameter	Description
<b>Additional IP</b>	Array of additional IPs that should be activated. Again the parameter <b>Reply to Ping</b> controls whether an address will respond to ICMP echo requests. <b>Note:</b> Maximum entries that do not reply to a ping: 256 (including <b>First-IP</b> and <b>Second-IP</b> ).

### 3.2.2 Monitoring

List 3-81 Server configuration (single box) - Monitoring settings - section Operation Mode

Parameter	Description
<b>Enable Monitoring on Secondary</b>	With <b>Monitoring on Secondary</b> enabled (default setting: <b>yes</b> ) the activated HA-partner as well will shutdown its services as soon as the monitored interfaces/IPs are not available from its own position. Set to <b>no</b> the unavailability won't be noticed and the services will continue to run. <b>Note:</b> In both cases will be probing on the secondary. The setting influences only the behaviour of the services in case of an unavailable secondary.

List 3-82 Server configuration (single box) - Monitoring settings - section IP Monitoring

Parameter	Description
<b>IP Monitoring Policy</b>	Here you may specify the monitoring policy. The following policies are available: <ul style="list-style-type: none"> <li>➤ <b>no-monitoring</b> (default)</li> <li>➤ <b>all-OR-all-present</b>                      Expects the IPs from at least one IP pool to be completely present. If you are monitoring multiple IPs in pool <b>Monitor IPs I</b> only, all these addresses have to be available. If you are monitoring multiple IPs in both pools <b>Monitor IPs I</b> and <b>Monitor IPs II</b>, the IP addresses of at least one of these pools have to be completely available.</li> <li>➤ <b>one-AND-one-present</b>                      Expects one IP to be available from each pool used. If you are monitoring multiple IPs in the pool <b>Monitor IPs I</b> only, at least one IP from this pool has to be available. If you are monitoring multiple IPs in both pools <b>Monitor IPs I</b> and <b>Monitor IPs II</b>, at least one IP address has to be available in each pool.</li> </ul>
<b>Monitor IPs I/ II</b>	Here you may specify IP addresses that must be reachable via the ICMP protocol by the box hosting the server in order for the server to stay up. Reachability is checked at 10 s intervals. In case no answer is received the IPs are probed every second for a 10 s period. Depending on the current monitoring settings, either if no response at all or no response from one of the IPs is received, the server is deactivated. The server is reactivated as soon as subsequent probes at 10 s intervals yield a positive result. The probing is carried out by the control daemon (a box service).

List 3-83 Server configuration (single box) - Monitoring settings - section Interface Monitoring

Parameter	Description
<b>Interface Monitoring Policy</b>	Here you may specify the interface monitoring policy. The following policies are available: <ul style="list-style-type: none"> <li>➤ <b>no-monitoring</b> (default)</li> <li>➤ <b>all-OR-all-present</b>                      Expects the interfaces from at least one interface pool to be completely present. If you are monitoring multiple interfaces in the pool <b>Monitor Devs I</b> only, all these interfaces have to be available. If you are monitoring multiple interfaces in both pools <b>Monitor Devs I</b> and <b>Monitor Devs II</b>, the interfaces of at least one of these pools have to be completely available.</li> <li>➤ <b>one-AND-one-present</b>                      Expects one interface to be available from each interface pool used. If you are monitoring multiple interfaces in the pool <b>Monitor Devs I</b> only, at least one interface from this pool has to be available. If you are monitoring multiple interfaces in both pools <b>Monitor Devs I</b> and <b>Monitor Devs II</b>, at least one interfaces has to be available in each pool.</li> </ul>

**List 3-83** Server configuration (single box) - Monitoring settings - section Interface Monitoring

Parameter	Description
<b>Monitor Interfaces I / II</b>	Here you may specify interfaces which must have a link in order for the server to stay up. The link status is checked on a regular basis. Depending on the current monitoring settings, either if no link at all or no link on one of the interfaces is recognized, the server is deactivated. The server is reactivated as soon as the link status of the monitored interface is up again. The probing is carried out by the control daemon (a box service).

### 3.2.3 Scripts

**List 3-84** Server configuration (single box) - Scripts configuration - section Server Scripts

Parameter	Description
<b>Start Script</b>	Free text area containing command sequences which are executed whenever the server is started up. Use 7-bit ASCII characters and standard BASH (Version 2 compliant) syntax.
<b>Stop Script</b>	Free text area containing command sequences which are executed whenever the server is shut down. Use 7-bit ASCII characters and standard BASH (Version 2 compliant) syntax. <b>Attention:</b> Using <code>phionctrl</code> in the Start and Stop Server fields might cause a deadlock. Do not use <code>phionctrl</code> in this place.

## 3.3 Server Configuration on MC-administered Boxes

On MC-administered boxes the **Active Box** and **Backup Box** fields are named slightly different (see list 3-79, page 95). The implications remain similar though:

**List 3-85** Server configuration (MC) - General configuration - section Virtual Server Definition

Parameter	Description
<b>Primary Box</b>	The box on which the service is meant to run has to be specified as <b>Primary Box</b> . In high availability (HA)-setups, two boxes can run active servers alternating to achieve a load-balanced system ( <b>High Availability</b> , page 375). When creating a server on a single MC-administered box, the box itself has to be specified as primary box. In HA-setups, where the configuration is always done on the primary box, the HA-partner has to be specified as secondary box, if it should run the server actively.
<b>Secondary Box</b>	In HA-setups ( <b>High Availability</b> , page 375) this field expects definition of the HA-partner.

### 3.3.1 Identity Tab

**List 3-86** Server configuration - IDENTITY tab - section Virtual Server Identity

Parameter	Description
<b>Server Private Key</b>	On MC administered boxes a server's private key is automatically generated when a server is created. In conjunction with VPN this key is used to identify the VPN servers against one another, which are located at the tunnel's endpoints. Click on the <b>New Key ...</b> button to generate a new 1024 bit long private RSA key. The key is automatically updated in the view of the VPN GTI Editor.
<b>Server Certificate</b>	This is the server's master signed server certificate.

### 3.3.2 GTI Networks

This configuration section is relevant in conjunction with VPN GTI (**phion management centre - 15. VPN GTI**, page 464).

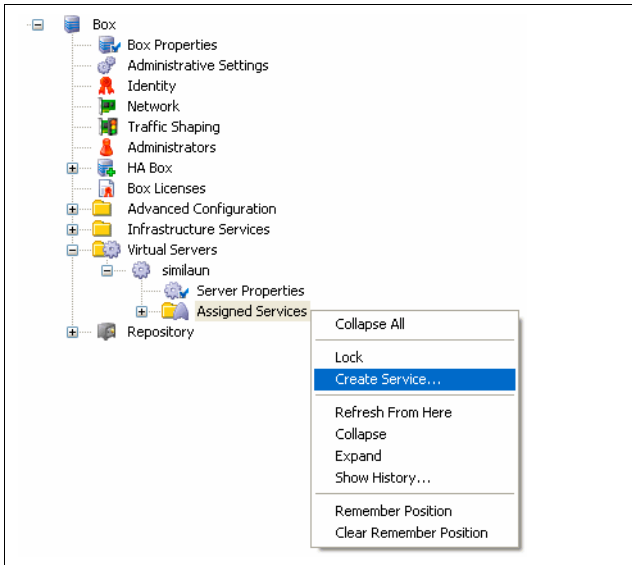
**List 3-87** Server configuration - NETWORKS tab - section Virtual Server/GTI Networks

Parameter	Description
<b>Server/GTI Networks</b>	If VPN tunnels have been configured with the VPN GTI Editor, all networks, which have to be reachable behind the tunnel's endpoints, have to be entered here. These reachable networks are displayed in read only view in the <b>Server/Service Settings tab</b> of the VPN service configuration area (see 15.2.2.3 Defining VPN Service Properties, page 468).

## 4. Introducing a New Service

Services are server elements, thus a server must already exist before a service can be created. Each Server directory contains a **Assigned Services** sub-directory. Services are created in this directory as depicted in figure 3-56.

Fig. 3-56 Context menu of the Services directory



### 4.1 Configuration

Select **Create Service ...** in the **Assigned Services** context menu to enter the configuration dialogue.

A service name may contain a maximum of six characters and must be unique. Services are either server-services or box-services. Box services provide functionality required to run the netfence system. They are factory defined and cannot be removed or introduced manually.

Administrators may only introduce server-services. Server-services are made available under an adjustable subset of IP addresses bound to the assigned server.

**Note:**

According to this structure, server deletion will automatically result in concurrent deletion of assigned services. Create backups of your configuration before changing server and service settings (5.3 Creating PAR Files, page 119).

#### 4.1.1 General view

List 3-88 Service Configuration - General - section Service Definition

Parameter	Description
<b>Disable Service</b>	This parameter allows deactivating the service. By default this parameter is set to <b>no</b> , that means the service will be active upon creation.
<b>Service Name</b>	The service's name supplied before. The name may contain up to 6 characters (digits, "-", and characters from the Latin character set excluding special characters). This is a read-only field, which means that an existing service cannot be renamed.
<b>Description</b>	Provide a brief but significant description of your service here.

List 3-88 Service Configuration - General - section Service Definition

Parameter	Description
<b>Software Module</b>	Select the software module and thus the functionality you wish to be provided by the service. Currently available choices for instance are Firewall, VPN-server, DHCP-Server, DNS, SNMPd (SNMP daemon for Tivoli NetView® network discovery), Proxy, Mail Gateway, and Spam-Filter.  <b>Note:</b> It depends on the type of license you have purchased whether you will actually be able to use all possible service types.  <b>Note:</b> If Model and Appliance type ( <b>Getting Started - 2. phion.i</b> , page 10, then Step 4 Defining System Settings) have been determined during box installation, only the services available for the corresponding model will be displayed.

List 3-89 Service Configuration - General - section Bind IPs

Parameter	Description
<b>Bind Type</b>	The <b>Bind Type</b> determines the method how the service is made available. By default and if available, the service will bind to both server IP addresses ( <b>All-IPs</b> ). Alternatively, it may be instructed to exclusively bind to either first or second server IP ( <b>First-IP, Second-IP</b> ) or any other explicitly defined server IP address(es) ( <b>Explicit</b> ).  <b>Note:</b> Explicitly defined IP addresses must be available in the <b>Additional IP</b> list in the Server Configuration file (see 3. Configuring a New Server, page 94).
<b>Explicit Bind IPs</b>	Into this list insert the explicit IP addresses the service should bind to. Available IP addresses are listed in the <b>Server Address Labels</b> list below.  <b>Note:</b> Only IP addresses that have been specified in the Server Configuration file the service belongs to may be used (see above).  <b>Note:</b> On a VPN server you may define up to 32 Bind IPs.

List 3-90 Service Configuration - General - section Available Server IPs

Parameter	Description
<b>Server Address Labels</b>	This list displays all IP addresses that are available in the Server Configuration file and may be used by the service. First and Second Server IP are flagged with the labels <b>S1</b> and <b>S2</b> , respectively.

#### 4.1.2 Statistics view

List 3-91 Service Configuration - Statistics - section Statistics Settings

Parameter	Description
<b>Generate Statistics</b>	This flag defines whether to generate statistical data for the service (default: <b>yes</b> ).
<b>Src Statistics</b>	This flag defines whether to generate IP source based statistical data for the service (default: <b>yes</b> ). Only volume over time but no correlation with temporal evolution will be recorded.
<b>Src Time-Statistics</b>	This flag defines whether to generate IP source based statistical data for the service (default: <b>yes</b> ). Both volume and correlation with temporal evolution will be recorded.
<b>Dst Statistics</b>	This flag defines whether to generate IP destination based statistical data for the service (default: <b>yes</b> ). Only volume over time but no correlation with temporal evolution will be recorded.
<b>Dst Time-Statistics</b>	This flag defines whether to generate IP destination based statistical data for the service (default: <b>yes</b> ). Both volume and correlation with temporal evolution will be recorded.
<b>Src-Dst Statistics</b>	This flag defines whether to generated IP source/destination pair based statistical data for the service (default: <b>yes</b> ). Only volume over time but no correlation with temporal evolution will be recorded.



**Note:**

Depending on the service, some statistics will ...

- be collected how they have been set in the configuration, **yes** or **no**: symbol ✓
- will always be collected, even if they are set to **no** in the configuration: symbol +
- will not be available: symbol -

**Table 3-22** Service configuration - Statistics dependent or independent from the statistics settings

Service	Generate Statistics	Src Statistics	Src Time Statistics	Dst Statistics	Dst Time Statistics	Src Dst Statistics
DHCP-Service	-	-	-	-	-	-
DHCP-Relay	-	-	-	-	-	-
DNS	-	-	-	-	-	-
Firewall	✓	✓	✓	✓	✓	✓
FTP-Gateway	+	✓	✓	✓	✓	✓
HTTP-Proxy	✓ [a]	✓ [a]	✓ [a]	✓ [a]	✓ [a]	✓ [a]
ISSProventiaWebFilter	-	-	-	-	-	-
Mail-Gateway	✓	✓	✓	✓	✓	✓
OSPFv2-Router	-	-	-	-	-	-
SNMPd	+	✓	✓	✓	✓	✓
SPAM-Filter	+	+	+	+	+	+
SSH-Proxy	-	-	-	-	-	-
Secure-Web-Proxy	✓ [a]	✓ [a]	✓ [a]	✓ [a]	✓ [a]	✓ [a]
Virus-Scanner	+	+	+	+	+	+
VPN-Service	✓	✓	✓	✓	✓	✓
Policy-Service	+	✓	✓	✓	✓	✓

a. after changing this setting a restart of the service is required

### 4.1.3 Notification view

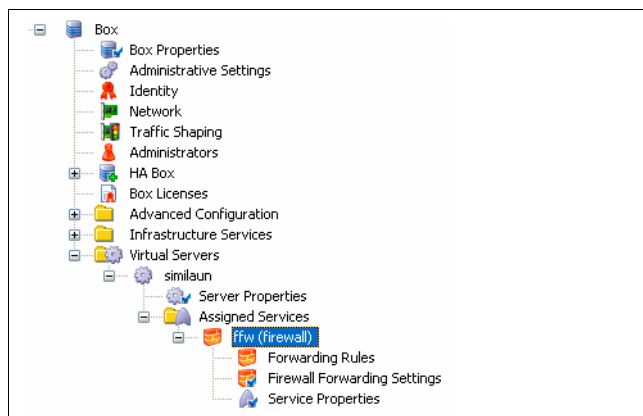
**List 3-92** Service Configuration - Notification - section Access Notification

Parameter	Description										
	In this section you may specify the service specific default level at which event based notification takes place in case of an attempted system access. <b>Note:</b> These settings are only meaningful for services that allow administrative access.										
<b>Service Default (Success)</b>	Service specific default notification type in case of successful administrative access to the service (if available). phion applications generate "phion Subsystem Login" notifications every time a user has successfully logged into an application that interacts with the graphical administration tool phion.a (for example control, event, statistics, config). The default setting is <b>Notice</b> .										
	<table border="1"> <thead> <tr> <th>Value</th> <th>Event type (ID)</th> </tr> </thead> <tbody> <tr> <td>Silent</td> <td>no event</td> </tr> <tr> <td>Notice</td> <td>Phion Subsystem Login Notice [2420]</td> </tr> <tr> <td>Warning</td> <td>Phion Subsystem Login Warning [2421]</td> </tr> <tr> <td>Alert</td> <td>Phion Subsystem Login Alert [2422]</td> </tr> </tbody> </table>	Value	Event type (ID)	Silent	no event	Notice	Phion Subsystem Login Notice [2420]	Warning	Phion Subsystem Login Warning [2421]	Alert	Phion Subsystem Login Alert [2422]
Value	Event type (ID)										
Silent	no event										
Notice	Phion Subsystem Login Notice [2420]										
Warning	Phion Subsystem Login Warning [2421]										
Alert	Phion Subsystem Login Alert [2422]										
<b>Service Default (Failure)</b>	Service specific notification type in case of an unsuccessful administrative access attempt (unknown admin, insufficient authorisation, wrong authorisation token) to the service (if available). The default setting is <b>Notice</b> .										
	<table border="1"> <thead> <tr> <th>Value</th> <th>Event type (ID)</th> </tr> </thead> <tbody> <tr> <td>Silent</td> <td>no event</td> </tr> <tr> <td>Notice</td> <td>Authentication Failure Notice [4110] or User Unknown [4100]</td> </tr> <tr> <td>Warning</td> <td>Authentication Failure Warning [4111] or User Unknown [4100]</td> </tr> <tr> <td>Alert</td> <td>Authentication Failure Alert [4111] or User Unknown [4100]</td> </tr> </tbody> </table>	Value	Event type (ID)	Silent	no event	Notice	Authentication Failure Notice [4110] or User Unknown [4100]	Warning	Authentication Failure Warning [4111] or User Unknown [4100]	Alert	Authentication Failure Alert [4111] or User Unknown [4100]
Value	Event type (ID)										
Silent	no event										
Notice	Authentication Failure Notice [4110] or User Unknown [4100]										
Warning	Authentication Failure Warning [4111] or User Unknown [4100]										
Alert	Authentication Failure Alert [4111] or User Unknown [4100]										

**List 3-92** Service Configuration - Notification - section Access Notification



Parameter	Description
	<b>Note:</b> The event <b>User Unknown</b> is generated when the Admin ID is not known to the underlying phion authentication module. Event type <b>Authentication Failure</b> is used when password or key do not match or the admin is not authorised to access the service (multi admin environment, only in conjunction with a management centre).

**Fig. 3-57** Service directory



Beside other module dependent configuration items, the file **Service Properties** will always be present upon creation of a service.



The service **ffw** for example, illustrated in figure 3-57, is a firewall service and therefore requires a file named  **Firewall Forwarding Settings** with service specific information such as port or maximum number of connections, and another file named  **Forwarding Rules** for accommodation of the firewall rule set.

For further service specific information on this topic, see the service specific operative sections of the documentation.

## 5. Managing the System

In this part we will discuss the remaining configuration instances that may be used to customise box operation.

### 5.1 Box Settings - Advanced Configuration

#### 5.1.1 System Settings

This configuration instance addresses the seasoned Linux expert. Normally there is no need to consult this file as the default settings have been chosen so as to comply with standard phion system requirements.

If you wish to use the phion system as a generic managed Linux platform you may come up against situations where modifications might be desirable. Most people will, however, simply use this file to get an overview as to what certain kernel relevant parameters are set to.

To open the system settings, double-click  **System Settings** (Node  **Advanced Configuration**).

##### 5.1.1.1 IPv4 Settings

List 3-93 System Settings - section General IP Settings

Parameter	Description
<b>TCP ECN Active</b>	<p>With <b>TCP ECN Active</b> (Explicit Congestion Notification) set to <b>Yes</b> it is possible to reduce the TCP traffic when a router load is at a maximum and therefore packet loss is possible.</p> <p><b>Attention:</b> Do not activate this parameter when using netfence gateways with Proxy or MailGW services configured. non-phion systems and some application filters may not be able to handle the ECN header options. When such external systems fetch the TCP header flags a 2-bit mistake occurs because of the way the ECN options are implemented into the TCP header. And this causes that the phion netfence does not establish the connection due to the not correctly answered SYN.</p> <p><b>Note:</b> For more detailed information concerning ECN have a look at RFC 3168.</p>
<b>IP Dyn Address</b>	<p>Only set this to <b>yes</b> if you are experiencing problems with network connections using dynamic IP address allocation (ADSL, cable modem). If the forwarding interface changes socket (and packet) along with this parameter set to <b>yes</b>, the source address while in SYN_SENT state gets rewritten ON RETRANSMISSIONS.</p>

#### 5.1.1.2 ARP Settings

List 3-94 System Settings- section ARP Settings

Parameter	Description
<b>ARP Src IP Announcement</b>	<p>Define different restriction levels for announcing the local source IP address from IP packets in ARP requests sent on an interface. This settings field uses the arp_announce parameter, whose values have been translated by phion to <b>any</b> (internal value = 0), <b>best</b> (internal value = 1) and <b>primary</b> (internal value = 2).</p> <p><b>Note the following excerpt from the kernel documentation:</b></p> <ul style="list-style-type: none"> <li>➤ <b>any</b> (internal value = 0) - Use any local address, configured on any interface.</li> <li>➤ <b>best</b> (internal value = 1, default) - Try to avoid local addresses that are not in the target's subnet for this interface. This mode is useful when target hosts reachable via this interface require the source IP address in ARP requests to be part of their logical network configured on the receiving interface. When we generate the request we will check all our subnets that include the target IP and will preserve the source address if it is from such subnet. If there is no such subnet we select source address according to the rules for setting primary.</li> <li>➤ <b>primary</b> (internal value = 2) - Always use the best local address for this target. In this mode we ignore the source address in the IP packet and try to select local address that we prefer for talks with the target host. Such local address is selected by looking for primary IP addresses on all our subnets on the outgoing interface that include the target IP address. If no suitable local address is found we select the first local address we have on the outgoing interface or on all other interfaces, with the hope we will receive reply for our request and even sometimes no matter the source IP address we announce.</li> </ul> <p><b>Note:</b> Increasing the restriction level gives more chance for receiving answer from the resolved target while decreasing the level announces more valid sender's information and thus is prone to violate privacy requirements.</p>
<b>ARP Cache Size</b>	<p>Defines the maximum number of entries allowed in the ARP cache (default: 8192).</p>

#### 5.1.1.3 Routing Cache

<p><b>Note:</b> Garbage Collection is done regularly by the kernel, the entries shown here provide full access to all relevant kernel parameters.</p>
---

List 3-95 System Settings - Routing Cache - section Routing Cache Settings

Parameter	Description
<b>Max Routing Cache Entries</b>	<p>Specifies the maximum number of entries in the kernel's routing cache (min: 8192, max: limited by the available memory , default: 32768). On systems with a large number of sessions and routed IP addresses this value may need to be increased.</p> <p><b>Note:</b> Increasing this parameter increases memory consumption marginally, on small appliances value 8192 will most likely suffice).</p>

List 3-96 System Settings - Routing Cache - section Garbage Collection

Parameter	Description
<b>GC Elasticity</b>	<p>Specified as integer log2 of an internal parameter used to steer the sensitivity of the garbage collection algorithm. It is provided for completeness only. Changing it requires a thorough understanding of the GC algorithm to achieve the desired effect (default: 8, allowed values: 1, 2, 4, 8, 16, 32).</p>

**List 3-96** System Settings - Routing Cache - section Garbage Collection

Parameter	Description
<b>GC Interval [s]</b>	This parameter is used by the kernel's regular GC loop and defines the loop time in seconds between two regular GC events (min: 1, max: 120, default: 60).
<b>GC Min Interval [s]</b>	The minimum time in seconds between two garbage collections (min: 1, max: 120, default: 60). This parameter is provided since GC may either occur throughout a regular GC loop (see above) or may be triggered by a kernel event outside the regular loop. This parameter warrants that in the latter case GC is not run too frequently. <b>Note:</b> Both parameters above ( <b>GC Interval [s]</b> and <b>GC Min Interval [s]</b> ) may be decreased when the routing cache has a tendency of growing very quickly thereby running the risk of a cache overflow. Frequent and unnecessary GC events will however decrease the system performance.
<b>GC Threshold</b>	A threshold value of cache entries which is used to determine the necessity of garbage collection and to which extent (that is, how radical) entries need to be removed (min: 1024, max: 65535, default: 8192). <b>Note:</b> This parameter should always be significantly smaller than the max number of cache entries.
<b>GC Timeout [s]</b>	Time in seconds after which an inactive routing cache entry is removed from the cache. Note that active entries may not be removed from the cache (min: 1, max: 300, default: 60). <b>Note:</b> Decreasing this value will help in keeping the routing cache smaller. If the same routing entry is typically needed again shortly afterwards a full routing lookup needs to be performed instead of a quick cache lookup.

### 5.1.1.4 I/O Settings

The remaining block of configuration entries is special in so far as the IDE-tuning option is only activated by rebooting the system. This prevents the user from repeatedly activating and deactivating this low-level setting on a running system. Doing so during full operation may cause a freeze of the operating system.

**List 3-97** System Settings - I/O Settings

Parameter	Description
<b>IDE-DMA Support</b>	Most recent IDE hard drives are capable of using direct memory access (DMA) which is by default not enabled by the Linux OS. Performance gains of up to 600 % are realistic when DMA is activated (on a per drive basis on DMA capable drives). If your system uses IDE hard disks you could try to change this setting to <b>yes</b> . You have to reboot your system for this to have any noticeable effect. Note that there is a non-zero chance that your system might freeze.
<b>Advanced IDE Options</b> (only available with parameter <b>IDE-DMA Support</b> set to <b>yes</b> )	This section may be used for optimising the IDE option. <b>Attention:</b> Do not modify these settings unless exactly knowing about the effects. phion recommends to contact your phion partner for details on configuration and to test the settings in a test environment before using them on active systems.
<b>I/O Tuning</b>	Set to <b>yes</b> if you wish to alter the default values of the maximum number of file handles and nodes the OS kernel will be able to handle.
<b>Open Files (max)</b>	Maximum number of open file descriptors the phion system is prepared to handle (min. 8192, max. 65536). Leave at default setting if you do not experience any problems. As a rule of thumb you would not allot more than 256 files per 4 MB of RAM.

### 5.1.1.5 Flash Memory

**Note:**

Flash settings will be ignored for all non-flash RAM-based appliances.

**List 3-98** Box Tuning - Flash Memory - section RAM Partition

Parameter	Description
<b>Size (%)</b>	This is the percental size of the tmpfs RAM partition related to the total available RAM (default: <b>20</b> ). Clearing this field makes the <b>Size (MB)</b> field below available, allowing specification of the the RAM partition size in MB.
<b>Size (MB)</b>	This is the size of the tmpfs RAM partition specified in MB. This field only becomes available if the <b>Size (%)</b> field above is cleared.


**List 3-99** Box Tuning - Flash Memory - section Log Settings

Parameter	Description
<b>Size Settings</b>	This configuration section allows specifying the size settings for all log file types.

**List 3-100** Box Tuning - Flash Memory - section Flash Appliance Settings

Parameter	Description
<b>Force Non Flash</b>	Setting to <b>yes</b> (default: <b>No</b> ) causes the box not to start in flash RAM mode, regardless of the storage architecture the flash RAM auto detection recognises. <b>Attention:</b> Enabling this feature may cause hardware damage. Use with due care.
<b>Force Flash</b>	Setting to <b>yes</b> (default: <b>No</b> ) causes the box to start in flash RAM mode, regardless of the storage architecture the flash RAM auto detection recognises.

## 5.1.2 Bootloader

The configuration dialogue  **Bootloader** addresses the difficult but nevertheless omnipresent issue of Linux kernel updates and boot time behaviour. As these two things are intimately interrelated, they are dealt with by a single configuration instance.

Under normal circumstances you will hardly ever have to make any changes to the default settings of this configuration instance. However, the one thing you will want to change is the boot loader password.

The dialogue consists of three logical groups of configuration parameters with two of them exclusively reserved for kernel software updates whilst the remaining one is dedicated to influencing boot time/prompt behaviour.

**Note:**

Remember that sending and activating a new configuration will not cause the boot loader maintenance module to trigger a kernel update. It will merely alter the header part of the loader configuration file while leaving the kernel untouched.



**Note:**

If you do not have any special hardware requirements you will find the default settings sufficient for proper operation. Setting the Kernel Update parameters to non-default settings requires a sound knowledge of the way in which the bootloader of a Linux system works.

In order to initiate a modification of the boot loader configuration as to which linux kernel to use when booting, you will have to carry out either a kernel software update or invoke a particular utility program from the command line to use the settings reserved for custom/manual kernel updates.

No matter whether you have just changed the boot behaviour or actually updated your kernel to a more recent version you will have to reboot your system for the changes to have any noticeable effect. The Box view of the

control window will always inform you of the current kernel/bootloader status.

To open, select  **Advanced Configuration** >  **Bootloader** and double-click.

List 3-101 Advanced Configuration - Bootloader - section Kernel Updates

Parameter	Description
<b>Update Policy</b>	Governs the way in which the system deals with a kernel update. The policies are: <ul style="list-style-type: none"> <li>➤ <b>automatic</b> (default) A freshly installed kernel is automatically set as default boot kernel.</li> <li>➤ <b>noupdate</b> When installing new kernels the update process of the bootloader configuration is disabled. Reconfiguration of the bootloader has to be performed manually.</li> </ul>
<b>SMP Kernel</b>	Set this parameter to <b>yes</b> (default: <b>no</b> ) when multiprocessor systems are in use (used during updates to find out which kernel is to be used).

List 3-102 Advanced Configuration - Bootloader - section Header Settings

Parameter	Description
<b>Use Linear Mode</b>	Advises the bootloader (LILO) to use linear sector addresses instead of sector/head/cylinder addresses. Linear addresses are translated at run time and do not depend on disk geometry. When using linear mode with large disks, the bootloader may generate references to inaccessible disk areas, because 3D sector addresses are not known before boot time.
<b>Loader Delay</b>	Sets a timeout (in tenths of a second) for keyboard input. If no key is pressed within the specified time, the first or default image is automatically booted. The phion settings for the boot loader allocate a range from 1 to 10 seconds, which means values ranging from 10 to 100, with 30 being the default.
<b>Password Protection</b>	When selected (as is the phion factory default), a password is required to boot the image if additional parameters are specified on the command line (for example single). Doing so increases physical security of the system and requires you to specify an appropriate loader password.
<b>Loader Password</b>	Plain text boot password required for authorisation to supply additional boot parameters to the boot loader and kernel manually. Note that you should choose your own loader password before using the system in a productive environment. The factory default is <b>ph10n</b> . <b>Note:</b> The password can only be stored in plain text format in the loader configuration file ( <code>/etc/lilo.conf</code> ) The remaining parameters are only considered when update policy is set to <b>custom</b> and the loader configuration is changed by invoking a utility program on the command line. For any other update policy or in case of header updates they are ignored.
<b>Boot Loader Location</b>	The default setting and thus behaviour is to determine the boot loader location from the current system setup (that is the configuration at the time the new settings are activated). By changing this parameter you can force a different location of the bootloader. <b>Note:</b> You have to specify a bootable partition or a master boot record.
<b>Serial Console</b>	This is the serial port, which is used to connect to the box by a serial connection. As default "COM1" is used. If there is no serial console on your system enter <b>none</b> .

List 3-102 Advanced Configuration - Bootloader - section Header Settings

Parameter	Description
<b>Global Append Option</b>	Use this to enter different commands to the kernel. <b>Attention:</b> For experts only. The options will be written to <code>/etc/lilo.conf</code> at the end of the append dialogue. <code>append="console=tty0 console=ttyS0,19200n8r *your option*"</code> <b>Note:</b> If a neffence gateway has more than 768 MB RAM and ACPF memory parameters (see Firewall Parameters below) are increased it could be necessary to increase the so-called 'vmalloc' kernel parameter. To increase the memory available for 'vmalloc' add "vmalloc=400M" here.
<b>Default Image Name</b>	By setting this value you can define a different default boot image for loading the phion system. You are required to reference the name of the "Boot Images" defined in <code>"/etc/lilo.conf"</code> . <b>Note:</b> If you do not know what a boot image is, read the online system manuals on LILO first.
<b>No ACPI</b>	Setting this option to <b>yes</b> will instruct the Linux kernel to disable ACPI when the box is booted. Use this when the interrupt routing in the ACPI table is wrong and you want to fall back to standard interrupt routing - or if the ACPI functions in the BIOS cause problems.

## 5.1.3 System Scheduler

This configuration dialogue is used to configure the settings of phion proprietary and other user-defined cronjobs. Note that the configuration dialogue represents a graphical front end to a special crontab named `/etc/cron.d/phioncron`. Standard crontab syntax is used for all entries in this file.

Since most cronjobs fall into one of five categories, which are hourly, daily, weekly, monthly, or annual jobs, appropriate configuration sections are provided. For more exotic jobs a special section **Generic Schedule** is provided, which lets you harness the full power of crontab syntax. You may for instance configure a job that is run every other day of the week but only in May and then every 5 minutes between 05:00 and 06:00.

### Note:

The phion crontab should contain at least two factory defined jobs pertaining to log file and statistics data management.



The storage policies are written to the file `/opt/phion/active/config/logstor.conf` on the box. This file needs to be read in (handed over as an argument) by the log file management utility `/opt/phion/modules/box/logstor/bin/logstor` and governs the way in which log files are treated.

### Note:

The utility program **logstor** is meant to be invoked by `crond`. It is thus mandatory to include an appropriate entry into the phion specific crontab. In particular it is important to reconcile the settings adopted for log storage with the times when `logstor` is run by `crond`.

### Note:

phion recommends running this program on a daily basis. An appropriate entry should thus be made into section **Daily Schedule**.

To open, select  **Advanced Configuration** >  **System Scheduler** and double-click.

➤ **Schedule Parameters**

Section containing key/value definitions of environment variables. These variables are intended to be used in conjunction with jobs.

Three variables are already pre-defined:

**LOGCONF** set to

/opt/phion/config/active/logstore.conf

**MAILTO** (left empty)

**SHELL** set to /bin/bash.

These three are directly interpreted by `crond`.

**Note:**

Variables must be prepended with `$` when referenced in a cronjob entry.

➤ **Daily Schedule**

cronjobs which are run on a hourly and daily basis.

➤ **Monthly Schedule**

cronjobs which are run on a weekly and monthly basis.

➤ **Yearly Schedule**

cronjobs which are run on a yearly basis.

➤ **Generic Schedule**

Advanced section for accommodating cronjobs, which do not fit into one of the preceding categories. Placing jobs in this section requires a basic understanding of standard crontab syntax.

All dialogue windows contain the same basic elements. First, there is a description field which is well suited for mnemonic purposes and of which we advise to make frequent use.

Next, you will need to specify at least one command, which will be run at the times configured in the remainder of the section instance. Since sometimes it might be convenient to be able to run several commands at the same time we have made provisions for specifying more than one command for each cronjob.

Finally, you will need to instruct the cron daemon when to run the desired command or commands. For the five predefined categories hourly, daily, weekly, monthly, and annual we have restricted the choice of options available for the date field of a crontab entry to what is needed most often. Everything that cannot be handled by these categories must be configured as a generic job.

Within each of the predefined categories you have extended control over the next smaller temporal element, that is for an hourly job over the minutes, for a daily job over the hours of the day. Even smaller temporal configuration elements may only be set to a single value

All other temporal elements are implicitly set to always (\*) and do not appear within the dialogue. In brief this warrants that a daily job is run every day of the year.

For the central temporal element (for example, daily - hours) you may specify either a comma separated list or a periodicity (run every ...).

As far as generic jobs are concerned you may make use of almost the full extent of available crontab formatting options.

**Fig. 3-58** Example: condensed excerpt from Paul Vixie's man page on crontab

```
Commands are executed by cron(8) when the minute, hour,
and month of year fields match the current time, and when
at least one of the two day fields (day of month, or day
of week) match the current time.
The day of a command's execution can be specified by
two fields -- day of month, and day of week. If both
fields are restricted (ie, aren't *), the command will be
run when either field matches the current time. For example
`30 4 1,155' would cause a command to be run at 4:30
am on the 1st and 15th of each month, plus every Friday.

Note that this means that non-existent times, such as
"missing hours" during daylight savings conversion, will
never match, causing jobs scheduled during the "missing
times" not to be run. Similarly, times that occur more
than once (again, during daylight savings conversion) will
cause matching jobs to be run twice.

cron(8) examines cron entries once every minute.

The time and date fields are:

field          allowed values
----          -
minute         0-59
hour           0-23
day of month   1-31
month          1-12
day of week    0-7 (0 or 7 is Sun)
                phion uses a range from 0 to 6
                with 0 denoting Sunday

A field may be an asterisk (*), which always stands for
`first-last'.

Ranges of numbers are allowed. Ranges are two numbers
separated with a hyphen. The specified range is inclusive
For example, 8-11 for an `hours' entry specifies
execution at hours 8, 9, 10 and 11.

Lists are allowed. A list is a set of numbers (or ranges)
separated by commas. Examples: `1,2,5,9', `0-4,8-12'.

Step values can be used in conjunction with ranges. Following
a range with `<number>' specifies skips of the
number's value through the range. For example, `0-23/2'
can be used in the hours field to specify command execution
every other hour (the alternative in the V7 standard
is `0,2,4,6,8,10,12,14,16,18,20,22'). Steps are also
permitted after an asterisk, so if you want to say `every
two hours', just use `*/2'.
                handled by option every in the dialogue;
                should not be used as entry to the
                list option

The entire command portion of the
line, up to a newline or % character, will be executed by
/bin/sh or by the shell specified in the SHELL variable of
the crontab. Percent-signs (%) in the command, unless
escaped with backslash (\), will be changed into newline
characters, and all data after the first % will be sent to
the command as standard input.
```

### 5.1.4 Inventory

This configuration file is purely optional and may assist you in keeping track of the kind of hardware your system consists of.

### 5.1.5 Log Cycling

This configuration file is used to configure the utility `logstor`, whose sole purpose is the storage management of log files. `logstor` is able to move log files (and optionally compress) to a destination directory or to remove files based on certain adjustable conditions. The utility is run periodically as a cron job.

The appropriate cron daemon settings are configurable through configuration dialogue **System Scheduler** (see 5.1.3 System Scheduler, page 102). What, however,

happens when logstor is run by the cron daemon is exclusively specified here.

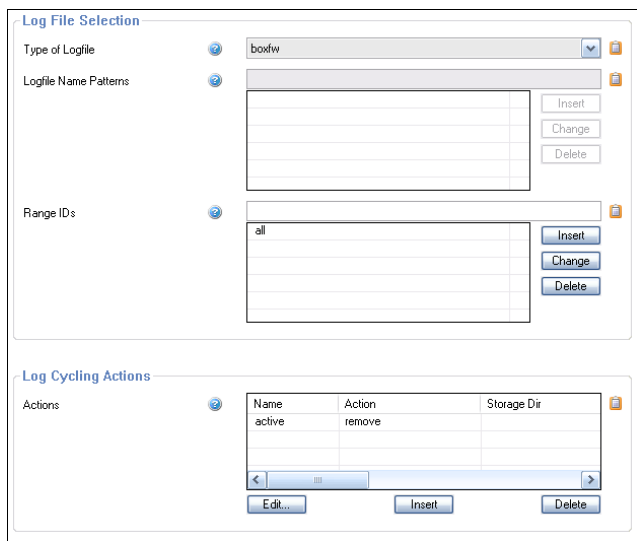
**List 3-103** Advanced Configuration - Log Cycling - section Common Settings

Parameter	Description
<b>Verbose Logging</b>	If set to <b>yes</b> the actions taken and the names of the affected files will be output to the specified log file. The default is no to reduce the amount of logged information.

**File Specific Settings**

Array of sections that describe the way in which certain types of log files are meant to be processed. It is advisable to create a separate section instance for each individual phion log file category, for example box, server, misc, ...

**Fig. 3-59** Log Cycling - section File Specific Settings



To open the the configuration dialogue, click the **Insert** button.

**List 3-104** Log Cycling - File Specific Settings - section Log File Selection

Parameter	Description
<b>Type of Logfile</b>	Predefined categories are: ➤ <b>all</b> - everything containing the string <b>.log</b> in its name, ➤ <b>box</b> - all logs whose names start with <b>box_</b> and contain string <b>.log</b> ➤ <b>boxfw</b> - all logs whose names start with <b>boxfw_</b> and contain string <b>.log</b> ➤ <b>fatal</b> - all logs containing <b>fatal</b> and <b>panic</b> ➤ <b>misc</b> - all logs containing string <b>.log</b> in their names but not starting on <b>box_</b> or <b>srv_</b> ➤ <b>server</b> - all logs whose names start with <b>srv_</b> and contain string <b>.log</b> ➤ <b>user</b> - user defined pattern match (see below).
<b>Logfile Name Patterns</b>	Only enabled when type <b>user</b> has been selected. You may enter a list of wild card expressions. Still only files with the suffix <b>.log</b> will be affected. <b>Note:</b> Protect wildcards with single quotes.

**List 3-104** Log Cycling - File Specific Settings - section Log File Selection

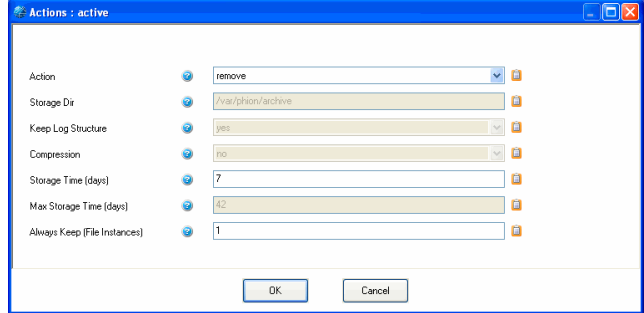
Parameter	Description
<b>Range IDs</b>	Enter the desired ranges. An entry may either be a single number, an interval, or literally void to denote no range. Leave it empty if their are no ranges.

**Log Cycling Actions**

Variable number of subsection each specifying a particular action to be taken. The action is only applied to log files of the specified type.

To open the configuration dialogue, click **Insert**.

**List 3-105** Log Cycling - File Specific Settings - section Log Cycling Actions



**List 3-106** Box Misc - Log Cycling - File Specific Settings - section Log Cycling Actions

Parameter	Description
<b>Action</b>	Predefined categories include rm (delete files), move (move files to an archiving directory), and purge (a more ruthless version of rm).
<b>Storage Dir</b>	Only enabled when action move has been selected. It determines the target directory for the move action.
<b>Keep Log Structure</b>	Only enabled when action move has been selected. It determines whether or not both the logs and the logcache subdirectories of <b>/var/phion</b> are replicated for the files to be moved. Leave set to the default of <b>yes</b> .
<b>Compression</b>	Only enabled when action move has been selected. If set to <b>yes</b> the files to be moved will be piped through <b>gzip -6</b> and thus compressed. An extension <b>".gz"</b> is automatically appended.
<b>Storage Time (days)</b>	Enabled for actions move and rm. Determines the keep time of a file (with respect to its modification date) before the specified action is applied to it.
<b>Max Storage Time (days)</b>	Enabled for action purge only. If a file is older (with respect to its modification date) than this number of days it will be removed regardless of whether or not is represents the sole file instance. This option is used for the removal of log files that are not maintained any longer.
<b>Always Keep (File Instances)</b>	Enabled for actions move and rm only. The respective action is not taken if not at least this number of instances of this type of log file remain untouched. It thus overrules entry <b>Storage Time</b> .

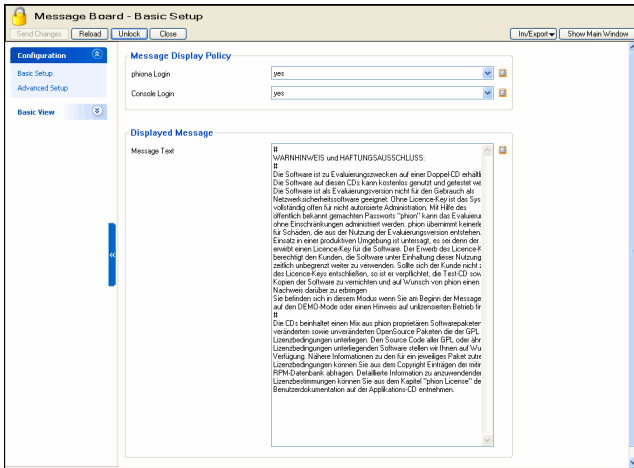


## 5.1.6 Message Board

In this section you can configure the messages which are displayed at login time via SSH, the phion.a GUI and on the console. Use only:

- Alphabetic characters
- Numerics
- # ! \_ , .

Fig. 3-60 Configuration Dialogue - Messages



**Note:**

Empty breaks, repeated spaces, and a single period (.) in an empty line will be ignored.

**Note:**

Check the display of the message at the login after editing.

## 5.1.7 Access Notification

Each system access constitutes an action with a substantial inherent security risk. In order to keep track of system access on all levels (operating system, phion infrastructure, and phion services) phion systems are equipped with an elaborate event based notification model. The advantage of active notification over simple log file based accounting is that a potential intruder will find it very difficult to conceal his actions. Moreover, a significant level of accountability of successful or unsuccessful system access attempts may be attained.

Notification is a complex matter and has been built on the following conceptual cornerstones:

- notification should be adjustable on a per service basis
- notification should be adjustable on a per administrator basis (management centre option)

As consequence the phion model makes use of five notification schemes, which provide ability to link an admin with a particular service specific notification setting:

Table 3-23 Overview of the five notification schemes on phion systems

Scheme	Description	Multi-admin option
service default	Default notification settings for all phion and system services capable of allowing access to the system. These settings are always in effect for user root. The same applies to all system-only users (phion for example).	no
silent	Automatically assigned to invisible users "ha" and "master". The scheme suppresses notification in case of successful access. Unsuccessful attempts are treated according to scheme "service default".	no
type 1	Multi-admin option, freely customisable	yes
type 2	Multi-admin option, freely customisable	yes
type 3	Multi-admin option, freely customisable	yes

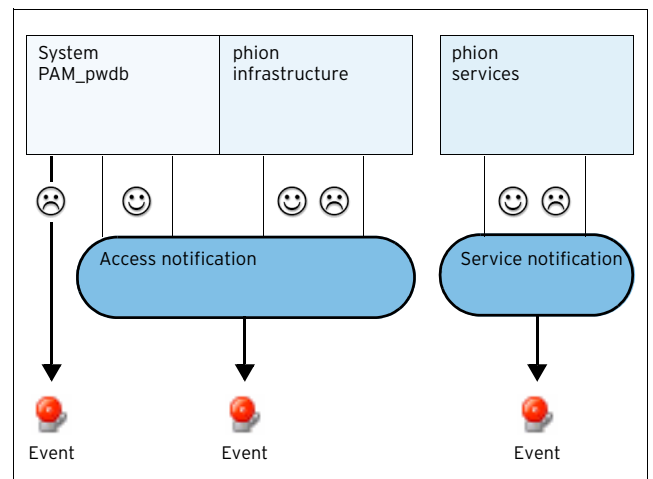
Each administrator is explicitly or implicitly equipped with a particular scheme which, in essence, is a collection of notification settings. These settings assign particular notification types to each phion service or otherwise relevant system service (for example SSHd or console login). Notification triggering for success and failure events can usually be configured individually, except for one notable exception - direct system access failure or access by an unknown user will always trigger an event.

The following notification types are currently in use:

- **Silent (no event)**
- **Notice**
- **Warning**
- **Alert**

The latter three may be used to modify the severity of a context dependent event type. A listing of generated events (Event-IDs 4100, 4110, 4111, 4112, 4130, 4131, 4132) can be found in **System Information** - 5. List of Default Events, page 516.

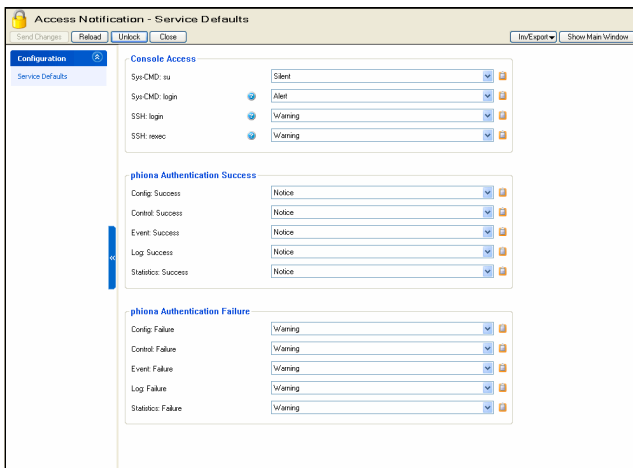
Fig. 3-61 Various configuration instances the phion notification model relies upon



The way in which services determine which event to generate upon a successful or unsuccessful authentication/access attempt is illustrated in figure 3-61. The service uses the login ID attempting access to verify its legitimacy on the system. Next, it determines the associated notification scheme for the login ID with service default constituting a fallback option. Finally, it determines the service-specific notification type from the applicable notification scheme. It then generates an appropriate event.

To open, select **Advanced Configuration** > **Access Notification** and double-click.

Fig. 3-62 Configuration Dialogue - Access Notification



List 3-107 Box Misc - Access Notification - section Console Access

Parameter	Description
<b>Sys-CMD: su</b>	Notification type for the su (Substitute User) command line tool. The notification settings used are not those of the system user invoking <b>su</b> but the system user whose identity is adopted.
<b>Sys-CMD: login</b>	Notification type for a successful login. Note that login here denotes direct system access via the console.
<b>SSH: login</b>	Notification type for a successful system access via SSH protocol.
<b>SSH: rexec</b>	Notification type for an access via SSH protocol for the purpose of remote command execution. Note that remote copy (scp) and secure FTP (sftp) would also fall into this category.  <b>Note:</b> The preceding four service instances do not have adjustable settings for the case of a failed access attempt. This is due to the fact that we believe that access failures at level operating system must always be recorded. To this end we have hardcoded the corresponding failure policy.

Two simple scenarios may be distinguished:

- Login is attempted with an unknown login ID thus triggering Event-ID **4100 User Unknown**.
- The authentication process fails for some other reason creating Event-ID **4110 Authentication Failure Notice**. Authentication failure on the second login attempt generates Event-ID **4111 Authentication Failure Warning**. Finally, if the maximum number of authentication attempts (usually 3) is exceeded notifications with Event-ID **4112 Authentication Failure Alert** are generated. Note that the latter will only be possible if an internal system error has occurred.

Throughout the remainder <service> will represent all phion infrastructure services:

- <Service> (Success)  
Notification type for successful access to infrastructure service <service>.

## 5.1.8 SSH

This configuration instance is used to configure certain aspects of the operation of the SSH daemon (based on OpenSSH, www.openssh.org).

### Note:

OpenSSH is a free version of the SSH protocol suite of network connectivity tools. SSH is part of the underlying phion Linux distribution which is available free of charge.

Each phion system is routinely equipped with a SSH daemon listening on TCP port 22 on all administrative IP addresses (the primary box IP and all further IPs to which administrative services are supposed to bind).

Access to a phion system via the SSH protocol is meant to be used for the purpose of software updates and rare maintenance tasks. All routine administrative tasks may normally be dealt with via the phion management console phion.a.

The management console phion.a allows direct access to a phion system via SSH protocol version 2 by means of integrated terminal functionality. Simply click on the icon **SSH** located on the left hand side navigation area and the following window will appear.

### Note:

phion has modified the SSH daemon so as to provide relevant information such as system access and remote command execution as well as protocol requests via the phion log and event notification logic. The corresponding log file is entitled sshd and may be found under the Box section of the log tree.

To open, select **Advanced Configuration** > **SSH** and double-click.

### 5.1.8.1 Basic Setup

List 3-108 Box Misc - SSH Basic Setup - section General Settings

Parameter	Description
<b>Event on SSH</b>	You may configure the SSHd related conditions that trigger event notification (Events <b>Daemon Startup Failed/Succeeded</b> [2070/2071] and <b>Daemon Shutdown Failed/Succeeded</b> [2072/2073]). Choose from four different settings: <ul style="list-style-type: none"> <li>➤ <b>start-failure</b> (default)</li> <li>➤ <b>+stop-failure</b></li> <li>➤ <b>++start-success</b></li> <li>➤ <b>+++stop-success</b></li> </ul> The list is additive, which means items further down the list automatically include all previous ones. <b>Note:</b> You will not be notified when SSHd is killed manually or just dies unexpectedly. The settings here only pertain to SSHd behaviour during controlled start or stop sequences.

**List 3-108** Box Misc - SSH Basic Setup - section General Settings

Parameter	Description
<b>Allow TCP Forwarding</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Specifies whether TCP forwarding is permitted. The default is <i>no</i>.</p> <p><b>Note:</b> Disabling TCP forwarding does not improve security unless users are also denied shell access, as they can always install their own forwarders by means of the ssh command.</p>
<b>Login Timeout</b>	<p>The server disconnects after this time if the user has not successfully logged in. The minimum time limit is 10 (seconds). The default is to wait for 90 (seconds).</p>
<b>Permit Root Login</b>	<p>This parameter defines whether a SSH login with user name <code>root</code> is possible/allowed.</p> <p><b>Note:</b> Denying root login via SSH causes the following configuration entities not to work: <b>Box Exec</b> tab and <b>Software Update</b> tab.</p>
<b>Check User Home</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Specifies whether sshd should check file modes and ownership of the user's files and home directory before accepting login. This is normally desirable because novices sometimes accidentally leave their directories or files writeable. The default is <i>yes</i>.</p>
<b>Send Keepalives</b>	<p>Specifies whether the server should send keepalive messages to the other side. If they are sent, death of the connection or crash of one of the machines will be properly noticed. However, this means that connections will die if the route is down temporarily, and some people find it annoying. On the other hand, if keepalives are not sent, sessions may hang indefinitely on the server, leaving "ghost" users and consuming server resources. The default is <i>yes</i> and the server will notice if the network goes down or the client host reboots. This avoids infinitely hanging sessions.</p>
<b>Supported Protocols</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Specifies the protocol versions sshd should support. The possible values are protocol version 2 only and protocol versions 2 and 1 (with version two being the preferred choice).</p> <p><b>Note:</b> phion recommends not to enable backwards compatibility support for protocol version 1 clients as protocol version 1 has been proven to be vulnerable to man-in-the-middle attacks. The phion client tries to use version 2 by default.</p>

### 5.1.8.2 Advanced Setup

**List 3-109** Box Misc - SSH Advanced Setup - section Protocol Version 2 Options

Parameter	Description
<b>Allow Compression</b>	<p>This parameter activates/deactivates using compression for SSH clients.</p>
<b>Force Key Authentication</b>	<p>Via this parameter key usage is enforced for SSH clients.</p> <p><b>Note:</b> If key usage is mandatory for external SSH clients when connecting to a box and automated login is desired without further user interaction, the client certificate's private key residing on the Microsoft Windows system has to be shaped into a UNIX understandable format. See 5.1.8.3 Handling Forced Key Authentication below for a description how to generate the required key.</p>
<b>Secure FTP Support</b>	<p>Setting this to <i>yes</i> (default: <i>no</i>) instructs sshd to implement the "sftp" file transfer subsystem. By default no subsystem is defined. Note that this option applies to protocol version 2 only. Secure FTP may be viewed as a more comfortable alternative to the humble scp command when trying to transfer bulk data to or from the box.</p>

**List 3-110** Box Misc - SSH Advanced Setup - section Protocol Version 1 Options

Parameter	Description
<b>Server Key Length (Bits)</b>	<p>Defines the number of bits in the ephemeral protocol version 1 server key. The minimum value is 512, and the default is 768. This setting applies only to protocol version 1.</p>
<b>Key Regeneration Period</b>	<p>In protocol version 1, the ephemeral server key is automatically regenerated after this many seconds (if it has been used). The purpose of regeneration is to prevent decrypting captured sessions by later breaking into the machine and stealing the keys. The key is only stored in memory. If the value is 0, the key is never regenerated. The phion default is 900 (seconds). This setting applies only to protocol version 1.</p>

### 5.1.8.3 Handling Forced Key Authentication

For various administrative purposes, for example statistics collection with external tools, it may be desired to randomly connect to a box with an external SSH client, thereby omitting user interaction. Unfortunately, the certificate's private key, which can be exported from the Certificate Store in encrypted PFX file format using the Microsoft Management Console (MMC), cannot be understood by the netfence gateway. The PFX file has to be converted to a UNIX understandable unencrypted private key in PEM format. Proceed as follows to prepare your system for remote SSH client usage:

#### Step 1 Create an administrative login

- In the configuration tree of the box browse to **Box** > **Administrators**.
- Add a new administrative account to the configuration. (For a description how to create an administrative account, see 2.2.7 Administrators, page 91.)
- Specify a significant **Name**. Set the administrator's **Authentication Level** to **Key**. Import the **Public RSA Key**, which has been issued for this user, from the **Microsoft Certificate Management** Store.

#### Step 2 Export the private key from the Certificate Management Store

- Open the Certificate Management Store by typing `C:\windows\system32\certmgr.msc` at the DOS prompt.
- Browse to the folder **Personal** > **Certificates**.
- Select the certificate, right-click and choose **All Tasks** > **Export ...** from the context menu. The Certificate Export Wizard opens.
- Select **Yes, export the private key**.
- In the PKCS #12 tab clear the checkbox **Enable strong protection**.
- Enter a password.
- Specify a file name (`private_key.pfx` in the example below).

#### Step 3 Copy the PKCS12 (.pfx) file to a UNIX client supporting OpenSSL (for example the netfence box)

#### Step 4 Convert the RSA Key from PKCS12 format to PEM format (encrypted)

- On the UNIX client browse to the RSA Key.  
Type the following at the command line interface:

```
# openssl pkcs12 -in private_key.pfx
-nocerts -out priv.key
```

`priv.key` specifies the file's name after conversion.

### Step 5 Extract the private key and generate and OpenSSH SSH-2 private key (unencrypted)

- Therefore, type the following at the command line interface:

```
# openssl rsa -in priv.key > ~/.ssh/
id_rsa_my_priv_key
```

`id_rsa_my_priv_key` specifies the file's name after decryption.

`~/.ssh/` is an arbitrarily chosen path on the UNIX client.

### Step 6 Log into the netfence gateway

- Type the following at the command line interface:

```
# ssh -i ~/.ssh/id_rsa_my_priv_key
-lloginname dest-ip
```

`lloginname` specifies the name of the administrative account as defined in [Step 1](#).

`dest-ip` specifies the netfence gateway's login IP.

Depending on the client, the key has been converted on, file permissions of the private key file possibly have to be adapted. If the gateway refuses key usage, change file permissions by typing:

```
chmod 600 ~/.ssh/id_rsa_my_priv_key
```

#### Note:

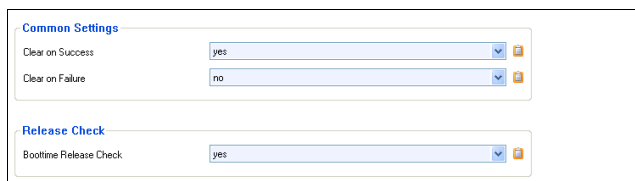
The transformed private key may be used with third party remote SSH clients. It may for example be utilised with SSH agents or be imported into PuTTYGen for further conversion into PuTTY's own file format (.ppk).

## 5.1.9 Software Update

The **Software Update** facility describes the delete-behaviour on a software update.

To open, select **Advanced Configuration** > **Software Update** and double-click.

Fig. 3-63 Configuration Dialogue - Software update



List 3-111 Advanced Configuration - Software Update - section Common Settings

Parameter	Description
<b>Clear on Success</b>	Should delete the rpm-file (the update-file) on successful update (default <b>yes</b> ).

List 3-111 Advanced Configuration - Software Update - section Common Settings

Parameter	Description
<b>Clear on Failure</b>	Should delete the rpm-file (the update-file) on failure update (default <b>no</b> ).

List 3-112 Advanced Configuration - Software Update - section Release Check

Parameter	Description
<b>Boottime Release Check</b>	If this option is set to <b>no</b> on startup of the netfence box no release consistency check is performed. especially on machines with a slower CPU this may reduce startup time by several minutes (default: <b>yes</b> ).

## 5.1.10 Watchdog

The **Watchdog** facility is a means by which you may set certain limits on critical system resources and ensure to have them checked at least once a minute. In the emergence of massive resource over-consumption or unexpected termination of core processes, such as the control daemon or the SSH daemon, the watchdog will try to remedy the situation by means of a repair facility or, as a last resort, resetting the system.

As such the watchdog complements the functionality provided by the control daemon. Amongst other things the watchdog is useful to ensure that the control daemon remains up and running at all times. It is equally useful to ensure a swift take-over by an optional high-availability partner in case the system freezes due to hardware or file-system problems.

The downside of running a watchdog is that the system can get reset by watchdog if a configurable number of repair attempts in a row have not sufficed to remove the problem. In this case the system may not be able to complete the bootstrap without human intervention due to file system inconsistencies, which have been incurred by a potential emergency shutdown. It is therefore imperative to understand the working principle of the watchdog before activating it on systems, to which you do not have immediate physical access.

As an intermediate step to full operation watchdog may be run in monitoring mode in which it will only report problems but not reboot the system.

Yet, certain severe error conditions such as a full process table will still cause watchdog to carry out an unconditional reboot.

### 5.1.10.1 General Working Principle

The Linux kernel provides a special device `/dev/watchdog`, which when opened must be written to within a minute, or the system will be reset. Each write delays the reboot time for another minute. Watchdog is the daemon process delaying this reset by writing to `/dev/watchdog` at least once every minute if the system is still healthy. What **healthy** means is configurable to a certain extent. If the system is found to have a non fatal problem watchdog will pass the respective error code to a repair routine (`/usr/sbin/repair`). If the routine returns a zero exit code to watchdog the system is considered successfully repaired. If this is not the case the system will be soft-booted by the watchdog. The watchdog achieves this by making use of its own built-in shutdown

procedure, so it has not to rely on the availability of potentially critical system resources.

**Note:**

If the shutdown fails the system is hard-reset by the kernel. Since this is all about a software watchdog the ability to reboot will always depend on the hardware state of the machines and its interrupts.

**5.1.10.2 Tests and Monitored Resources**

Watchdog performs the following checks:

**Table 3-24** Overview of the checks watchdog runs

Check whether ...	Configurable	Parameterisation	Recovery
process table is full	no	none	immediate reboot
file table overflow occurred	no	none	repair policy dependent
enough free memory available	yes	as percentage of total RAM plus swap	repair policy dependent
load average exceeds a max value	yes	separately for 1, 5 and 15 min. averages	repair policy dependent
a give process is still running	yes	separate settings for control and SSH daemon	repair policy dependent

If any of these checks except for the process table check fails, watchdog will invoke the repair binary (`/usr/sbin/repair`). If the process table is full the repair binary cannot be executed, therefore an immediate soft reset is the only available consequence. Should any of

these tests last longer than one minute the machine will be rebooted as well.

**5.1.10.3 Repair Logic**

A "last resort" repair system must remain sufficiently simple to accomplish its task. If the checks or repair routine try to be too smart the decision process becomes error prone with the effect that appropriate reaction is delayed and the kernel will eventually force a hard-reset of the system. The odd premature yet smooth reboot represents a mere nuisance whilst a single unnecessary hard reset can compromise system integrity. Still it is undesirable to have a system always reboot whenever the slightest resource limit infringement occurs. We thus provide the administrator with a choice of four repair policies by way of which watchdog's reaction to a problem may be influenced:

**Note:**

The maximum number of repair attempts applies to each monitored entity separately. This means that file table overflow, memory shortage, ... each is allotted a separate counter.

**Note:**

Negative error codes designate special errors generated by the check routines of watchdog. All other errors conform to the standard error coding scheme of Linux.

**Table 3-25** Listing of the four available error handling policies offered by the repair utility of the watchdog module

Policy [index]	Parameters	Description
Ignore_Errors [0]	none	Monitoring mode: if the repair binary is invoked, it will just log the error condition and then return <b>0</b> to the watchdog
Repair_or_Ignore [1]	number of repair attempts	Default mode: The following severe errors will cause repair action if the maximum number of consecutive attempts has not been exceeded for the particular error type. Otherwise, a reboot is triggered.
		<b>Error name</b> <b>Error number</b> <b>Description</b>
		ENFILE                      23                      Too many open files in system
		ENOMEM                    12                      Cannot allocate memory
		ESRCH                      3                        No such process
		ENOENT                    2                        No such file or directory
		EINVMEM                  -7 <code>/proc/meminfo</code> contains invalid data
		EMAXLOAD                -3                      Load average too high
		ENOLOAD                  -5 <code>/proc/loadavg</code> contains no data
All other errors are ignored and <b>0</b> is returned to watchdog		
Repair_or_Reboot [2]	number of repair attempts	Strict mode: behaviour is exactly the same as described above except that all other not explicitly listed errors are returned to watchdog causing a re-boot of the system. The idea behind this is that a repair action is only meaningful when the error cause is relatively well known.
Always_Reboot [3]	none	Paranoid mode: if the repair binary is invoked the error condition is logged and the error code is returned to watchdog, causing a re-boot of the system

**5.1.10.4 Repair Strategy**

Depending on the passed type of error the repair binary will attempt to remedy the situation by appropriate counter measures. To this end we have assumed the following simple assignment of handed over error types to system problems:

**Table 3-26** Error code to error origin assignment assumed by the repair utility

Error code	Assumed system problem
ENFILE (23)	Out of file descriptors (that is file table overflow)
ENOMEM (12) EINVMEM (-7)	Low on memory

**Table 3-26** Error code to error origin assignment assumed by the repair utility

Error code	Assumed system problem
EMAXLOAD (-3) ENOLOAD (-5)	Maximum allowed system load average exceeded
ESRCH (3) ENOENT (2)	Monitored process has died or its pid-file is missing

➤ **File table overflow**

If a file table overflow occurs the repair binary will increase the number of available file descriptors by 10 %. If the error condition persists it will continue increasing the number of available file descriptors until the maximum number of repair attempts has been exhausted. The number of already undertaken repair



attempts is written to file `/var/run/watchdog.state.fd`.

**Note:**

Increasing the number of available file descriptors will raise kernel memory consumption and may eventually lead to a memory shortage.

➤ Process termination

Watchdog will at most monitor two daemon processes, the control daemon and the SSH daemon. It does so by checking whether the processes corresponding to the process ids given in `/var/run/control.pid` and `/var/run/sshd.pid` are still running, respectively. The strategy of the repair binary differs for the two daemons. If the control daemon is down it will first be stopped (`/opt/phionctrl box stop control`) and subsequently started (`/opt/phionctrl box start control`). Immediately afterwards a check is performed to determine whether or not the restart attempt has been successful. Only if the restart attempt has failed the repair counter is incremented and written to file `/var/run/watchdog.state.pid`. Finally, if the maximum number of repair attempts has been reached a last attempt to recover from the failure condition is made by shutting down and restarting the whole phion subsystem (`/opt/phionctrl shutdown; /opt/phionctrl startup`). If the error condition persists, which means `controld` is still not running, a reboot is requested.

If the SSH daemon is down an attempt to restart it is made by invoking `/etc/rc.d/init.d/ssh condrestart`. The repair counter is never incremented thus allowing for an arbitrary number of restart attempts. The idea here is that repeated failures to activate SSHd are not deemed a sufficient condition to autonomously restart the system.

**Note:**

In order to facilitate system maintenance, for example for software updates which involve a temporary shutdown of either `controld` or `sshd`, the repair binary will ignore error code `ESRCH`, if a file `/var/run/watchdog.state.service` exists. The phion software update procedure will automatically create and remove this file. If you interact with the system on the command line make sure to touch and subsequently remove this file when shutting down or blocking `controld`. Alternatively, you may shutdown [restart] `watchdog` by invoking:

```
/etc/rc.d/init.d/watchdog stop [start]
```

Due to the fact that netfence gateways are operated as dedicated systems resource problems are most likely caused by phion service processes being under too heavy load for the size of the system. To be on the safe side memory shortages or excessive loads are thus attributed to the operation of the phion subsystem as a whole.

To block the `watchdog-repair-routine` it is necessary to start the `/etc/phion/bin/servicemode` and enter the required time in minutes.

➤ Memory shortage

The phion subsystem is shut down (`/opt/phionctrl shutdown`) and subsequently restarted (`/opt/phionctrl startup`). The number of such

already undertaken repair attempts is written to file `/var/run/watchdog.state.mem`.

➤ Maximum load exceeded

The phion subsystem is shut down (`/opt/phionctrl shutdown`) and subsequently restarted (`/opt/phionctrl startup`). The number of such already undertaken repair attempts is written to file `/var/run/watchdog.state.load`.

**Note:**

The repair counters as well as the service indicator file are automatically reset during a reboot, since all contents of `/var/run` are automatically purged by the system. Furthermore, all counter files but not the service file, are deleted when `watchdog` is restarted, that also means whenever the configuration is changed.

➤ Operational Events

Errors the repair binary generates related to system information are the events 34 [Critical System Condition], 510 [Invalid Argument], and 4202 [System Reboot] (see 5.2 Operational Events, page 517).

### 5.1.10.5 Watchdog GUI - Basic Setup

Select  **Advanced Configuration** >  **Watchdog** and double-click.

**List 3-113** Advanced Configuration - Watchdog Basic Setup - section Monitoring Policy

Parameter	Description
<b>Run S.M.A.R.T</b>	This parameter (default: <b>yes</b> ) creates an event if a critical condition occurs on a HD (Event-ID <b>34</b> ).
<b>Run Watchdog</b>	States whether or not <code>watchdog</code> is active. Default is <b>no</b> .

**List 3-114** Advanced Configuration - Watchdog Basic Setup - section Watchdog Repair Policy

Parameter	Description
<b>Repair Mode</b>	Only active when <b>RUN WATCHDOG</b> is set to <b>yes</b> . Defines the way in which errors are dealt with by the repair utility. See explanation above. Default is <b>Repair_or_Ignore</b> .
<b>Repair Attempts</b>	Number of repair attempts per checked entity (default: 3). See explanation above.

### 5.1.10.6 Watchdog GUI - Watchdog Details

**List 3-115** Advanced Configuration - Watchdog Details - section Watchdog Operational Setup

Parameter	Description
<b>Realtime Mode</b>	Set to <b>yes</b> (default) <code>watchdog</code> locks itself into memory, so it does never get swapped out. On a system under heavy load this setting minimises the risk that the daemon process possibly might not manage to write to the kernel device in due time (60 s).
<b>Scheduler Priority</b>	Sets the scheduler priority for operation in realtime mode. Leave this set to 1 unless you are a savvy Linux expert with deep operating system knowledge. <code>Watchdog</code> uses round-robin scheduling ( <code>SCHED_RR</code> ). The larger the number the higher the priority of the process. Standard user-space processes are usually assigned priority 0.
<b>Check Interval [sec]</b>	The interval in seconds between two writes to the kernel device. The kernel drivers expects a write operation at least once every 60 s. Each write is accompanied by a check on all monitored system entities.



**List 3-115** Advanced Configuration - Watchdog Details - section Watchdog Operational Setup

Parameter	Description
<b>Verbose Logging</b>	Set to <b>yes</b> for verbose mode. This mode will log status information to syslogd with facility LOG_LPR. Syslogd will forward this log traffic to the phion syslog interface psyslogd which in turn will redirect the log stream into log tree node Box > Watchdog > Monitor. Load average, monitored process (pid) status, memory usage, and alive time of watchdog are reported.
<b>Logtick</b>	Logtick allows adjustment of the number of intervals skipped before a verbose log message is written to syslogd. The default value of 3 already reduces log traffic and consequently disc space consumption by 66 %.

**List 3-116** Advanced Configuration - Watchdog Details - section Watchdog Monitored Entities

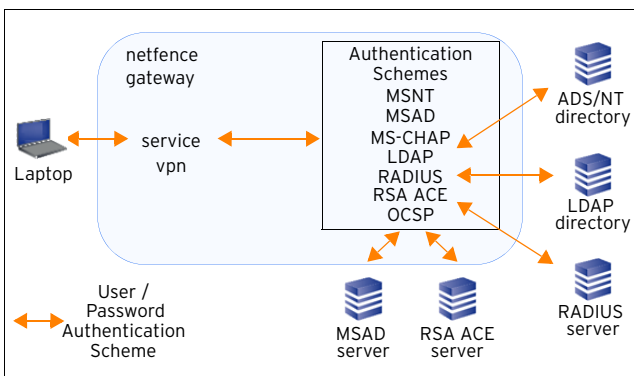
Parameter	Description
<b>Max Memory Used</b>	Sets an upper bound for memory usage before the repair binary steps into action (default: 95 %). <b>Note:</b> Both RAM and swap space are taken into account.
<b>Check System Load</b>	Set to <b>yes</b> (default) in order to have watchdog monitor the average system load.
<b>Max Load [1min]</b>	Maximum 1 min average system load. Default is <b>24</b> .
<b>Max Load [5mins]</b>	Maximum 5 mins average system load. Default is <b>18</b> .
<b>Max Load [15mins]</b>	Maximum 15 mins average system load. Default is <b>12</b> .
<b>Watch Control Daemon</b>	Set to <b>yes</b> to have watchdog monitor the process state of control daemon. See the explanation above for details.
<b>Watch SSH Daemon</b>	Set to <b>yes</b> to have watchdog monitor the process state of SSH daemon. See the explanation above for details. <b>Note:</b> Whenever the repair utility is invoked it will log the error passed to it by watchdog and all actions taken by it into log tree node <b>Box &gt; Watchdog &gt; Sysrepair</b> . Moreover you will be actively notified by the event notification mechanism.

## 5.2 Box Settings - Infrastructure Services

### 5.2.1 Authentication Service

External user authentication for different services is provided by the phion infrastructure daemon (aka **phibsd**).

**Fig. 3-64** Scheme for external authentication provided by the phion infrastructure daemon



**Note:** OCSP is not available for direct end user authentication but is used for online certificate verification by the VPN server.

The internal mechanism is as follows:

**Step 1** A service like vpn or proxy is configured to perform external user authentication. In its configuration it has to know a scheme to do that.

**Step 2** It gives the authentication request together with the scheme name to the phion infrastructure daemon which tries to authenticate the user according to the received scheme by itself.

To provide both, referential integrity and flexibility, there are predefined schemes, which can be referenced by all services. Due to their underlying authentication facility they are called:

- MSNT (see 5.2.1.6 MSNT Authentication)
- Active Directory (see 5.2.1.1 MSAD Authentication, page 111 and 5.2.1.2 MS-CHAP Authentication, page 112)
- LDAP (see 5.2.1.3 LDAP Authentication, page 113)
- RADIUS (see 5.2.1.4 Radius Authentication, page 114)
- RSA ACE (see 5.2.1.5 RSA-ACE Authentication, page 114)
- OCSP (Online Certificate Status Protocol; see 5.2.1.7 OCSP Authentication, page 115)

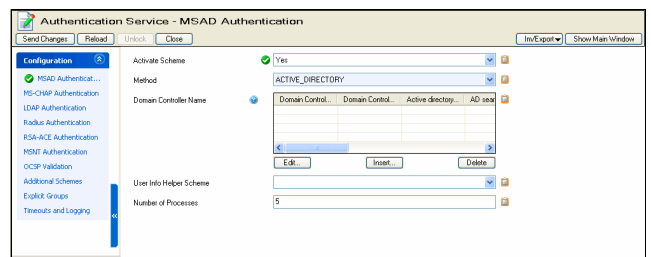
**Note:** For testing your authentication schemes without having/configuring proxy and VPN, phion provides a tool called **phibstest** (located in `/opt/phion/bin`). Use extension `phibstest -h` for additional information concerning the usage of this tool.

Furthermore, you can introduce more schemes to authenticate users, but you are not allowed to give them one of the names above. It is also forbidden to use the name **local** since it is used by the services to use internal authentication.

To open, select **Infrastructure Services > Authentication Service** and double-click.

#### 5.2.1.1 MSAD Authentication

**Fig. 3-65** Configuration Dialogue - MSAD Authentication



**Attention:** If the Active Directory of the Windows 2003 Server domain is running in Native mode, it is mandatory to deactivate Kerberos pre-authentication for each user.

**Attention:**

Having the domain as BaseDN (for example DC=xyz,DC=com) can cause problems as Active Directory may refuse the BaseDN lookup. The behaviour is irrational, though. If possible, add an OU= entry to your BaseDN.

**Note:**

Please consider that the administrator must have corresponding read access.

List 3-117 MSAD Authentication

Parameter	Description
<b>Activate Scheme</b>	Setting to <b>yes</b> (default: <b>no</b> ) starts the corresponding authentication processes and makes the configuration section <b>Domain Controller Name</b> available.
<b>Method</b>	This is the authentication method the scheme utilises (read-only).
<b>Basic</b>	Click the <b>Insert ...</b> button to enter the domain controller configuration dialogue. See list 3-118, list 3-119, and list 3-120 for parameter description.
<b>User Info Helper Scheme</b>	Select one of the authentication schemes in the combo box if users group information should be gained from a different authentication scheme. For example, if the identity verification should use the radius scheme, but group information should be queried from a LDAP directory. In this case configure "LDAP" as User Info Helper Scheme in the RADIUS scheme and use the RADIUS scheme as authentication scheme (in the VPN configuration). Only authentication schemes of type MSAD or LDAP may be used as <b>User Info Helper Scheme</b> .
<b>Number of Processes</b>	Number of authentication processes that are launched to handle requests. Increase if you have slow authentication servers (default: 5).

List 3-118 MSAD Authentication - Basic - section Basic

Parameter	Description
<b>Domain Controller Name</b>	This is the name of the primary domain controller without domain suffix. The name must be DNS-resolvable.
<b>Domain Controller IP</b>	Optionally, insert the IP address of the domain controller. If given, the IP address overrules the host name.
<b>Active directory searching user</b>	This is the DN (Distinguished Name) of the user with permission to search MSAD (Microsoft Active Directory) and to view group information. <b>Note:</b> The distinguished name can be viewed in the attribute field of the user (management console) ( <b>Appendix - 1.1.1 MSAD, page 524</b> ).
<b>AD searching user password</b>	These fields expect the searching user's password.
<b>Base DN</b>	This parameter specifies where to search for user information. The more ample the Base DN is configured (for example only <b>DC=...</b> ) the longer the search will take.
<b>Use MSAD-groups with NTLM</b>	Set to <b>yes</b> (default: <b>no</b> ) to synchronise user groups from MSAD periodically and let the netfence gateway handle them offline. MSAD offline-groups are needed for NTLM-authentication. <b>Note:</b> If you have configured an <b>MS-CHAP</b> Authentication Scheme at the same time, see <b>Netbios Domain Name</b> , page 112 for details on domain name assignment.
<b>Cache MSAD-groups</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables the MSAD searching user to retrieve group information from the periodically synchronised database. Querying the database will reduce network-traffic and server-load on the MSAD server. <b>Note:</b> Set parameter <b>Use MSAD-groups with NTLM</b> (see above) to <b>yes</b> if you want to use this function.
<b>Offline sync (every n min./hour)</b>	This parameter specifies how often to synchronise the offline database. Default setting is every <b>60</b> minutes per hour.

List 3-119 MSAD Authentication - Basic - section Mail Lookup

Parameter	Description
<b>Additional Mail Fields</b>	Enhanced mail lookup for mail-gateways recipient lookup: <ul style="list-style-type: none"> <li>➤ The MSAD-field <b>proxyAddresses</b>, which is used in MSAD for the mail-aliases: all in MSAD configurable mail-addresses will be found by a mailgw recipient lookup.</li> <li>➤ Configuration field <b>Additional Mail Fields</b>: this field takes a comma separated list of meta-directory field names, which are searched for a mail address too. This configuration field may not contain spaces. Only LDAP attributes are allowed (explicit), and no GUI description fields. If you are not sure use an LDAP browser.</li> <li>➤ in contrast to the default fields <b>mail</b> and <b>proxyAddresses</b>, all additional fields are search by means of pattern search (prepended * and appended *)</li> </ul>

List 3-120 MSAD Authentication - Basic - section Extended

Parameter	Description
<b>Use SSL</b>	Select the <b>Use SSL</b> checkbox to establish the connection to the LDAP directory using SSL.
<b>Follow Referrals</b>	Select the <b>Follow referrals</b> check box to search the MSAD Global Catalogue and follow LDAP Referrals.
<b>Max. Hops for Referrals</b>	This field specifies the maximum referrals to follow.

### 5.2.1.2 MS-CHAP Authentication

The Microsoft Challenge Handshake Authentication Protocol Version 2 (**MS-CHAP V2**) authentication method can be used to authenticate VPN clients over PPTP and L2TP. In addition, it can be used for proxy authentication. To use the MSCHAPv2 authentication method with a netfence gateway it is required to integrate the netfence gateway as a member into a Windows domain (NT4, Windows 2000, and Windows 2003 domains).

**Note:**

Use the **Domain Control** button, accessible through the **Box** tab in the **Control Centre** to add a netfence gateway to a Windows domain (**Control Centre - 2.6 Box Tab, page 38**).

List 3-121 Parameters for MS-CHAP Authentication

Parameter	Description
<b>Activate Scheme</b>	Setting to <b>yes</b> (default: <b>no</b> ) starts authentication processes required for this scheme and activates domain configuration fields below.
<b>Method</b>	This is the authentication method the scheme utilises (read-only).
<b>Domain Realm</b>	This is the name of the Windows domain the authenticator is going to query.
<b>Netbios Domain Name</b>	If the Netbios domain name differs from the MS Active Directory domain name, insert the NetBIOS domain name into this field. The Netbios domain name is applicable when a user logs on to a Windows domain. Domain name association must therefore be specified unambiguously, in order to guarantee a user's correct group assignment. <b>Note:</b> This configuration option is of importance especially in conjunction with: user group synchronisation, which is needed for NTLM authentication (see <b>Use MSAD-groups with NTLM, page 112</b> ). ISS Proventia Web Filter configuration when user group filters apply (see <b>Affected Groups / Users, page 345</b> ).
<b>Workgroup Name</b>	MS Active Directory workgroup name. Use this field if the workgroup name differs from the MS Active Directory domain name ( <b>Domain Realm</b> ).

**List 3-121** Parameters for MS-CHAP Authentication

Parameter	Description
<b>Domain Controller</b>	This is the IP address of the domain controller. <b>Note:</b> If you have additionally configured an MSAD authentication scheme (see 5.2.1.1 MSAD Authentication) utilising the option <b>Use MSAD-groups with NTLM</b> (see page 112), the netfence gateway must be able to resolve the DNS name of the Domain Controller.
<b>WINS Server</b>	This is the IP address of the domain's Windows Internet Name Service (WINS) server. <b>Note:</b> If you have additionally configured an MSAD authentication scheme (see 5.2.1.1 MSAD Authentication) utilising the option <b>Use MSAD-groups with NTLM</b> (see page 112), the netfence gateway must be able to resolve the DNS name of the WINS server.
<b>User Info Helper Scheme</b>	Select one of the authentication schemes in the combo box if users group information should be gained from a different authentication scheme. For example, if the identity verification should use the radius scheme, but group information should be queried from a LDAP directory, then configure "LDAP" as User Info Helper Scheme in the RADIUS scheme and use the RADIUS scheme as authentication scheme for example in the VPN configuration. Only authentication schemes of type MSAD or LDAP may be used as <b>User Info Helper Scheme</b> .
<b>Number of Processes</b>	Number of authentication processes that are launched to handle requests. Increase if you have slow authentication servers (default: 5).
<b>Net Join Status</b>	This field is a read only informational field showing the status of the join to the Windows domain.

### 5.2.1.3 LDAP Authentication

**List 3-122** Parameters for LDAP Authentication - section LDAP

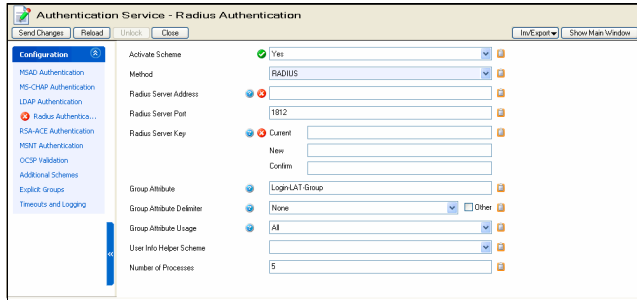
Parameter	Description
<b>Activate Scheme</b>	If set to <b>yes</b> (default: <b>no</b> ) the corresponding authentication processes are started and the configuration section <b>LDAP Base DN</b> is available.
<b>Method</b>	Displays the selected method (read-only field).

**List 3-122** Parameters for LDAP Authentication - section LDAP

Parameter	Description
<b>LDAP Base DN</b>	If set to <b>yes</b> (default: <b>no</b> ) the corresponding authentication processes are started and the configuration section <b>LDAP Base DN</b> is available.
<b>LDAP Base DN</b>	Distinguished name for user organisational unit.
<b>LDAP Server</b>	IP address the LDAP authenticator asks.
<b>LDAP Server Port</b>	Port of the LDAP server (default: 389).
<b>LDAP User Field</b>	Name of the User field in the LDAP directory.
<b>LDAP Password Field</b>	Name of the Password field in the LDAP directory.
<b>LDAP Admin DN</b>	Name of an administrator who is authorised to perform requests.
<b>LDAP Admin Password</b>	Password of an administrator who is authorised to perform requests.
<b>Group Attribute</b>	Name of the attribute field on the LDAP server containing group information. Note that attribute fields on LDAP server are customisable. If you are unsure about the required field name, the LDAP server administrator will be able to provide the correct information. <b>Note:</b> Services that process group information (for example ISS Proventia Web Filter, see Affected Groups / Users, page 345) require Group Attribute specification. They will not be able to match group conditions if the attribute field is not or is specified incorrectly.
<b>Use SSL</b>	When selected the authenticator uses SSL for connections to the authentication server.
<b>Bind To Authenticate</b>	When selected the authenticator directly logs on to the LDAP server for verification of user authentication data. Use this option, when the LDAP server does not expose user passwords but instead hides them even from an administrator's view.
<b>User Info Helper Scheme</b>	Select one of the authentication schemes in the combo box if users group information should be gained from a different authentication scheme. For example, if the identity verification should use the radius scheme, but group information should be queried from a LDAP directory, then configure "LDAP" as User Info Helper Scheme in the RADIUS scheme and use the RADIUS scheme as authentication scheme for example in the VPN configuration. Only authentication schemes of type MSAD or LDAP may be used as <b>User Info Helper Scheme</b> .
<b>Number of Processes</b>	Number of authentication processes that are launched to handle requests. Increase if you have slow authentication servers (default: 5).

### 5.2.1.4 Radius Authentication

Fig. 3-66 Configuration Dialogue - Radius

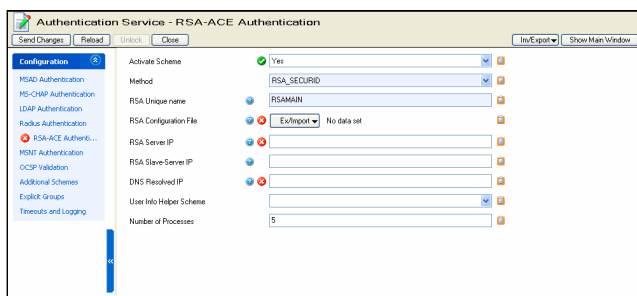


List 3-123 Parameters for Radius Authentication

Parameter	Value
<b>Activate Scheme</b>	If set to <b>yes</b> the corresponding authentication processes are started.
<b>Method</b>	Displays the selected method (read-only field).
<b>Radius Server Address</b>	IP address the RADIUS authenticator asks.
<b>Radius Server Port</b>	Port of the RADIUS server (default: 1812).
<b>Radius Server Key</b>	Pre-shared secret to authorise the request. <b>Attention:</b> Do not use backslashes in your key.
<b>Group Attribute</b>	Due to the structure of RADIUS and its implementation into phion netfence, the group information has to be entered into <b>Login-LAT-Group</b> (as defined in this read-only-field) in order to be processed.
<b>Group Attribute Delimiter</b>	The delimiter divides groups and therefore allows you to use more than one group. The standard options are <b>None</b> (default) and <b>Blank</b> . By ticking the check box <b>Other</b> it is possible to enter any character that indicates a group info change.
<b>Group Attribute Usage</b>	Through this parameter you define the group information that is going to be used (for example, <b>CN=...</b> , <b>OU=...</b> , <b>DC=...</b> ). The available options are <b>All</b> (default), <b>First</b> and <b>Last</b> .
<b>User Info Helper Scheme</b>	Select one of the authentication schemes in the combo box if users group information should be gained from a different authentication scheme. For example if the identity verification should use the radius scheme, but group information should be queried from a LDAP directory, then configure "LDAP" as User Info Helper Scheme in the RADIUS scheme and use the RADIUS scheme as authentication scheme for example in the VPN configuration. Only authentication schemes of type MSAD or LDAP may be used as <b>User Info Helper Scheme</b> .
<b>NAS-ID</b>	This is the NAS identifier.
<b>NAS IP Address</b>	Some radius server require NAS credentials to be set. Define in this field the IP address.
<b>NAS IP Port</b>	Some radius server require NAS credentials to be set. Define in this field the IP port.
<b>Number of Processes</b>	Number of authentication processes that are launched to handle requests. Increase if you have slow authentication servers (default: 5).

### 5.2.1.5 RSA-ACE Authentication

Fig. 3-67 Configuration Dialogue - RSA SECURID

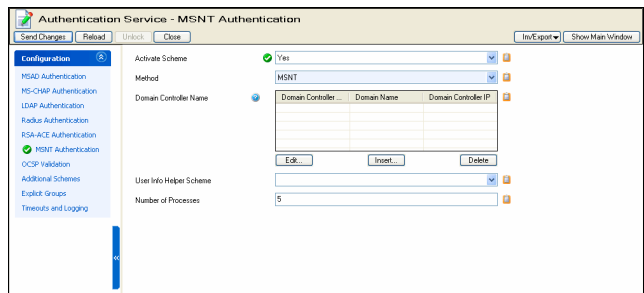


List 3-124 Parameters for RSA-ACE Authentication

Parameter	Description
<b>Activate Scheme</b>	If set to <b>yes</b> the corresponding authentication processes are started.
<b>Method</b>	Displays the selected method (read-only field).
<b>RSA Unique Name</b>	Displays the name of the RSA server (read-only field).
<b>RSA Configuration File</b>	This parameter serves to import/export the configuration file that is provided by the RSA SecurID server ( <code>sdconf.rec</code> ).
<b>RSA Server IP</b>	This IP address is the one of the RSA Server.
<b>RSA Slave-Server IP</b>	Optionally it is possible to enter a slave server in order to maintain connectivity.
<b>DNS Resolved IP</b>	This IP address indicates the one that is used to connect to the RSA server. If this IP address does not correspond to the configured client IP the server has, the connection will be refused.
<b>User Info Helper Scheme</b>	Select one of the authentication schemes in the combo box if users group information should be gained from a different authentication scheme. For example if the identity verification should use the radius scheme, but group information should be queried from a LDAP directory, then configure "LDAP" as User Info Helper Scheme in the RADIUS scheme and use the RADIUS scheme as authentication scheme, for example in the VPN configuration. Only authentication schemes of type MSAD or LDAP may be used as <b>User Info Helper Scheme</b> .
<b>Number of Processes</b>	Number of authentication processes that are launched to handle requests. Increase if you have slow authentication servers (default: 5).

### 5.2.1.6 MSNT Authentication

Fig. 3-68 Configuration Dialogue - MSNT



List 3-125 Parameters for MSNT Authentication

Parameter	Description
<b>Activate Scheme</b>	Setting to <b>yes</b> (default: <b>no</b> ) starts the corresponding authentication processes and makes the configuration section <b>Domain Controller Name</b> available.
<b>Method</b>	This is the authentication method the scheme utilises (read-only).
<b>Domain Controller Name</b>	This is the host name of the system the authenticator asks. The host name has to be DNS-resolvable by the name server the netfence gateway queries. Click the <b>Insert ...</b> button to enter the domain controller configuration dialogue.
<b>Domain Controller Name</b>	This is the name of the primary domain controller without domain suffix. The name must be DNS-resolvable.
<b>Domain Name</b>	This is the name of the domain.
<b>Domain Controller IP</b>	Insert the IP address of the domain controller. This IP address overrules the host name.
<b>User Info Helper Scheme</b>	Select one of the authentication schemes in the combo box if users group information should be gained from a different authentication scheme. For example if the identity verification should use the radius scheme, but group information should be queried from a LDAP directory, then configure "LDAP" as User Info Helper Scheme in the RADIUS scheme and use the RADIUS scheme as authentication scheme, for example in the VPN configuration. Only authentication schemes of type MSAD or LDAP may be used as <b>User Info Helper Scheme</b> .

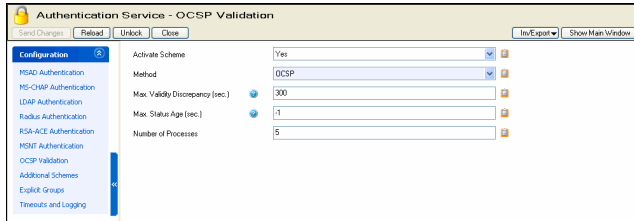


List 3-125 Parameters for MSNT Authentication

Parameter	Description
<b>Number of Processes</b>	Number of authentication processes that are launched to handle requests. Increase if you have slow authentication servers (default: 5).

### 5.2.1.7 OCSP Authentication

Fig. 3-69 Configuration Dialogue - OCSP



List 3-126 Parameters for OCSP Authentication

Parameter	Description
<b>Activate Scheme</b>	If set to <b>yes</b> (default: <b>no</b> ) the corresponding authentication processes are started.
<b>Method</b>	Displays the selected method (read-only field).
<b>Max. Validity Discrepancy (sec.)</b>	Defines the time gap between nefence gateway and the OCSP server (default: <b>300</b> seconds). If the time difference exceeds this limit, requests are counted as not valid.
<b>Max. Status Age (sec.)</b>	Specifies the maximum status age of requests (default: <b>-1</b> that is unlimited). OCSP servers hold files containing the current status and attach this value to the info section. As soon as this threshold is exceeded the request is counted as not valid.
<b>Number of Processes</b>	Number of authentication processes that are launched to handle requests. Increase if you have slow authentication servers (default: 5).

### 5.2.1.8 Additional Schemes

Use this configuration section to introduce additional authentication schemes. An additional scheme may for example configure usage of a second proxy server in your network with an alternative authentication server. The number of additional schemes has no limitation.

The available settings/options are the same as the ones described under 5.2.1 Authentication Service, page 111.

**Note:**

References to additional schemes are not checked for integrity. Be aware that schemes may be deleted though VPN users rely on their existence.

### 5.2.1.9 Explicit Groups

This tab allows assigning user names to groups (especially for authentication schemes that do not provide group information such as MSAD or RSA ACE).

List 3-127 Parameters for Explicit Authentication

Parameter	Description						
	Use the Edit ..., Insert ... and Delete buttons to modify the configuration of Explicit Groups.						
<b>Explicit Groups</b>	<table border="1"> <thead> <tr> <th>Group Name</th> <th>Define a group name here.</th> </tr> <tr> <th>Login Name</th> <th>Create users here which should belong to the group just defined. Be sure to add the users to the listing on the right by clicking <b>Insert ...</b></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Group Name	Define a group name here.	Login Name	Create users here which should belong to the group just defined. Be sure to add the users to the listing on the right by clicking <b>Insert ...</b>		
Group Name	Define a group name here.						
Login Name	Create users here which should belong to the group just defined. Be sure to add the users to the listing on the right by clicking <b>Insert ...</b>						
<b>External DB Files</b>	If group/user information is already available in Berkeley DB files, a reference to these files may be placed here.						

### 5.2.1.10 Timeouts and Logging

List 3-128 Parameters for Timeouts and Logging - section Log Settings

Parameter	Description
<b>Log Groups</b>	Set to <b>yes</b> if user group information should be reported in the log.
<b>Log Add. Meta-directory Fields</b>	Set to <b>yes</b> if additional meta-directory fields should be reported in the log.

List 3-129 Parameters for Timeouts and Logging - section Timeout Settings

Parameter	Description
<b>Request Timeout (sec)</b>	Define here authentication timeout.
<b>Challenge Timeout (sec)</b>	Define here the NTLM/MS-CHAP challenge timeout.

## 5.2.2 Host Firewall Rules

See **Firewall** - 3. Local Rules, page 162

## 5.2.3 Syslog Streaming

The Syslog Streaming configuration defines the handling of log file messages which are to be transferred to another system for analysing purposes. Log messages of MC-administered boxes can be transmitted to their MC (MC Syslog server), but they can just as well be transmitted to any other system designed for log file collection. The following configuration sections allow specification of the transmission process.

**Note:**

If log messages are transferred to a phion MC Syslog Server please consult **phion management centre** - 11. MC Syslog, page 446 for additional information.

### 5.2.3.1 Basic Setup

List 3-130 Infrastructure Services - Syslog Streaming - Basic Setup - section Operational Setup

Parameter	Description
<b>Idle Mode</b>	Syslogging is activated by default (setting <b>no</b> , which means not idle). When active, the service listens for incoming log messages from its managed boxes and hence processes them as configured through the following parameters. Nonetheless, even when idle (setting <b>yes</b> , which means system is idle) it as well listens for incoming messages to avoid ICMP Port Unreachable messages being sent back to the connecting systems. It then simply discards the received messages.
<b>Max Queued Messages</b>	Via this parameter, the maximum possible number of log entries fitting into the output queue can be defined (default 4096). The out-message queue is used when writing to disk, transferring to MC or when having relay targets (external log host).  If the number of entries in the output queue exceeds this limit, further log entries are lost. It is therefore important to set this parameter to the estimated number of messages in a message burst. If bursts extend the bandwidth of the external log host, the syslog-engine can buffer the messages and feed them into the destination pipe after the burst has collapsed.
<b>Max Int TCP Conns</b>	This parameter applies to the maximum number of concurrent loopback connections to the syslog proxy. Since this number normally is very low the default value (50) can be used.
<b>TCP Retry Interval</b>	The time to wait before an expired connection (to MC or external log host) is re-established. Note that this parameter only applies to log destinations with TCP specified as Transmission Mode.

**List 3-130** Infrastructure Services - Syslog Streaming - Basic Setup - section Operational Setup

Parameter	Description
<b>GC Idle Threshold</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>This parameter defines the threshold (number of objects in memory) after which garbage collection is initiated when idle (no messages within 10 ms; default: <b>200</b>).</p>
<b>GC Busy Threshold</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>This parameter defines the threshold (number of objects in memory) after which garbage collection is initiated even when busy (default: <b>3000</b>).</p> <p>If this limit is exceeded messages will be lost.</p>

**List 3-131** Infrastructure Services - Syslog Streaming - Basic Setup - section System Identification & Authentication

Parameter	Description
	<p><b>Note:</b> This parameter group is only available in <b>Advanced View</b> mode.</p>
<b>Use Box Certificate/Key</b>	<p>Defines the certificate/key used by the box for SSL based authentication to a destination system. Setting this parameter to <b>yes</b> (as it is by default) means that actual box certificate and private key as listed in configuration node <b>Identity</b> are used. <b>No</b> means that a separate service specific certificate is used (see entries below).</p> <p><b>Note:</b> Set this parameter to yes if log files a streamed without SSL Encapsulation, as setting no turns SSL Private Key and Certificate into mandatory values.</p>
<b>SSL Private Key</b>	<p>If the parameter above is set to <b>no</b>, this value contains the 1024 bit RSA key optionally used for SSL based authentication.</p>
<b>SSL Certificate</b>	<p>If the parameter above is set to <b>no</b>, this value contains the digital x.509v3 compliant self signed certificate (by key above) used for SSL based authentication.</p>

### 5.2.3.2 Logdata Filters

#### Section LOG FILTERS

This section enables defining profiles specifying the log file types to be transferred / streamed ...

**Fig. 3-70** Infrastructure Services - Syslog Streaming - Logdata Filters - section Top Level Logdata

Parameter	Description
<b>Data Selection</b>	<p>The log files offered for selection here are superordinate log files built up of several instances of box and service levels. The following data can be selected:</p> <p><b>Fatal_log.</b> These are the log contents of the fatal log (log instance name: fatal)</p> <p><b>Firewall_Audit_Log.</b> These are the log contents of the firewall's machine readable audit data stream. Whether data is streamed into the <b>Firewall_Audit_Log</b> has to be configured in the Firewall Parameter Settings on box-level (see SECTION Audit Info Generation &gt; Audit-Delivery: <b>Syslog-Proxy</b>). The log instance name corresponding to <b>Syslog-Proxy</b> selected will be trans7.</p> <p><b>Note:</b> When "Log-File" is selected in the firewall's configuration the data will go into a log file named Box-&gt;Firewall-&gt;audit (which means the instance is named box_Firewall_audit) and thus this filter setting is not applicable. The pertinent one then would be a selection of category "Firewall" within the box selection portion of the filter.</p>

**List 3-132** Infrastructure Services - Syslog Streaming - Logdata Filters - section Affected Box Logdata

Parameter	Description
<b>Data Selector</b>	<p>This parameter defines what kind of box logs are to be affected by the syslog daemon. The following options are available: <b>All</b> (any kind of box log is affected), <b>None</b> (none is affected) and <b>Selection</b> (default; activates parameter group <b>Data Selection</b>, see below).</p>
<b>Data Selection</b>	<p>Take into consideration that this parameter group is only available if parameter <b>Data Selector</b> is set to <b>Selection</b>. The following parameters are available for configuration:</p>
<b>Log Groups</b>	<p>This menu offers every log group for selection that is available on a netfence gateway (For example, Control, Event, Firewall, ...).</p>
<b>Log Message Filter</b>	<p>This parameter is used for defining the affected log types:</p> <ul style="list-style-type: none"> <li>• <b>Selection</b> (activates parameter <b>Selected Message Types</b>, see below)</li> <li>• <b>All</b> (default)</li> <li>• <b>All-but-Internal</b></li> <li>• <b>Notice-and-Higher</b></li> <li>• <b>Warning-and-Higher</b></li> <li>• <b>Error-and-Higher</b></li> </ul> <p>As can be seen the available options are "group selections". If one explicit log type is required, choose <b>Selection</b> and set the wanted type in parameter <b>Selected Message Types</b>, see below.</p>
<b>Selected Message Types</b>	<ul style="list-style-type: none"> <li>- <b>Selected Message Types</b></li> </ul> <p>This parameter allows setting explicit log types to be affected by syslogging. The following types are available:</p> <ul style="list-style-type: none"> <li>• <b>Panic</b></li> <li>• <b>Security</b></li> <li>• <b>Fatal</b></li> <li>• <b>Error</b></li> <li>• <b>Warning</b></li> <li>• <b>Notice</b></li> <li>• <b>Info</b></li> <li>• <b>Internal</b></li> </ul>

**List 3-133** Infrastructure Services - Syslog Streaming - Logdata Filters - section Affected Service Logdata

Parameter	Description
<b>Data Selector</b>	<p>This parameter defines what kind of logs created by services are to be affected by the syslog daemon. The following options are available: <b>All</b> (any kind of service log is affected), <b>None</b> (none is affected) and <b>Selection</b> (default; activates parameter group <b>Data Selection</b>, see below).</p>
<b>Data Selection</b>	<p>Take into consideration that this parameter group is only available if parameter <b>Data Selector</b> is set to <b>Selection</b>.</p>
<b>Log Server-Services</b>	<p>Here you define server and service where log messages are streamed from.</p>
<b>Log Message Filter</b>	<p>This parameter is used for defining the affected log types:</p> <ul style="list-style-type: none"> <li>• <b>Selection</b> (activates parameter <b>Selected Message Types</b>, see below)</li> <li>• <b>All</b> (default)</li> <li>• <b>All-but-Internal</b></li> <li>• <b>Notice-and-Higher</b></li> <li>• <b>Warning-and-Higher</b></li> <li>• <b>Error-and-Higher</b></li> </ul>
<b>Selected Message Types</b>	<p>This parameter allows setting explicit log types to be affected by syslogging. The following types are available:</p> <ul style="list-style-type: none"> <li>• <b>Panic</b></li> <li>• <b>Security</b></li> <li>• <b>Fatal</b></li> <li>• <b>Error</b></li> <li>• <b>Warning</b></li> <li>• <b>Notice</b></li> <li>• <b>Info</b></li> <li>• <b>Internal</b></li> </ul>



### 5.2.3.3 Logstream Destinations

This section enables defining profiles specifying the transfer / streaming destination of log messages.

**List 3-134** Infrastructure Services - Syslog Streaming - Logstream Destinations - section Destination Address

Parameter	Description
<b>Remote Loghost</b>	Since an MC-administered box knows its corresponding MCs IP address, a predefined destination <b>Management-Centre</b> can be selected. When an external log host is used, the setting <b>explicit IP</b> (default) activates the parameter <b>Loghost IP Address</b> (see below) where the destination IP has to be entered.
<b>Loghost IP Address</b>	This parameter is only available if <b>Remote Loghost</b> has been set to <b>explicit IP</b> . In this case, the destination IP address of an external log host has to be entered here.
<b>Loghost Port</b>	This parameter defines the destination port for delivering syslog messages. The phion MC syslog service listens on port TCP 5143 for SSL connections and on TCP and UDP port 5144 for unencrypted streaming. The default is to use encryption for delivery, therefore port 5143 is preconfigured.  <b>Attention:</b> If you change the port assignment to another port, adjusting the local firewall rule set might become necessary.

**List 3-135** Infrastructure Services - Syslog Streaming - Logstream Destinations - section Data Transfer Setup

Parameter	Description
<b>Transmission Mode</b>	This parameter allows selecting the transmission protocol ( <b>TCP</b> or <b>UDP</b> - default; for SSL connections TCP is automatically set).
<b>Sender IP</b>	Defines the IP address used for sending the log data.
<b>Use SSL Encapsulation</b>	This option may be turned off when the log stream is transmitted to the MC and the box has a management tunnel to the MC. For MC transmission without box tunnel activating this option is recommended. Note also that transmission to a non-netfence system should be SSL encapsulated for reasons of privacy.
<b>Peer SSL Certificate</b>	This parameter is only active if the destination system is not a phion management centre. The <b>Peer SSL Certificate</b> is needed when <b>verify_peer_with_locally_installed_certificate</b> has been defined at parameter <b>SSL Peer Authentication</b> and parameter <b>Use SSL Encapsulation</b> has been set to <b>yes</b> .
<b>SSL Peer Authentication</b>	Defines the way in which a destination system is authenticated when using SSL based authentication (authentication of the destination server by the box being a client). The list offers the following choices: <b>verify_peer_with_locally_installed_certificate</b> (default) - The destination system is verified against a locally stored certificate either in the respective destination section or the MCs certificate. This setting is useful when log messages are delivered to a system outside the scope of phion management centres.  <b>Note:</b> For centrally administered netfence gateways this is the only applicable option. <b>verify_peer_certificate</b> - The destination system is verified against a locally stored CA certificate. <b>no_peer_verification</b> - The peer is considered as trusted without verification.  <b>Attention:</b> For security reasons it is NOT recommended to use <b>no_peer_verification</b> .

**List 3-136** Infrastructure Services - Syslog Streaming - Logstream Destinations - section Log Data Tagging

Parameter	Description
<b>Override Node Name</b>	The log entities sent to an external log host contain the name and structural information (range/cluster) of the sending box and the name of the log file. With this parameter set to <b>yes</b> this information can be overridden (default: <b>no</b> ).
<b>Explicit Node Name</b>	Only available if <b>Override Node Name</b> set to <b>yes</b> . Setting this value an explicit node name can be set. This node name is inserted into each log entity sent to the external log host.

**List 3-136** Infrastructure Services - Syslog Streaming - Logstream Destinations - section Log Data Tagging

Parameter	Description
<b>Prepend Hierarchy Info</b>	Only available if <b>Override Node Name</b> set to <b>yes</b> . This parameter allows fine tuning of the prefix which is inserted into each log entity sent to the external log host.
<b>Add UTC Offset</b>	Log files generated on a box are stamped with the local box time. The UTC time offset compared to the local time is recorded though, and can be examined in the <b>TZ</b> column in the log viewer ( <b>Log Viewer</b> - 2.3 View Segment, page 292). The UTC time offset information is not included by default (setting: <b>no</b> ) when log files are streamed to the management centre. Setting to <b>yes</b> adds the UTC time offset information to streamed log files, so that these files may be analysed uniformly in case the MC collects log files from multiple boxes placed in various time zones.

### 5.2.3.4 Logdata Streams

By configuring this section relations between log patterns and log destinations are established. Thus it is possible to make a combination of each log pattern (a sort of filter) and log destination to allow fine granulated target selection.

**Note:**  
With **Management-Centre** selected as **Remote Loghost** the streamed log files will be stored under `/phion0/mlogs/range/cluster/box` on the MC.

**List 3-137** Infrastructure Services - Syslog Streaming - Logdata Streams - section Stream Configuration

Parameter	Description
<b>Active</b>	This parameter allows you to activate/deactivate the selected log stream profile. By default, for example when creating a new profile, this parameter is set to <b>yes</b> .
<b>Log Destinations</b>	Here the available log destinations (defined in 5.2.3.3 Logstream Destinations, page 117) can be selected.
<b>Log Filters</b>	Here the available log patterns (defined in 5.2.3.2 Logdata Filters, page 116) can be selected.

## 5.2.4 Control

Browse to **Infrastructure Services > Control** to open the configuration area. The configuration options in this place amongst others allows you to define the limits determining when the events High System Load (Event-ID 30) and Excessive System Load (Event-ID 31) are generated. It as well allows you to customise the time interval, after which idle phion.a- and SSH-sessions are automatically terminated.

### 5.2.4.1 Monitoring Setup

**List 3-138** Infrastructure Services - Control - Monitoring Setup - section Monitoring Parameters

Parameter	Description
<b>Startup Poll Interval [secs]</b>	This parameter specifies the period of time that has to expire after booting or activating the network until a HA action can take place (default: 10). This is important especially with "slow learning" NICs that need quite a time after booting/activating until the link is activated.

**List 3-138** Infrastructure Services - Control - Monitoring Setup - section Monitoring Parameters

Parameter	Description
<b>Regular Poll Interval [secs]</b>	This parameter defines the amount of time between the HA heartbeats. The smaller the values are, the faster HA reaction can take place (default: 5 seconds). The default value prevents too fast HA take-overs. When you are using the Firewall with transparent failover feel free to set this parameter to 1 second. But take into consideration that the partner system reacts instantly with a take-over during server starts/stops or network activation. In this case first block the server before doing anything else.  <b>Note:</b> This parameter also affects the reaction time for activating/deactivating routes and server (Monitor IPs).

**List 3-139** Infrastructure Services - Control - Monitoring Setup - section HA Monitoring Parameters

Parameter	Description						
<b>Translated HA IP</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>Translated HA IP</b></td> <td rowspan="3">For network setups providing a private uplink between two HA boxes, it is possible to define a translation table specifying the IP address to use for communication between the two HA partners. The <b>Translated HA IP</b> thereby identifies a box' primary Management IP as specified in the Box Network configuration dialogue (<b>Management IP (MIP)</b>, page 62). The <b>Alternative HA IP</b> is part of the private uplink network defined through Section Additional Local Networks, page 62,. The parameter <b>Usage</b> allows specifying, how to proceed if the alternative HA IP becomes unavailable.  <b>Attention:</b> Take into consideration that the <b>Alternative IP addresses</b> have to be added manually to the corresponding firewall rule (inbound).  <b>Note:</b> See <b>High Availability - 2</b>. Setting up a HA System, page 378 for a configuration example using Translated HA IPs in a private uplink network.</td> </tr> <tr> <td><b>Alternative HA IP</b></td> </tr> <tr> <td><b>Usage Policy Description</b></td> </tr> </tbody> </table>	Parameter	Description	<b>Translated HA IP</b>	For network setups providing a private uplink between two HA boxes, it is possible to define a translation table specifying the IP address to use for communication between the two HA partners. The <b>Translated HA IP</b> thereby identifies a box' primary Management IP as specified in the Box Network configuration dialogue ( <b>Management IP (MIP)</b> , page 62). The <b>Alternative HA IP</b> is part of the private uplink network defined through Section Additional Local Networks, page 62,. The parameter <b>Usage</b> allows specifying, how to proceed if the alternative HA IP becomes unavailable.  <b>Attention:</b> Take into consideration that the <b>Alternative IP addresses</b> have to be added manually to the corresponding firewall rule (inbound).  <b>Note:</b> See <b>High Availability - 2</b> . Setting up a HA System, page 378 for a configuration example using Translated HA IPs in a private uplink network.	<b>Alternative HA IP</b>	<b>Usage Policy Description</b>
Parameter	Description						
<b>Translated HA IP</b>	For network setups providing a private uplink between two HA boxes, it is possible to define a translation table specifying the IP address to use for communication between the two HA partners. The <b>Translated HA IP</b> thereby identifies a box' primary Management IP as specified in the Box Network configuration dialogue ( <b>Management IP (MIP)</b> , page 62). The <b>Alternative HA IP</b> is part of the private uplink network defined through Section Additional Local Networks, page 62,. The parameter <b>Usage</b> allows specifying, how to proceed if the alternative HA IP becomes unavailable.  <b>Attention:</b> Take into consideration that the <b>Alternative IP addresses</b> have to be added manually to the corresponding firewall rule (inbound).  <b>Note:</b> See <b>High Availability - 2</b> . Setting up a HA System, page 378 for a configuration example using Translated HA IPs in a private uplink network.						
<b>Alternative HA IP</b>							
<b>Usage Policy Description</b>							

**List 3-140** Infrastructure Services - Control - Monitoring Setup - section ICMP Gateway Monitoring Exemptions

Parameter	Description
<b>No Probing for Interfaces</b>	This parameter allows excluding gateways that are reachable via the offered interface items from regular ICMP-based probing. The following interfaces are available: <b>UMTS-Link</b> <b>xDSL-Link</b> <b>DHCP-Link</b> <b>ISDN-Link</b> <b>SERIAL-Link</b>

### 5.2.4.2 Administrative Sessions

**List 3-141** Infrastructure Services - Control - Administrative Sessions - section Auto Logout Setup

Parameter	Description
<b>phiona Max. Idle [Mins.]</b>	This parameter defines the maximum idle time for a phiona session (default: 60min).  <b>Note:</b> After this time interval the session is closed and it must be re-established.
<b>Console Max. Idle [Mins.]</b>	This parameter defines the maximum idle time for a shell/SSH session (default: 60min).

**List 3-142** Infrastructure Services - Control - Administrative Sessions - section Session Password Setup

Parameter	Description
<b>Disable Session Passwords</b>	Creates a session password after the first successful login to a box. In the course of this first login the login credentials are verified against the information stored on the Smartcard/eToken. Subsequent access will then use the dynamically created session password thereby speeding up authentication.

### 5.2.4.3 CPU-Load Monitoring

Use this tab to define threshold values triggering generation of the events *High System Load* [30] and *Excessive System Load* [31].

The values entered into the configuration fields specify the maximum number of processes that may simultaneously wait for execution (in either inbound or outbound direction) within the given time until an event message is created. For example, the default value of **24** in the parameter field **Critical 1 Min. Average** means that as soon as the load has reached the number of 24 waiting processes within an average time of 1 minute, the event *Excessive System Load* [31] shall be created.

**List 3-143** Infrastructure Services - Control - CPU-Load Monitoring - section Performance

Parameter	Description
<b>Performance Statistics</b>	Select <b>yes</b> to collect performance statistic data.

**List 3-144** Infrastructure Services - Control - CPU-Load Monitoring - section CPU-Load Warning Thresholds

Parameter	Description
<b>Average 1/5/15 Mins</b>	These three parameters define threshold values for generation of Event-ID <i>High System Load</i> [30].

**List 3-145** Infrastructure Services - Control - CPU-Load Monitoring - section CPU Load Error Thresholds

Parameter	Description
<b>Average 1/5/15 Mins</b>	These three parameters define threshold values for generation of Event-ID <i>Excessive System Load</i> [31].

## 5.2.5 Statistics

For a description of **Statistics** see **Statistics - 3.1** Service Configuration, page 300.

## 5.2.6 Eventing

For a description of **Eventing** settings see **Eventing**, page 305.

## 5.2.7 General Firewall Configuration

For a description of **Firewall Settings** see **Firewall - 2.1.1** General Firewall Configuration, page 126.

### 5.2.8 Log Configuration

The log daemon is a box service and represents an integral part of the phion box infrastructure. Operation characteristics of the log daemon and instructions as to extract information from the system are to be found in **Log Viewer**, page 289.

**List 3-146** Infrastructure Services - Log Configuration - section Log Configuration

Parameter	Description
<b>Log to Disk</b>	This parameter activates/deactivates writing of log files to disk (default: <b>yes</b> ).  <b>Note:</b> Take into consideration that even when setting this parameter to no VPN server (IKE) and proxy will keep writing log files to the disk.

## 5.3 Creating PAR Files

For backup and recovery reasons, the complete box configuration may be exported into the phion proprietary PAR (**phion Archive**) file.

A PAR file stores the following configuration elements:

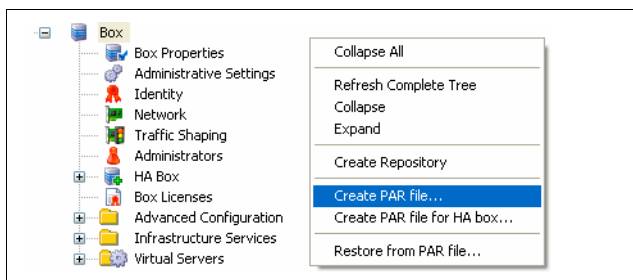
- Box configuration and settings
- Server and service settings
- Repository settings

PAR files are applicable for the following tasks:

- Restore box and management centre Configurations (see 5.4 Restoring/Importing from PAR File)
- Re-install a system with kickstart disk and PAR file (**Getting Started** - 1.3 Installation with a Saved Configuration, page 8)

PAR files may be created from the following places in the configuration tree:

**Fig. 3-71** Creating a PAR file



#### On single boxes and on box level of management centres:

- Right-click **Box** in the configuration tree and select **Create PAR file ...** from the context menu.

#### On server level of management centres:

- Right-click **Multi-Range** in the configuration tree and select **Create PAR file ...** from the context menu. This action creates a master PAR file of the complete MC configuration tree.

- Right-click **Box** (accessible through **Multi-Range** > **<rangenam>** > **<clusternam>** > **Boxes**) and select **Create PAR file for box ...** from the context menu. This action creates a PAR file of the specific box' configuration only.

PAR files may either be saved as regular **.par** or as compressed **.pgz** files.

**Note:**

Consider the following settings when creating PAR files of comprehensive configurations:  
The time provided for PAR file generation is determined by **Socket Connect** and **Read** values configurable in the phion.a **Settings** > **Client** tab > section **Timeout (Getting Started** - 4.2 Client, page 22). If these timeouts are exceeded the PAR file cannot be created. Should you experience problems creating a PAR file, change both values to approx. **200 sec.** (or higher) temporarily. **Remember to revoke settings** when having finished your tasks as these timeouts are a factor in other configuration areas as well.

**Note:**

It is recommendable to create PAR files on a regular basis.

**Note:**

PAR files may also be created at the command line interface (command `phionar`; see Command Line Interface documentation for further information). Thus, with a cronjob, you may automate PAR file creation and archiving.

## 5.4 Restoring/Importing from PAR File

PAR files allow you to restore/import specific box or complete management centre configurations.

PAR files are applicable for the following tasks:

#### Restoring single boxes and box configurations of management centres

Execute this task when restoring the backup of a box configuration.

- Right-click **Box** in the configuration tree and select **Restore from PAR file ...** from the context menu.
- Browse for the **.par** or **.pgz** file that should be restored.
- The applicable configuration changes will not be activated immediately. Click the **Undo** button, if you want to withdraw from restoring. Otherwise, click the **Activate** button to restore the box configuration.

**Note:**


Box configurations may not be restored on MC level. To restore a functional backup of a misconfigured box, delete the box in the management centre tree and thereafter use **Import Box from PAR** instead (see below).

### Restoring management centre configurations

Execute this task when restoring the backup of a complete management centre tree.





**Note:**

If you are restoring the configuration of an MC that has been installed freshly after crash recovery, do not forget to restore the box configuration of the MC as well.

- Right-click  **Multi-Range** in the configuration tree and select **Restore from PAR file ...** from the context menu.
- Browse for the **.par** or **.pgz** file that should be restored.
- The applicable configuration changes will not be activated immediately. Click the **Undo** button, if you want to withdraw from restoring. Otherwise, click the **Activate** button to restore the MC configuration.

### Importing box configurations into the management centre

Execute this task when importing new or former box configurations into the management centre.

- Right-click  **Boxes** (accessible through  **Multi-Range** >  <rangename> >  <clustername>) and select **Import Box from PAR ...** from the context menu.
- Browse for the **.par** or **.pgz** file that should be imported.
- Insert a **Box Name**.
- Click the **Activate** button to activate configuration changes.

### Installing a box with PAR file and kickstart disk

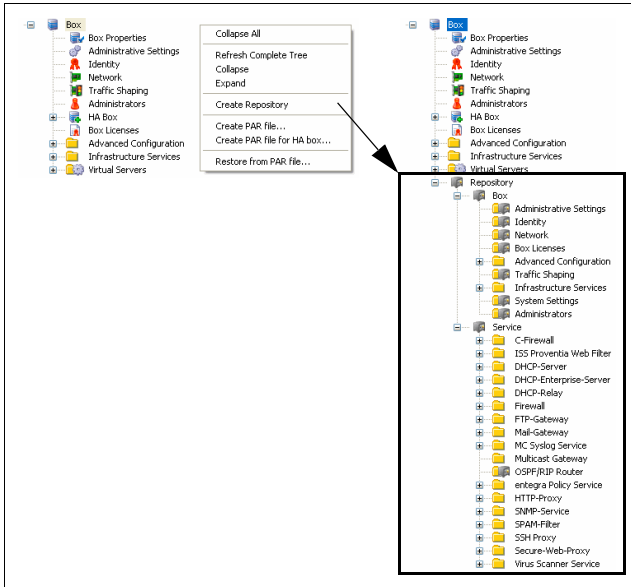
Use PAR files deriving from box configurations to install a preconfigured system.

Refer to **Getting Started** - 1.3 Installation with a Saved Configuration, page 8 for details on installation with PAR file and kickstart disk.

## 6. Repository

The phion box configuration tree may be added a further top level element, the so-called **Repository**. Repositories are available for each configuration instance of the tree, for example **Settings**, **Cron**, ...

Fig. 3-72 Way of supplying a box with a repository



You may use the individual repository subdirectories as storage containers for edited configuration data of the respective type.

**Note:**

Due to compatibility reasons, two nodes are structured in a different way in box repository tree than within box range tree configuration:

- **Authentication Service** is placed in **Advanced Configuration** and not in **Infrastructure Services**
- **System Settings** is placed in **Box** and not in **Advanced Configuration**

### 6.1 Creating a Repository

You have to click on the **Activate** button to actually create the **Repository** tree element. With the creation of a repository the options available for configuration nodes in the context menu will be augmented by entries **Copy to Repository** and **Copy From Repository** (only visible when the corresponding node is locked).

If you select option **Copy From Repository** a dialogue will open allowing you to browse the contents of the respective repository. Simply click on the file instance whose contents you wish to be written to the locked configuration instance. When you are done click the **OK** button.

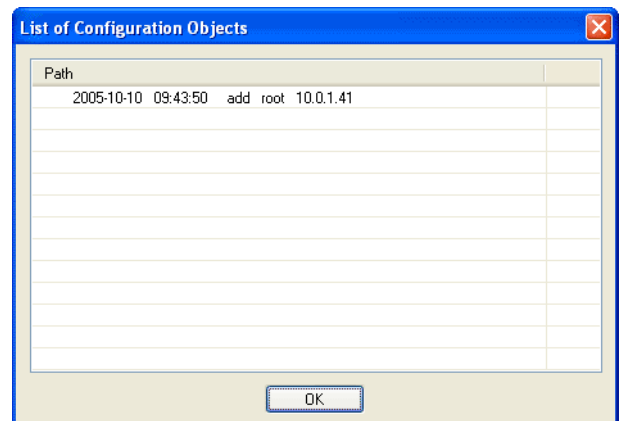
If you select option **Copy To Repository** which is also available for an unlocked tree node a similar dialogue will appear.

**Note:**

In order to successfully copy to a repository you will have to lock the destination file (if you wish to write over an existing file). Otherwise it suffices to click on the directory for an input field to open at the bottom of the dialogue. Here you simply enter the name under which the node is meant to be archived.

In order to obtain more information as to when or by whom a node was created, modified or locked the context menu contains an option **Show History**.

Fig. 3-73 Show History window



This may be of particular interest when your organisation makes use of root aliases.

A "fresh" phion netfence always contains a default box repository containing data set with the most common settings (for example for appliances).





# Firewall

<b>1.</b>	<b>Overview</b>	
1.1	Firewall Configuration .....	125
1.2	Firewall Notions .....	125
1.3	Firewall GUI .....	125
<b>2.</b>	<b>Firewall Configuration</b>	
2.1	Global Parameters and Default Settings .....	126
2.2	Rule Set Configuration .....	132
2.3	Advanced Options for Firewall Rules .....	151
2.4	Delete, Copy and Paste within the Firewall Configuration .....	160
2.5	Cascaded Rule Sets .....	160
<b>3.</b>	<b>Local Rules</b>	
3.1	General .....	162
3.2	Restrictions of Local Action and Connection Types .....	162
<b>4.</b>	<b>Testing and Verifying of Rule Sets</b>	
4.1	General .....	163
4.2	Overlapping Rules .....	163
4.3	Rule Tester .....	163
4.4	Test Report .....	164
<b>5.</b>	<b>Example Configuration</b>	
5.1	General .....	165
5.2	Advanced Settings in the Example Setup .....	168
<b>6.</b>	<b>Real Time Information and Manipulation</b>	
6.1	GUI Elements .....	169
6.2	Real Time Status .....	169
6.3	Access Cache .....	173
6.4	Authenticated User .....	176
6.5	Dynamic Rules and Data .....	176
6.6	Shaping .....	177
6.7	Tracing Connections .....	177
6.8	Audit Log .....	178
<b>7.</b>	<b>Firewall Rule Sets</b>	
7.1	Direct Modification and Activation .....	179
<b>8.</b>	<b>Log Files</b>	
8.1	Standard Log Files .....	179
<b>9.</b>	<b>Bridging</b>	
9.1	General .....	180
9.2	Bridging Goals and Benefits .....	180
9.3	Bridging Methods .....	180
9.4	Security .....	182
9.5	Implementation of Logical Entities .....	182
9.6	Bridging Configuration .....	183

## 10. Firewall Authentication

10.1	Configuring Firewall Authentication .....	188
10.2	phion Firewall Authentication Client .....	192
10.3	Monitoring .....	192

## 11. RPC

11.1	General .....	193
11.2	ONCRPC .....	193
11.3	DCERPC .....	196
11.4	Monitoring .....	198

# 1. Overview

The heart of the available netfence software modules is the firewall module. This chapter treats with the configuration of the firewall module as well as with the tools, which allow the administrator to steer the firewall behaviour while it is running.

The chapter is basically divided into three parts:

- Overview
- Detailed description of the configuration (including a real-world example)
- Insights in the runtime steering of the firewall engine

The phion netfence firewall module handles any IP traffic that is handled by the system. Basically it is divided into four different types of traffic:

- **Loopback**  
Traffic where source AND destination are local addresses and processes
- **Local In** (Local rules - Inbound)  
Traffic with a local destination address and process
- **Local Out** (Local rules - Outbound)  
Traffic with a local source address and process
- **Forward** (Forwarding rules)  
Traffic traversing the system

## 1.1 Firewall Configuration

The behaviour of the system as a whole is basically determined of four configuration layers:

- System Network and Server Configuration
- Host Firewall Rules
- General Firewall Configuration
- Firewall Forwarding Settings

The first part is covered by the global configuration chapter of this manual. This chapter takes the correct network and server configuration for granted. That means that the routing table of the system is configured to work properly and the IPs of the server the firewall service is connected to are correct and active.

All configuration tasks are principally done either on the management centre tree or on the tree of a single-managed box. The firewall rule set, however, can be configured in an alternative way by means of the operative firewall GUI itself. This way underlies the same mechanism the ordinary way does. It is thus not possible to circumvent the transaction mechanism of the configuration procedure.

**Attention:**  
If you do not find any rule set on your system to configure, go back to the configuration chapter and perform the following steps:

**Step 1** Configure network properties of your system

**Step 2** Introduce a server on your system

### Step 3 Introduce a firewall service on your system

**Note:**  
The forwarding firewall is only active either without any license key or with a valid license including the firewall module.

To create a new rule, lock the affected rule set (either **Local Rule Set** or **Forwarding Rule Set**) and click the context menu entry **New**.

**Attention:**  
Rule names may contain a maximum of 50 characters and digits.

## 1.2 Firewall Notions

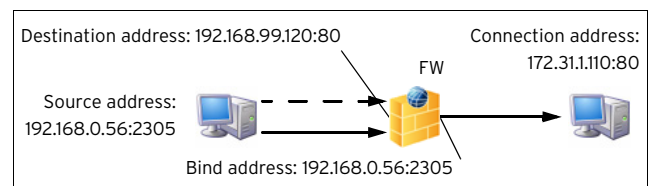
The firewall module is able to handle two types of transport mechanisms:

- stateful ACPF (Application Controlled Packet Forwarding)
- TAP (Transparent Application Proxying)

The latter method is only available for TCP traffic, because it does not make sense to simulate connections for connectionless protocols.

Since all netfence versions before version 2.4 used exclusively TAP as forwarding mechanism, the notions are still the same as it is in socket based notions.

**Fig. 4-1** Basic connection diagram describing the notions used throughout the netfence firewall engine



**Table 4-1** Firewall notions

IP: Port	Description
Source	Origin of IP request
Destination	Target of original IP request
Bind	Origin of IP request initiated by the firewall system
Connection	Target of IP request initiated by the firewall system

## 1.3 Firewall GUI

Like most of the netfence services, the firewall service incorporates a specific graphical administration user interface providing real-time data and tools for real-time manipulation. Additionally, it enables rule set configuration.

## 2. Firewall Configuration

### 2.1 Global Parameters and Default Settings

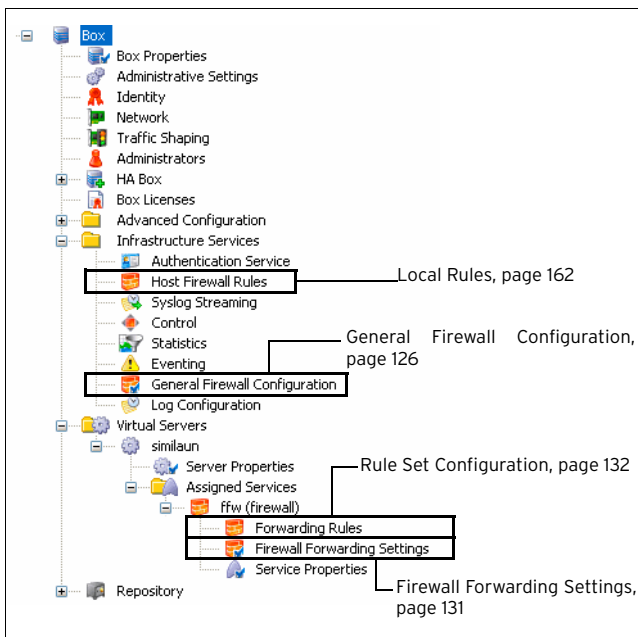
Beside the rule set there are several global parameters, which steer the behaviour of the firewall engine as a whole. Changing some of these parameters makes it necessary to restart the firewall service.

#### Attention:

All active connections will get lost during this procedure.

The settings are divided into two parts: the first part regarding the firewall engine as a whole (see 2.1.1 General Firewall Configuration, page 126), which is actually a box service, and the part which is only valid for the service layer part and affects the forwarding and service infrastructure issues only (see 2.1.2 Firewall Forwarding Settings, page 131).

Fig. 4-2 Tree locations of the general firewall settings



#### 2.1.1 General Firewall Configuration

##### Note:

To activate changes made in this part of the configuration, click button **phion Restart** (for further information concerning effects of **phion Restart** see **Control Centre** - 2.6 Box Tab, page 38).

#### 2.1.1.1 Peer-to-Peer Detection

P2P-detection is assigned per firewall rule and can only be used in the forwarding firewall rule set. See 2.3.2 Peer-to-Peer Detection, page 153 for general information and configuration details.

The following global options are available:

List 4-1 Box Services - General Firewall Configuration - Peer-to-Peer Detection

Parameter	Description
<b>Enable Peer-To-Peer Detection</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables P2P-detection.
<b>Peer-To-Peer Policy</b>	From the list select the handling policy for detected P2P traffic. <ul style="list-style-type: none"> <li>➤ <b>Detect-Only</b> Detects and reports P2P traffic in the firewall access cache but takes no action.</li> <li>➤ <b>Drop-Traffic</b> Blocks detected P2P traffic.</li> <li>➤ <b>Limit-Bandwidth</b> Limits the bandwidth for detected P2P traffic considering the limit value specified below.</li> </ul>
<b>Peer-To-Peer Bandwidth (KBit/s)</b>	This option is enabled by policy setting to <b>Limit-Bandwidth</b> . It specifies the maximum bandwidth that should be allowed for P2P traffic.
<b>Detect All Available Protocols</b>	<b>yes</b> all protocols that are known are detected. <b>no</b> no protocols are detected. Choose protocol at <b>Protocol Selection</b> .
<b>Protocol Selection</b>	Choose your appropriate protocol.

#### 2.1.1.2 Global Limits

##### Note:

After increasing **Session Limits and Memory Settings** restarting the firewall service may fail if there is not sufficient kernel address space available.

The default size of kernel address space that is reserved for the firewall is 256 MB. The address space can be extended by using the `vmalloc` kernel parameter. The syntax of `vmalloc` is:

```
vmalloc=<Size>K|M|G
```

- `<Size>` is the new size of the kernel address space reserved for storing the firewall data.
- K, M or G is the unit of `<Size>` which is **K**ilobyte, **M**egabyte or **G**igabyte.

**Example:** `vmalloc=512M` reserves 512 Megabytes for the firewall.



To increase the kernel address space enter the `vmalloc` parameter in **Config** > **Box** > **Advanced Configuration** > **Bootloader** > **Global Append Options**. Then activate the new settings and reboot the box.

**List 4-2** General Firewall Configuration - Global Limits - section Session Limits and Memory Settings

Parameter	Description
<b>ACPF Memory [MB]</b>	This parameter is read-only and displays the estimated memory requirement according to the settings below. If the following settings are increased and the displayed read-only value exceeds 200 MB an additional bootloader parameter may be required.  On i686 boxes with more than 768MB RAM that require additional <code>vmalloc</code> space to satisfy the increased memory demand of non-default firewall settings we recommend to increase the <code>vmalloc</code> area in steps of 128MB, starting at the 384MB. Reboot the box after setting the parameter and wait if the firewall service successfully starts after the system boot. Do not use <code>vmalloc</code> areas bigger than 640MB. The <code>vmalloc</code> area is shared among several kernel subsystems. Therefore the exact size of the allocated <code>vmalloc</code> area that is required to load the firewall cannot be predetermined.  Setting the "vmalloc" parameter to enable increased <code>acpf</code> memory operation is discouraged on systems with 768MB of RAM or on "i386" architecture systems. Setting this parameter on those boxes could negatively affect the system performance and/or stability. The architecture of a installed netfence box can be determined with the following command: <pre>rpm -q kernel --qf %{ARCH} \\\n</pre>
<b>Max. Session Slots</b>	Maximum number of session slots: 800000 (min: 2000; default: 65536). <b>Note:</b> If this parameter is set to its maximum, set <code>vmalloc=896M</code> <b>Note:</b> A value of 32768 requires around 40 MB RAM.
<b>Max Acceptors</b>	Maximum pending accepts for inbound rules (min: 2000; max: 2000000; default: 8192). An acceptor is a dynamic implicit rule that is generated by plugins handling dynamic connection requests. The FTP protocol for example uses a data connection beside the control connection on TCP port 21 to perform the actual file transfer. By analysing the FTP protocol, the firewall knows when such data connections occur and thus creates an acceptor allowing the corresponding data transfer session.
<b>Max. Pending Inbounds</b>	Maximum number of pending TCP inbound requests (min: 2000; max: 65536; default: 16384). This parameter only comes into effect, when inbound traffic is activated in the corresponding rule.
<b>Max. Plugins</b>	Maximum number of rules using plugins (min: 0; max: 65536; default: 8192).
<b>Dyn. Service Name Entries</b>	Maximum number of dynamic service name entries (min: 0; max: 65536; default: 8192).
<b>Max. Dynamic Rules</b>	Maximum number of dynamically activated rules (min: 1; max: 1024; default: 128).
<b>Max. Multiple Redirect IPs</b>	Maximum number of IPs in rules with multiple redirect target IPs (min: 1; max: 1024; default: 128).

**List 4-3** General Firewall Configuration - Global Limits - section Access Cache Settings

Parameter	Description
<b>Max. Access Entries</b>	min: 128; max: 8192; default: 2048
<b>Max. Block Entries</b>	min: 128; max: 8192; default: 2048
<b>Max. Drop Entries</b>	min: 128; max: 8192; default: 2048
<b>Max. Fail Entries</b>	min: 128; max: 8192; default: 2048
<b>Max. ARP Entries</b>	min: 128; max: 8192; default: 2048
<b>Max. SIP Calls</b>	min: 64; max: 8192; default: 512; see <b>Voice over IP - 4. SIP</b> , page 360 for details
<b>Max. SIP Transactions</b>	min: 64; max: 8192; default: 512; see <b>Voice over IP - 4. SIP</b> , page 360 for details

**List 4-3** General Firewall Configuration - Global Limits - section Access Cache Settings

Parameter	Description
<b>Max. SIP Media</b>	min: 64; max: 16384; default: 1024; see <b>Voice over IP - 4. SIP</b> , page 360 for details
<b>Max. DNS Entries</b>	Maximum number of DNS queries triggered through creation of network objects of type <b>Hostname</b> (see 2.2.4.1 Hostname (DNS Resolvable) Network Objects, page 141) (default: <b>512</b> ). 75 % of the configured value are reserved for use by the forwarding, the remaining 25 % for use by the local firewall rule set. The combination of maximum value and percentage determines the <b>Index</b> number of network objects that are visualised in the Firewall Monitoring GUI (see 6.5.1 Dynamic Rules, page 176). <b>Attention:</b> DNS queries will not be executed for network objects exceeding the maximum values and consequently, firewall rules using these objects will never match. <b>Note:</b> A network object that is used by forwarding and local firewall at the same time will trigger two DNS queries and will be counted twice.

### 2.1.1.3 Session Limits

**List 4-4** General Firewall Configuration - Session Limits

Parameter	Description
<b>Max UDP (%)</b>	Maximum percentage of granted UDP sessions (min: 1; max: 100; default: 30; parameter <b>Max. Session Slots</b> (see 2.1.1.2 Global Limits, page 126) defines the number of available sessions, and this is 100 %). <b>Note:</b> With eventing activated (parameter <b>UDP Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW UDP Connection Limit Exceeded</b> [4009] is generated when the limit is exceeded.
<b>Max Echo (%)</b>	Maximum percentage of granted ICMP sessions (min: 1; max: 100; default: 30; parameter <b>Max. Session Slots</b> (see 2.1.1.2 Global Limits, page 126) defines the number of available sessions, and this is 100 %). <b>Note:</b> With eventing activated (parameter <b>Echo Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW ICMP-ECHO Connection Limit Exceeded</b> [4027] is generated when the limit is exceeded.
<b>Max Other (%)</b>	Maximum percentage of granted sessions of any IP Protocol except TCP, UDP, ICMP (min: 1; max: 100; default: 10; parameter <b>Max. Session Slots</b> (see 2.1.1.2 Global Limits, page 126) defines the number of available sessions, and this is 100 %). <b>Note:</b> With eventing activated (parameter <b>Other Limit Exceeded</b> set to <b>yes</b> , see page 130), the event <b>FW OTHER-IP Session Limit Exceeded</b> [4029] is generated when the limit is exceeded.
<b>Max Local-In Session/Src</b>	Maximum number of sessions per source IP. If this number is larger than <b>Max. Session Slots</b> (see 2.1.1.2 Global Limits, page 126), it is restricted by that (min: 1; max: -; default: 8192). <b>Note:</b> With eventing activated (parameter <b>Session/Src Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW Global Connection per Source Limit Exceeded</b> [4024] is generated when the limit is exceeded.
<b>Max Local-In UDP/Src</b>	Maximum number of UDP sessions per source IP (min: 1; max: -; default: 512). <b>Note:</b> With eventing activated (parameter <b>UDP/Src Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW UDP Connection per Source Limit Exceeded</b> [4008] is generated when the limit is exceeded.
<b>Max Local-In Echo/Src</b>	Maximum number of ICMP Echo sessions per source IP (min: 1; max: -; default: 512). <b>Note:</b> With eventing activated (parameter <b>Echo/Src Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW ICMP-ECHO Connection per Source Limit Exceeded</b> [4026] is generated when the limit is exceeded.

List 4-4 General Firewall Configuration - Session Limits

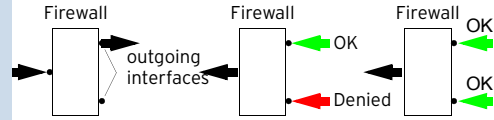
Parameter	Description
<b>Max Local-In Other/Src</b>	Maximum number of sessions of any IP protocol (except TCP, UDP, ICMP) per source IP (min: 1; max: -; default: 128). <b>Note:</b> With eventing activated (parameter <b>Other/Src Limit Exceeded</b> set to <b>yes</b> , see page 130), the event <b>FW OTHER-IP Connection per Source Limit Exceeded</b> [4028] is generated when the limit is exceeded.
<b>Inbound Threshold (%)</b>	If the number of pending accepts exceeds the threshold, the firewall switches to <i>inbound</i> mode (min: 1; max: 100; default: 20). <b>Note:</b> With eventing activated (parameter <b>Pending Accepts Critical</b> set to <b>yes</b> , see page 130), the event <b>FW Activating Perimeter Defence (inbound mode)</b> [4004] is generated when the limit is exceeded.
<b>SYN Cookie High Watermark (%)</b>	Percentage (of maximum pending inbounds) of pending inbound accepts to switch to SYN cookie usage for enhanced SYN flooding protection (min: 0; max: 100; default: 20).
<b>SYN Cookie Low Watermark (%)</b>	Percentage (of maximum pending inbounds) of pending inbound accepts to go back to ordinary SYN handling (min: 0; max: 100; default: 15).
<b>Max Pending Local Accepts/Src</b>	Maximum number of pending accepts per source IP (min: 5; max: 1024; default: 64).
<b>Max TAP Worker</b>	(min: 5; max: 1024; default: 100).
<b>Max Socks Worker</b>	(min: 5; max: 1024; default: 20).

### 2.1.1.4 Operational

List 4-5 General Firewall Configuration - Operational

Parameter	Description
<b>Use Kernel Rule Set</b> [default: no]	<b>no:</b> Kernel Rule Set not enabled <b>yes:</b> Kernel Rule Set enabled <b>accelerated:</b> Kernel Rule Set in accelerated-mode enabled  Setting to <b>yes</b> or <b>accelerated</b> transfers the forwarding firewall rule set into kernel space. Opting for rule matching directly within the operating system kernel improves the performance of the firewall's connection establishment rate. For achievable rates refer to the documentation <b>phion Data Sheets</b> . As a rule of thumb for about 1000 session/s the kernel rule set should be enabled for better firewall performance. Additionally if many firewall objects (> 200) are used the <b>accelerated</b> option is recommended. <b>Note:</b> Activating this parameter deactivates the option to use Tracing conditions (see 6.7.2 Tracing of Connections Matching Defined Conditions, page 177).
<b>Global TCP Delay Policy</b>	Decides if Nagle algorithm is used by default. Can be overruled for single connection objects (default: <b>NagleEnabled</b> ).
<b>Accept Policy</b>	Possible values are <b>inbound</b> or <b>outbound</b> . The value configured here is used as Server default value in the Accept Policy section of the rule creation/editing dialogue ( <b>Firewall</b> - 2.3.3.3 Accept Policies, page 157).
<b>ARP Reverse Route Check</b>	Setting this parameter to <b>yes</b> causes that answers to ARP requests are checked whether Source IP and interface are correct.

List 4-5 General Firewall Configuration - Operational

Parameter	Description
<b>Global Reverse Device Policy</b>	The options of this parameter specify whether requests and replies have to use the same (outgoing) interface to be accepted ( <b>device-fixed</b> , default) or not ( <b>device-may-change</b> ).  The figure shows: Request (left) - Reply for setting device-fixed (middle) - Reply for setting device-may change (right). <b>Attention:</b> This parameter specifies the global policy. You may change the policy per rule, though it is NOT recommended to do so.
<b>Allow Active-Active Mode</b>	Active-Active firewall operation mode is deactivated by default (setting: <b>no</b> ). It has to be enabled in preparation for operation of multiple active firewalls on one box with a load balancer connected upstream.
<b>Log Synced Sessions</b>	This setting determines logging of access cache sessions, which have been synchronised between HA partners (default: <b>yes</b> ). Set to <b>no</b> to disable logging.
<b>Enable FW Compression</b>	The setting of this parameter determines utilisation ability of firewall compression in connection objects (list 4-34, page 146). Firewall compression is deactivated by default (default: <b>No</b> ). <b>Note:</b> Firewall compression is only applicable between firewalls operating on netfence gateway. When activated, option <b>Enable FW Compression</b> <b>MUST</b> be set to <b>yes</b> on all systems participating in compressed traffic. <b>Attention:</b> Do not enable firewall compression on gateways situated at the rim of untrustworthy networks in order to avoid DoS attacks based on bulk sending of compressed data packets. An attacker might forward IPCOMP packet copies originating from the compressed session to the firewall, thus forcing it to load consuming decompression tasks. If compressed traffic is required at the perimeter, make use of compressed VPN traffic. Authentication mechanisms included in VPN technology prevent the DoS exploit stated above ( <b>VPN</b> - 2.7.1.2 Traffic Intelligence (TI), page 223).
<b>Disable Assembler Ciphers</b>	By default these Assembler Ciphers are enabled. Due to the assembler implementation for AES/SHA/MD5 the VPN performance has been increased significantly.
<b>VPN Rate Limit (Mbits/sec)</b>	This parameter may be used to limit the measure at which VPN traffic is encrypted and decrypted respectively. The default value <b>0</b> does not impose any restriction. <b>Note:</b> Change this value should you experience excessive CPU load in an environment with many VPN tunnels.
<b>VPN HW Modules</b>	If you have installed and intend to use a crypto hardware accelerator board for encryption load splitting with VPN, select the hardware module, which is required to load the corresponding functions. Momentarily netfence gateways support the <b>Broadcom_582x</b> module. <b>Note:</b> When operating a hardware accelerator card the encryption engine may be chosen per tunnel (TINA tunnels, see <b>HW Acceleration</b> , page 221 / IPSec tunnels, see <b>HW Accel.</b> , page 227)
<b>Rule Change Behaviour</b>	Specifies whether an existing connection is terminated ( <b>Terminate-on-change</b> , default) or not ( <b>Keep-on-change</b> ) if the rule set changes and the session is no longer allowed by the new rule set.

List 4-5 General Firewall Configuration - Operational

Parameter	Description
<b>Generic Forwarded Networks</b>	Traffic between networks inserted into this field will be excluded from firewall monitoring and will be forwarded without source and destination differentiation, even if no forwarding firewall is installed.  <b>Attention:</b> Local sessions are not reevaluated on rule change. This parameter has only effect on forwarding sessions. Workflow for enforcing changed local rules: manually terminate local sessions in the Firewall Active tab.  <b>Attention:</b> Only make use of this feature, if you are operating your netfence system for routing and NOT for firewall purposes, as generic network forwarding might cause severe security issues.
<b>No Rule Update Time Range</b>	This option allows defining a time range during which firewall rules may not be updated. Use international time format, for example to disallow rule update from 14:00 through 22:00, insert 14-22.
<b>Send TCP RST for OOS Pkts.</b>	Firewall sends TCP RST packets to these networks if it detects packets not belonging to an active session. This is useful to avoid timeouts on certain servers.

### 2.1.1.5 Audit and Reporting

#### Section *Limits and Operational Settings*

List 4-6 General Firewall Configuration - Audit and Reporting tab - section Limits and Operational Settings

Parameter	Description
<b>Resolve Access Cache IPs</b>	Setting this parameter to <b>yes</b> (default: <b>no</b> ) causes that IP addresses can be resolved to hostnames in the firewall access cache (see 6.3.1 Available Filter Options, page 173).
<b>Port Scan Threshold</b>	If the number of blocked requests exceeds this limit (within <b>Port Scan Detection Interval</b> ), a port scan is detected (min: 2; max: 1000000000; default: 10). The eventing setting <b>Port Scan</b> (see page 130) defines whether to generate an event or not, when a port scan is detected.
<b>Port Scan Detection Interval</b>	Detection interval in seconds to check for not allowed activity (min: 0; max: 1000000000; default: 60). In combination with the parameter <b>Port Scan Threshold</b> it defines the condition when to report a port scan.
<b>Forward Log Policy</b>	This parameter defines whether server specific FFW logs should be written to both box and server log ( <b>Box-And-Server File</b> , default), only to the server logs ( <b>Server-File-Only</b> ) or only to the box logs ( <b>Box-File-Only</b> ).
<b>Log Level</b>	Cumulative logging allows some reduction of log file lengths and tries to avoid indirect denial of service (DoS) attacks.
<b>Cumulative Interval [s]</b>	Interval (in sec) for which cumulative logging is activated for either matching or similar log entries. To enter cumulative logging the entries have to be identical in all of the identifiers of a log entry except of the source port (min: 1; max: 60; default: 1).
<b>Cumulative Maximum</b>	Maximum number of log entries within the same rule and resulting in the same reason which triggers cumulative logging (default: 10).
<b>Statistics for Local Firewall</b>	This option enables the creation of statistics for the local firewall.
<b>Use Service Names for Statistics</b>	Via this parameter you define whether statistics contain the port ( <b>no</b> , default) or the set service name ( <b>yes</b> , see 2.2.5.1 Parameters of Services, parameter Service Label, page 144);

List 4-7 General Firewall Configuration - Audit and Reporting tab - section Eventing Settings

Parameter	Description
<b>Generate Events</b>	Enables configuration of Eventing Settings below.
<b>Settings</b>	see list 4-10, page 129

List 4-8 General Firewall Configuration - Audit and Reporting tab - section Audit Information Generation

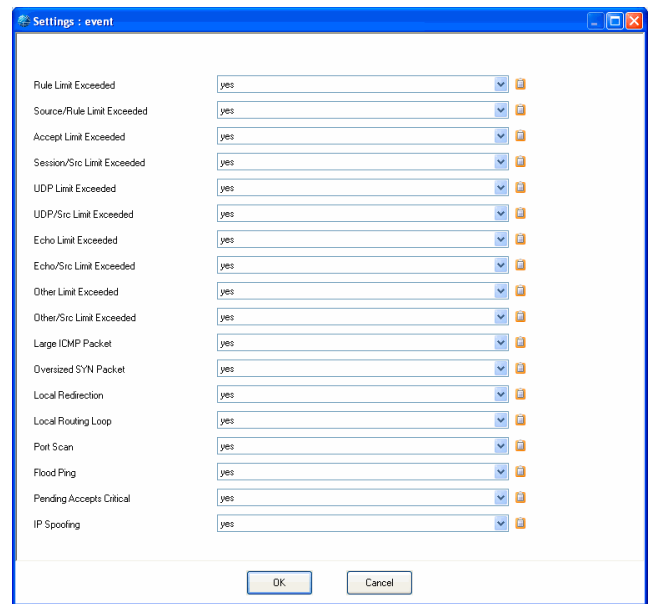
Parameter	Description
<b>Generate Audit Info</b>	Enables configuration of Firewall Audit below.
<b>Settings</b>	see list 4-11, page 130

List 4-9 General Firewall Configuration - Audit and Reporting tab - section Connection Tracing

Parameter	Description
<b>Settings</b>	see list 4-13, page 131

#### Section *Eventing Settings*

Fig. 4-3 Config Section - Eventing Settings



This section consists of the pull-down menu **Generate Events** (default: **yes**) and **Settings**.

To open the configuration dialogue, click the **Set** button.

List 4-10 General Firewall Configuration - Eventing Settings

Parameter	Description
<b>Rule Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW Rule Connection Limit Exceeded</b> [4016] when the limit for <b>Max. Number of Sessions</b> (Advanced Rule Parameters, see page 155) is exceeded.
<b>Source/Rule Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW Rule Connection per Source Limit Exceeded</b> [4018] when the limit for <b>Max. Number of Sessions per Source</b> (Advanced Rule Parameters, see page 155) is exceeded.
<b>Accept Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW Pending TCP Connection Limit Reached</b> [4006] when the limit for <b>Max Pending Accepts/Scr</b> (Firewall Forwarding Settings > Firewall tab, see page 131) is exceeded.
<b>Session/Src Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW Global Connection per Source Limit Exceeded</b> [4024] when the limit for either <b>Max Local-In Session/Src</b> (see page 127) or <b>Max. Forwarding Session/Src</b> (see page 131) is exceeded.
<b>UDP Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW UDP Connection Limit Exceeded</b> [4009] when the limit for <b>Max UDP (%)</b> (see page 127) is exceeded.
<b>UDP/Src Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW UDP Connection per Source Limit Exceeded</b> [4008] when the limit for either <b>Max Local-In UDP/Src</b> (see page 127) or <b>Max. Forwarding UDP/Src</b> (see page 131) is exceeded.
<b>Echo Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW ICMP-ECHO Connection Limit Exceeded</b> [4028] when the limit for <b>Max Echo (%)</b> (see page 127) is exceeded.
<b>Echo/Src Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW ICMP-ECHO Connection per Source Limit Exceeded</b> [4026] when the limit for either <b>Max Local-In Echo/Src</b> (see page 127) or <b>Max. Forwarding Echo/Src</b> (see page 131) is exceeded.

List 4-10 General Firewall Configuration - Eventing Settings

Parameter	Description
<b>Other Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW OTHER-IP Session Limit Exceeded</b> [4029] when the limit for <b>Max Other (%)</b> (see page 127) is exceeded.
<b>Other/Src Limit Exceeded</b>	Setting <b>yes</b> creates the event <b>FW OTHER-IP Connection per Source Limit Exceeded</b> [4028] when the limit for either <b>Max Local-In Other/Src</b> (see page 128) or <b>Max. Forwarding Other/Src</b> (see page 131) is exceeded.
<b>Large ICMP Packet</b>	Setting <b>yes</b> creates the event <b>FW Large ICMP Packet Dumped</b> [4012] when the limit for <b>Max Ping Size</b> ( <b>Firewall</b> > <b>Service Objects</b> > <b>ICMP Echo</b> ) is exceeded and the packet is dropped.
<b>Oversized SYN Packet</b>	Setting <b>yes</b> creates the event <b>FW Oversized SYN Packet Dumped</b> [4010] when an oversized SYN packet is dropped by the firewall.
<b>Local Redirection / Local Routing Loop</b>	Setting <b>yes</b> triggers the events <b>FW Forwarding Loop Suppressed</b> [2500] and <b>FW Local Redirection Suppressed</b> [2502] when the FW server IP is addressed directly and no proper rule set is defined.
<b>Port Scan</b>	Setting <b>yes</b> creates the event <b>FW Port Scan Detected</b> [4000] when the limit for <b>Port Scan Threshold</b> (see page 129) is exceeded.
<b>Flood Ping</b>	Setting <b>yes</b> creates the event <b>FW Flood Ping Protection Activated</b> [4002] when the minimum ping delay ( <b>Firewall</b> > <b>Service Objects</b> > <b>Min Delay</b> , page 144) is under-run.
<b>Pending Accepts Critical</b>	Setting <b>yes</b> creates the event <b>FW Activating Perimeter Defence (inbound mode)</b> [4004] when the limit for <b>Inbound Threshold (%)</b> , see page 128) is exceeded.
<b>IP Spoofing</b>	Setting <b>yes</b> generates the events <b>FW IP Spoofing Attempt Detected</b> [4014] or <b>FW Potential IP Spoofing Attempt</b> [4015] when the firewall identifies an IP spoofing attempt (interface mismatch) or SYN flooding attack (see 2.3.3.3 Accept Policies, page 157). <b>Note:</b> The detection option only applies to rules, which have been configured with <b>Source</b> (and/or <b>Reverse</b> ) <b>Device</b> setting <b>matching</b> (see 2.2.8 Interface Groups, page 150).

### Section **Audit Information Generation**

The firewall audit facility allows propagating firewall events to other facilities, which may process the information for further usage (for example storing it into an SQL database).

Activate firewall audit by enabling parameter **Generate Audit Info**.

The following methods are available for event propagation:

List 4-11 Audit Information Generation - Settings - section Audit Info Transport

Parameter	Description
<b>Audit Delivery</b>	<ul style="list-style-type: none"> <li>➤ <b>Local-File</b></li> <li>➤ <b>Local-File-And-Forward</b></li> <li>➤ <b>Forward-Only</b></li> <li>➤ <b>Legacy-Log-File</b> Log into self-contained file.</li> <li>➤ <b>Legacy-Syslog-Proxy</b> Forward via syslog streaming.</li> <li>➤ <b>Legacy-Executable</b> Pipe log stream into an executable (stdin). All processing or propagation is performed by the executable</li> <li>➤ <b>Legacy-Send-UDP-Packet</b> Send log stream entries as UDP packets to an IP address/port.</li> </ul>
<b>Executable</b>	Only available with <b>Audit Delivery</b> type <b>Legacy-Executable</b> . Specify the executable in this place.
<b>Send to IP Address</b>	Only available with <b>Audit Delivery</b> type set to <b>Local-File-And-Forward</b> , <b>Forward-Only</b> , or <b>Legacy-Send-UDP-Packet</b> . Specify IP address and port the log stream should be addressed to in this place. If no IP and port is set, data will be send to the management centre.
<b>Send to Port</b>	

List 4-11 Audit Information Generation - Settings - section Audit Info Transport

Parameter	Description
<b>ACPF Allowed Msg Buffer</b>	Number of ACPF buffered bytes to allow messages.
<b>ACPF Blocked Msg Buffer</b>	Number of ACPF buffered bytes to block messages.
<b>ACPF Dropped Msg Buffer</b>	Number of ACPF buffered bytes to drop messages.

List 4-12 Audit Information Generation - Settings - section Recorded Conditions

Parameter	Description
	This section expects specification of conditions, which should be reported. The following event types can be reported:
	➤ <b>Allowed Sessions</b>
	➤ <b>Blocked Sessions</b>
	➤ <b>Session Termination</b>
	➤ <b>Failed Sessions Termination</b>
	➤ <b>Dropped Packets</b>
	➤ <b>Invalid ARPs</b>
	➤ <b>Allowed Local Sessions</b>
	➤ <b>Blocked Local Sessions</b>
	➤ <b>Log Local Session Termination</b>
	➤ <b>Failed Local Sessions</b>

An audit event entry consists of a CR terminated line of ASCII characters. Each line holds 23 pipe ("|") separated values. Sample:

```
1129102500|Block:|FWD|eth0|ICMP|BLOCKALL|10.0.3.80|0|10.0.3.73|0||4002|Block by Rule|0.0.0.0|0|0.0.0.0|0||00:07:e9:09:04:30|0|0|0|0|0
```

Table 4-2 Audit events

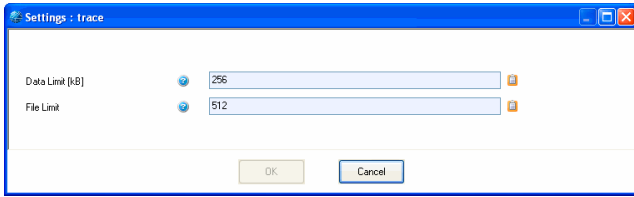
Column	Value	Type
1	Time	Unix seconds
2	Log Operation	Table: Log Operations
3	Session Type	Table: Session Type
4	Input Network Device	String
5	IP Protocol	String
6	Firewall Rule	String
7	Source IP Address	IP Address
8	Source Port Number	0-65535
9	Destination IP Address	IP Address
10	Destination Port Number	0-65535
11	Service Name	String
12	Reason Code	Number
13	Reason	String
14	Bind IP Address	IP Address
15	Bind Port Number	0-65535
16	Connection IP Address	IP Address
17	Connection Port Number	0-65535
18	Output Network Device	String
19	MAC Address	6 colon separated hex bytes
20	# of Input Packets	Number
21	# of Output Packets	Number
22	# of Input Bytes	Number
23	# of Output Bytes	Number
24	Duration	1/100 seconds



### Section **Connection Tracing**

To open the configuration dialogue, click the **Edit** button.

**Fig. 4-4** Connection Tracing configuration



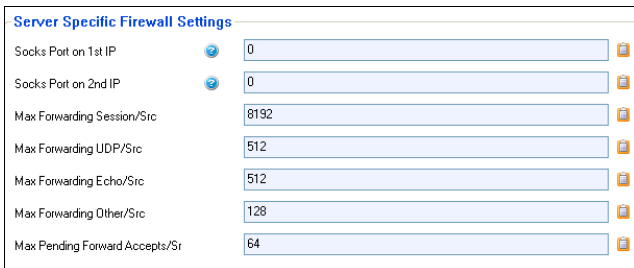
**List 4-13** General Firewall Configuration - Connection Tracing

Parameter	Description
<b>Data Limit (kB)</b>	Max. size of trace per connection (min: 10; max: 4096; default: 256).
<b>File Limit</b>	Max. number of files=traces (min: 10; max: 1024; default: 512).

## 2.1.2 Firewall Forwarding Settings

### 2.1.2.1 Firewall

**Fig. 4-5** Config Section - Firewall Forwarding Settings - Firewall



**List 4-14** Firewall Forwarding Settings - Firewall - section Server Specific Firewall Settings

Parameter	Description
<b>Socks Port on 1st IP</b>	Port of socks connections on first server IP.
<b>Socks Port on 2nd IP</b>	Port of socks connections on second server IP.
<b>Max. Forwarding Session/Src</b>	Maximum number of sessions per source IP (min: 1; max: -; default: 8192). <b>Note:</b> With eventing activated (parameter <b>Session/Src Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW Global Connection per Source Limit Exceeded</b> [4024] is generated when the limit is exceeded.
<b>Max. Forwarding UDP/Src</b>	Maximum number of UDP sessions per source IP (min: 1; max: -; default: 512). <b>Note:</b> With eventing activated (parameter <b>UDP/Src Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW UDP Connection per Source Limit Exceeded</b> [4008] is generated when the limit is exceeded.
<b>Max. Forwarding Echo/Src</b>	Maximum number of ICMP Echo sessions per source IP (min: 1; max: -; default: 512). <b>Note:</b> With eventing activated (parameter <b>Echo/Src Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW ICMP-ECHO Connection per Source Limit Exceeded</b> [4026] is generated when the limit is exceeded.

**List 4-14** Firewall Forwarding Settings - Firewall - section Server Specific Firewall Settings

Parameter	Description
<b>Max. Forwarding Other/Src</b>	Maximum number of sessions of any IP protocol (except TCP, UDP, ICMP) per source IP (min: 1; max: -; default: 128). <b>Note:</b> With eventing activated (parameter <b>Other/Src Limit Exceeded</b> set to <b>yes</b> , see page 130), the event <b>FW OTHER-IP Connection per Source Limit Exceeded</b> [4028] is generated when the limit is exceeded. Maximum number of sessions of any IP protocol (except TCP, UDP, ICMP) per source IP (min: 1; max: -; default: 128). <b>Note:</b> With eventing activated (parameter <b>Other/Src Limit Exceeded</b> set to <b>yes</b> , see page 130), the event <b>FW OTHER-IP Connection per Source Limit Exceeded</b> [4028] is generated when the limit is exceeded.
<b>Max. Pending Forward Accepts/Src</b>	Maximum number of pending accepts per source IP (min: 5; max: 1024; default: 64). <b>Note:</b> With eventing activated (parameter <b>Accept Limit Exceeded</b> set to <b>yes</b> , see page 129), the event <b>FW Pending TCP Connection Limit Reached</b> [4006] is generated, when this limit is exceeded.

### 2.1.2.2 RPC

This section is used in conjunction with RPC. For a detailed description, please have a look at 11.2.2 Configuring Active ONCRPC, page 194, as well as at 11.2.2.1 Configuring Active&Passive ONCRPC (recommended), page 195.

### 2.1.2.3 Bridging

This section is used to configure Bridging Groups and Interfaces. For a detailed description, please have a look at 9. Bridging, page 180.

### 2.1.2.4 Authentication

This section is used in conjunction with Firewall Authentication. For a detailed description, please have a look at 10.1.1.1 Authentication, page 188.

### 2.1.2.5 Phibs

This section is used in conjunction with Firewall Authentication. For a detailed description, please have a look at 10.1.1.2 Phibs, page 189.

### 2.1.2.6 WWW

This section is used in conjunction with Firewall Authentication. For a detailed description, please have a look at 10.1.1.3 WWW tab, page 189.

### 2.1.2.7 H.323 / SIP

These sections are used in conjunction with Voice over IP. Please consult **Voice over IP**, page 355, for additional information.

## 2.2 Rule Set Configuration

There is a slight difference between managing a firewall rule set locally or on a management centre. On a locally administered system, the rule sets are edited either via the firewall GUI or the boxconfig GUI. Nevertheless it is the same rule set, whereas on the management centre the rules are part of the data tree which holds all configuration data of the boxes, servers and services. Therefore, rule administration via a management centre is strictly separated from the control and status overview of the firewall.

Nevertheless, the firewall configuration GUI of the configuration daemons is the same as the configuration part of the firewall GUI itself. Hence it is not described separately.

Firewall configuration uses a set of notions which is necessary to know. Firewalls in general are confronted with a request of the following kind:

**Source-IP:Source-Port** wants to connect to **Destination-IP:Destination-Port**

The rule set of the firewall now decides what should happen with such a request. Generally, there are three ways to handle a request:

- it can be blocked
- it can be allowed
- it can be rewritten

### Note:

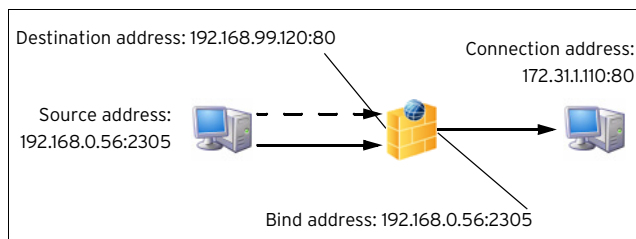
Depending on what kind of rule set is currently created/modified, the following has to be taken into consideration:

**Local FW:** When introducing a new rule that blocks an established connection, the connection has to be terminated manually in order to set the new rule and its connection block active.

**Forwarding FW:** When introducing a new rule that blocks an established connection, it can be configured whether the active connection should be blocked.

Before describing the details of creating rules, we must look at the basics of establishing connections with a phion firewall.

**Fig. 4-6** Schematic of terms involved in establishing a network connection through a phion firewall



Establishing a connection handled by a phion firewall generally involves four IP addresses with ports (if the IP protocol uses them). They are called source, destination, bind, and connection. Without a firewall there would be only source and destination. The firewall rule set deduces the link connection between Bind-IP and Connection-IP and authorises the firewall engine to establish it, then

transferring the packet or the data stream from the Source-Destination connection to the Bind-Connection link. We speak of different types of rules, for example pass, redirecting, mapping, source-nat, destination-nat, ..., depending on how bind and connection address are related to source and destination address.

The real core of the firewall configuration is the rule set. It consists of an ordered set of rules, which interconnects a source-IP:source-port / destination-IP:destination-port quadruple to a bind-IP:bind-port / connection-IP:connection-port. The firewall engine uses the so-called **first-match algorithm** to decide which rule shall be applied. This means the action taken by the firewall engine is uniquely defined by source IP, destination IP, destination port.

The netfence firewall rule set knows two basic entities to describe and fix the behaviour of the firewall engine:

- Action types (see 2.2.3.3 Action Section)  
The action type first decides whether the firewall should do anything at all, then describes the relationship between destination and connection.
- Connection Elements (see 2.2.6 Connection Elements)  
The connection type describes the relation between source and bind address.

### 2.2.1 General Characteristics of the Firewall Graphical Interface

It is desirable that data sets can be arranged in such a way that the most wanted information catches the eye. Giving consideration to these needs, the phion Firewall GUI incorporates several sortation mechanisms.

To simplify matters, the main characteristics regarding arrangement and ordering of data in the various windows will be described together in this chapter. Characteristics exceeding this description are positioned in the respective chapter itself.

#### 2.2.1.1 Title Bar(s)

- **Changing the column sequence**  
Information situated in the main window of each configuration window is captioned with a title bar. The data sets themselves are arranged in columns. The column sequence may be adjusted to personal needs, either by using the standard context menu (see 4.2 Standard Context Menu, page 395) or by dragging and dropping the respective column to another place.
- **Ordering data sets**  
In most windows, data sets may be arranged ascending or descending respectively by clicking into the column labelling of the respective title bar.

#### 2.2.1.2 Context Menu Entries

- Right-clicking into any configuration area without selected item makes the standard context menu available through the menu item **Tools** (see 4.2 Standard Context Menu, page 395).
- Right-clicking on a selected item in any configuration window makes the same menu items available as shown



in the navigation bar of the respective section displayed on the left side. In each case, the items are valid for the specific section only.

- In some windows the context menu item **Set Color ...** allows flagging data sets with a user-specific colour for the purpose of highlighting them.
- In some windows the context menu item **Show in Groups** allows switching between two views, the classical view, a continuous list, or a list combining groups of elements.

### 2.2.1.3 The Object Viewer

The Object Viewer is designed to assist in creating or modifying a rule set, by making distinct objects, such as network, service, connection, ICMP, and time objects quickly available.

Open a rule by double-clicking it and select the checkbox **Object Viewer** in the rule's navigation bar or select **Rules > Object Viewer** from the **Configuration** navigation bar to open the Object Viewer.

When opened from the rule window the Object Viewer is opened sticking to the right of it. Grab the viewer and drag it to a place, where it does not disturb other configuration windows. Adjust the viewer to stay on top permanently by sticking the blue needle.

When opened directly from the rule creation/modification dialogue by ticking the checkbox **Object Viewer** in the navigation bar, a special function is available: Selecting a specific tab in the viewer then immediately changes the navigation bar items in the rule window. Selecting an object hence activates the specific menu items related to it. It is thus not only possible to configure existing objects in the rule set; new objects can additionally be created by launching the object editing dialogues from the navigation bar. Furthermore, existing objects can be dragged from the object viewer into the rule set directly, and be dropped at a place where they fit (also see 2.2.3.1 Creating a New Rule).

### 2.2.1.4 Rule Markers

In the rule overview window rules are sometimes flagged with diverse icons in various columns. The icons are intended to give a quick overview of a rule's main characteristics and are and indicate policy limitations. The following icons are in use:

**Table 4-3** Rule marks utilised in the rule overview window

Icon	Action	Indication to ...
	<b>Attention!</b>	This icon (displayed in the rule view of the rule window) and the conjoint labelling <b>!!! ATTENTION !!! Changed values!</b> indicate that for the respective rule Content Filter and/or Advanced settings values have been changed (see 2.3.1 Content Filter (Intrusion Prevention) and 2.3.3 Advanced Rule Parameters).

**Table 4-3** Rule marks utilised in the rule overview window

Icon	Action	Indication to ...
	<b>Block</b>	This icon is added to rule elements in the column display, which have been configured to <b>BLOCK on Mismatch</b> in the <b>Rule Mismatch Policy</b> section of the Advanced settings dialogue (see 2.3.3 Advanced Rule Parameters).
	<b>Deny</b>	This icon is added to rule elements in the column display, which have been configured to <b>DENY on Mismatch</b> in the <b>Rule Mismatch Policy</b> section of the Advanced settings dialogue (see 2.3.3 Advanced Rule Parameters).
	<b>User authentication required</b>	This icon is added to the <b>Name</b> column if the rule requires user authentication due to configuration of the <b>Authentication</b> parameter in the Advanced configuration dialogue (see 2.2.3.8 Authenticated User Section).
	<b>Timed</b>	This icon is added to the <b>Name</b> column if the rule has been configured as dynamic rule (see 2.3.5 Dynamic Activation).
	<b>Time restricted</b>	This icon is added to the Name column if a time restriction has been configured for the respective rule using a <b>Time Object</b> (see 2.2.3.10 Time Objects) or the <b>Time Restriction</b> parameter (see Time Restriction, page 155) in the Advanced settings dialogue.
	<b>2-way</b>	This icon is added to the <b>Name</b> column if a rule has been configured to apply in both directions.
	<b>Content filter set</b>	This icon is added to the <b>Name</b> column if a content filter has been configured in the rule through parameter <b>Content Filter</b> in the Content/IPS configuration dialogue (see 2.3.1 Content Filter (Intrusion Prevention)).
	<b>Source IP exposed</b>	This icon is added to the <b>Action</b> column if connection type <b>Client</b> is set, which causes the client's source IP to be exposed in a connection (see 2.2.6 Connection Elements).
	<b>Stream is forwarded</b>	This icon is added to the <b>Action</b> column if <b>Stream Forwarding</b> is configured as data transfer <b>Method</b> in the TCP Policy section of the Advanced configuration dialogue (see 2.3.3 Advanced Rule Parameters).
	<b>Source Interface is set to Continue on Mismatch</b>	This icon is used when the Source Interface has been set to Continue on Mismatch (see 2.2.3.9 Source Interface Section / Reverse Interface Section).
	<b>Data flow is compressed</b>	This icon is added to the Action column when the Connection Object the rule references to has been configured with traffic compression in either direction (see 2.2.6 Connection Elements).

### 2.2.2 Navigation Bar Items

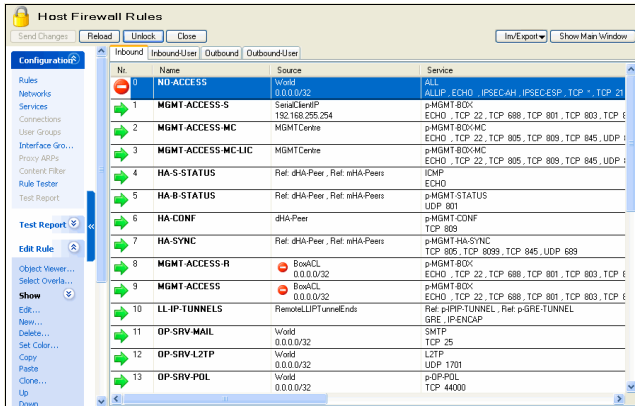
The netfence firewall rule set consists of various configuration entities (Networks, Services, Connections, Proxy ARPs and Content Filters), which can be created and maintained independently from the rule set itself. They are then pieced together building a logical formation.

The firewall configuration window is divided into two organisational areas:

- a **navigation bar** on the left side and

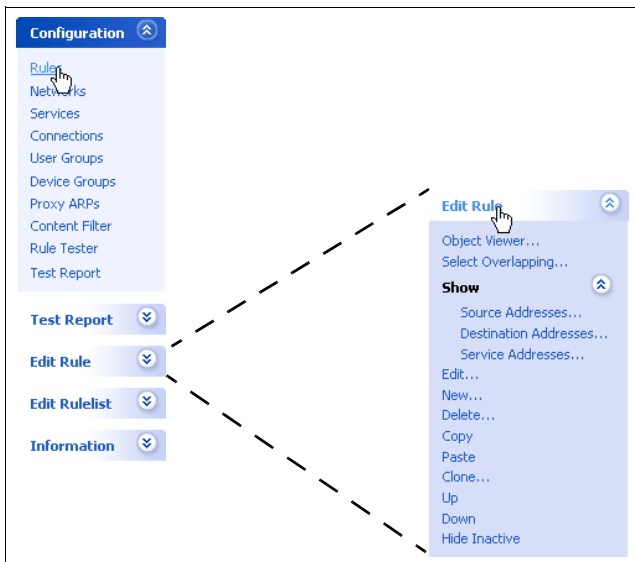
➤ the **configuration area** in the main window.

Fig. 4-7 Rule set configuration interface



The item **Configuration** is the navigation bar's main element. Clicking a sub-item of it displays further navigation items directly related to the element that is to be configured.

Fig. 4-8 Open navigation bar



The following organisational segments are made available through the navigation bar:

List 4-15 Items of the Navigations Bar's main element "Configuration"

View	Description	see
<b>Rules</b>	Click <b>Rules</b> to configure general settings applying to the rule set, and to create and modify single rules and rule list in the <b>Firewall - Rules</b> window.	page 135
<b>Networks</b>	Click <b>Networks</b> to define network objects (for referencing purpose within the <b>Firewall - Networks</b> window).	page 140
<b>Services</b>	Click <b>Services</b> to define service objects (for referencing purpose within the <b>Firewall - Services</b> window).	page 143
<b>Connections</b>	Click <b>Connections</b> to define connections objects (for referencing purpose within the <b>Firewall - Connections</b> window).	page 145
<b>User Groups</b>	Click <b>User Groups</b> to define users/user groups (for referencing purpose within the <b>Firewall - User</b> window).	page 150

List 4-15 Items of the Navigations Bar's main element "Configuration"

View	Description	see
<b>Interface Groups</b>	Click <b>Interface groups</b> to define interface objects (for referencing purpose within the <b>Firewall - Device Groups</b> window).	page 150
<b>Proxy ARPs</b>	Click <b>Proxy ARPs</b> to define proxy ARP objects (for referencing purpose within the <b>Firewall - Proxy ARPs</b> window).	page 150
<b>Content Filter</b>	Click <b>Content Filters</b> to define filter patterns for intrusion prevention purpose in the <b>Firewall - Content Filter</b> window.	page 151
<b>Rule Tester</b>	Click <b>Rule Tester</b> to test the integrity of rules in the <b>Firewall - Rule Tester</b> window.	page 163
<b>Test Report</b>	Click <b>Test Report</b> to archive and/or modify executed test reports in the <b>Firewall - Test Report</b> window.	page 164

**Note:**  
Regard the following **navigation bar items** in the **Firewall - Rules** window with special attention:

➤ **Show**  
Use the Show function to get a quick overview of objects used in a rule set.

Select a rule in the rule set overview (Firewall - Rules) window and click **Show** in the main navigation bar. The following sub-items are now displayed for further choice:

- **Source Addresses**
- **Destination Addresses**
- **Service Addresses**

Click each of these items in the sub-menu. For every link clicked, a new window opens, displaying Source, Destination, and Service Addresses of the selected rule respectively. Browse through the rules in the rule overview window and notice the changing addresses in the address windows.

➤ **Hide/Show Inactive**  
Rules can be disabled temporarily by ticking the checkbox inactive (inactive checkbox, page 136). Click **Hide Inactive** to remove an inactive rule from the view. Click **Show Inactive** to fade it in again.

➤ **Select Overlapping**  
This feature can be used to test a rule set's integrity. For a detailed description see 4.2 Overlapping Rules, page 163.

**Note:**  
Regard the following **context menu items** in the **Firewall - Rules** window with special attention:

➤ **New / Edit / Delete Section ...**  
Sections are available with firewall Feature Level set to Release 3.6.0, 4.0.0 and 4.2.0 (list 4-16, page 135, **Setup**). Sections can be introduced to tidy up the view in large rule sets. Select **New Section ...** to create a section and specify a name for it. All existing rules are automatically assigned to the first created section. As

soon as multiple sections have been created, rules can be dragged from it to other sections.

**Attention:**

Rules should be arranged in sections according to their processing workflow.

When a section is deleted with **Delete Section ...**, only the section header is removed, the sortation order of the rules remains unchanged.

**Note:**

Changing the Feature Level to a lower level than 3.4.0 irreversibly deletes configured sections.

➤ **Show in Sections**

Creating a section automatically activates the view **Show in Sections**. Clear this menu item to switch back to the default view.

### 2.2.3 Rules Configuration

The rule set is configured and managed in the **Firewall - Rules** window. To enter the rules configuration window click **Configuration > Rules** in the navigation bar.

The Firewall - Rules window displays the rule set in the main window and makes the following further main navigation bar items available:

➤ **Test Report**

This item allows testing the rule set's integrity (see 4. Testing and Verifying of Rule Sets, page 163 for a detailed description).

➤ **Edit Rule**

This item makes elements available allowing creation and modification of rules (see 2.2.3.1 Creating a New Rule).

**Note:**

With multiple rules selected in the rule overview window the right-click context menu entry **Edit Multiple Rules** becomes available. See 2.3.3.1 Multiple Rules Editing, page 156 for a summary of attributes, which can be edited together.

**Note:**

The option **Edit Multiple Rules** is not available if the view is set to **Show in Sections** and a section is selected. Select "real" rules only.

➤ **Edit Rulelist**

This item allows the creation of subordinate rule lists, to which specific items from the main rule list can be cascaded (see 2.5.1 Cascaded Rule Lists, page 160 for a detailed description).

**Note:**

Forwarding Firewall: The actions **New Rulelist** and **Remove Rulelist** can be executed through the context menu on the tabs of the rulelist(s).

➤ **Information**

Elements in this navigation bar item apply to global rule set settings. The following actions are available:

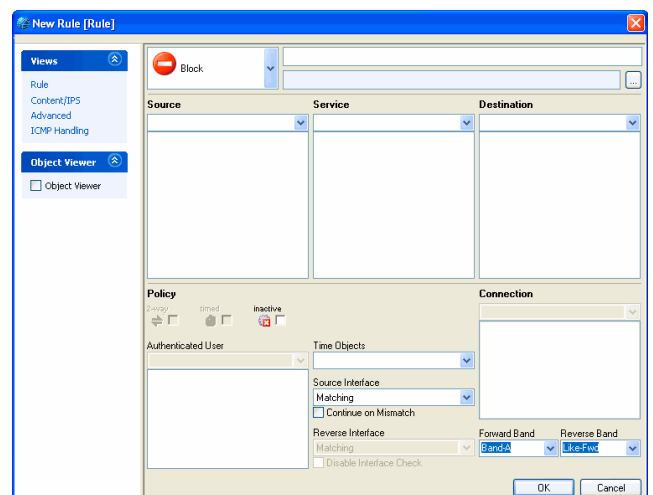
**List 4-16** Subordinate elements of the item Information in the navigation bar

Action	Description
<b>Setup</b>	Via this button the version compatibility of the rule set is defined. <b>Attention:</b> To use all features of the firewall rule set it is necessary to set the feature level explicitly to 3.4.0/3.6.0/4.0.0/4.2.0. This is necessary since a rule set containing 3.4.0/3.6.0/4.0.0/4.2.0 features is not compatible with a firewall of release 3.2.0 or 2.4.2. For setting the rule set version, lock the rule set and enter the menu by clicking <b>Setup</b> in the navigation bar.
<b>Export Rulelist ...</b>	Clicking this item exports the rule list to a file. Rule list files (.fwrule7 files) should be created as backup files before modifying a working rule set.
<b>Import Rulelist ...</b>	Clicking this item allows importing contents of a rule list (.fwrule7) file.
<b>Reload Externals</b>	Global firewall objects are updated.
<b>Reload GTI Objects</b>	This function is only available for MC administered firewalls in combination with a running VPN service. A global GTI Object is created for every tunnel endpoint inserted into the Global VPN GTI Editor ( <b>phion management centre</b> - 15. VPN GTI, page 464, 15.1.2 User Interface - Canvas Section, page 465). The function <b>Reload GTI Objects</b> reloads networks objects, which have been introduced in the graphical tunnel interface through creation of tunnel endpoints. Lock the <b>Global Firewall Objects</b> node ( <b>phion management centre</b> - 6.3.2.1 Global GTI Objects, page 411) and click <b>Reload GTI Objects</b> to refresh the view after new tunnel endpoints have been introduced. GTI objects are arranged in the dynamic networks section and their names begin with a prefixed <i>GTI-Server</i> label. <b>Note:</b> <i>GTI-Server</i> objects are inherited as references by the Local and Forwarding Firewall rule sets of each Firewall service related to the tunnel endpoint and may be used for rule specification.

#### 2.2.3.1 Creating a New Rule

To create a new rule, lock the rule set and click **Edit Rule > New ...** in the navigation bar. This opens the **New Rule** dialogue (figure 4-9):

**Fig. 4-9** New Rule dialogue





### Contents of the navigation bar

The rule configuration window opens with its default view, the **Rule** view. Further available views, which can be chosen by clicking the elements in the navigation bar item **Views** in the rule window, are the following:

- **Content/IPS**  
Allows selecting a content filter applying to the rule. Creation and modification of content filters is described in 2.3.1 Content Filter (Intrusion Prevention), page 151
- **Advanced**  
Allows configuring advanced settings applying to the rule. A summary of existing advanced settings parameters is given in 2.3.3 Advanced Rule Parameters, page 154.
- **ICMP Handling**  
Allows configuring a specific ICMP handling applying to the rule. A summary of ICMP settings is given in 2.3.4 ICMP Handling, page 158.
- Clicking the checkbox **Object Viewer** opens the viewer directly adhering to the rule window. The object viewer's behaviour pattern is described in 2.2.1.3 The Object Viewer.

### Contents of the main rule window

The range of fields available or activated in the main rule window is predetermined by specific selections made in previous fields. A rule, for example defining to block a connection attempt, can never apply both ways. The checkbox **2-way** is thus already activated, when  **Block** is selected. Selecting  **Pass** on the other hand, activates the **2-way** checkbox and expects input in the **Connection** section.

Amongst others, the following parameters are always available for configuration, regardless of the configured action:

List 4-17 Firewall configuration - Rule Creation/Editing

Parameter	Description
<b>Name</b>	This uppermost field of the rule window takes the rule's name. Assigning a name to the rule is mandatory. The maximum length of this parameter is 50 characters.
<b>Description</b>	Enter a significant description of the rule.
<b>Timed</b> checkbox	Via this checkbox it is possible to activate the rule dynamically. Due to the complexity of this feature, have a look at the description under 2.3.5 Dynamic Activation, page 159.
<b>inactive</b> checkbox	Ticking this checkbox deactivates the rule. For reactivation of the rule simply clear the checkbox again. Inactive rules can be removed from or faded in the view by clicking <b>Show/Hide Inactive</b> in the navigation bar.
<b>Forward Band</b> <b>Reverse Band</b>	These parameters are used with traffic shaping activated ( <b>Configuration Service</b> - 2.2.6 Traffic Shaping, page 81).

### 2.2.3.2 Source Section






This section describes the source IP address/netmask of the connection affected by the rule. You may select an already existing network object from the menu or enter an explicit IP address/netmask.

The configuration dialogue in this place, is the same as described under 2.2.4 Network Objects, page 140.

### 2.2.3.3 Action Section

This section defines the handling of a connection attempt. The following actions are available:

List 4-18 Firewall configuration - Action section

Icon	Action	Defining property	Additional parameters	
	<b>Block</b>	Ignore all traffic which matches the rule and do not answer to any matching packet.		
	<b>Deny</b>	Dismiss any traffic and send <ul style="list-style-type: none"> <li>• TCP-RST (for TCP requests)</li> <li>• ICMP Port Unreachable (for UDP requests)</li> <li>• ICMP Denied by Filter (for other IP protocols) to the source.</li> </ul>		
	<b>Pass</b>	Destination IP/Port is identical to Connection IP/Port.	<b>2-Way</b>	This opens the route the other way around.  <b>Attention:</b> This can be a severe security hole if you do it carelessly. Depending on the connection type of the rule the reverse direction can be of pass or a redirect type. Activating the check box will work regardlessly.
	<b>Redirect</b>	General Destination IP/Port Rewriting. Connection type can be chosen freely (can be used to have source NAT and destination NAT at once).	<b>Fallback</b> <b>Cycle</b>	Policy for the use of the IPs in the target list. <b>Fallback</b> always redirects to the first available IP in the list. <b>Cycle</b> calculates which one to use from the source IP. So the same source will be redirected to the same target every time.
	<b>Redirect Object</b>	General Destination network/Port Rewriting. Connection type can be chosen freely (can be used to have source NAT and destination NAT at once).	<b>Fallback</b> <b>Cycle</b>	Policy for the use of the IPs in the target list. <b>Fallback</b> always redirects to the first available IP in the list. <b>Cycle</b> calculates which one to use from the source IP. So the same source will be redirected to the same target every time.

List 4-18 Firewall configuration - Action section

Icon	Action	Defining property	Additional parameters	
	<b>Map</b>	One destination IP or a whole subnet can be mapped to another IP-object of some size. The map is also available the reversed way. The connection type can either be client (destination NAT) or any pre-defined Translation Map (see 2.2.6.3 Translation Map, page 149).	<b>2-Way</b>	This opens the route the other way around.  <b>Attention:</b> This can be a severe security hole if you use it carelessly. The type of a reverse map would be of pass type with explicit source NAT. Activating the check box will work regardless.  <b>Attention:</b> When using a map object in parameter <b>Connection Type</b> all connections not affected by this map rule are forwarded with connection type <b>proxy dyn</b> .
	<b>Local Redirect</b>	Traffic is redirected to a local application (Transparent Proxying)  <b>Note:</b> Advanced parameters and timeouts of this type behave like in the local firewall.		
	<b>Local Redirect Object</b>	Traffic is redirected to a network object.  <b>Note:</b> Advanced parameters and timeouts of this type behave like in the local firewall.		
	<b>Broad-Multicast</b>	Traffic is propagated to multiple interfaces (only needed with Bridging, see 9. Bridging, page 187).	Propagation list field	Defines the interface distributing broad-and multicast messages.
	<b>Cascade</b>	No traffic is yet affected. It is a jump into other parts of the rule set (see 2.5.2 Cascaded Rule Sets, page 160).	Rule set list	Defines the rule set traffic is cascaded to.
	<b>Cascade Back</b>			
	<b>Execute</b>	All traffic is piped into the STDIN ( <b>STANdard IN</b> ) of a program running on the server.	Executable field	Name of the binary (full pathname)

### 2.2.3.4 Destination Section







The available settings in this section depend on the configured **Action** type:

List 4-19 Firewall configuration - Destination section

Icon	Action	Destination	Additional parameters	
	<b>Block</b>	You may select an already existing network object from the menu. The configuration dialogue in this place is the same as described under 2.2.4 Network Objects, page 140.	<b>Explicit</b>	You may enter an explicit IP address/netmask. The configuration dialogue in this place, is the same as described under 2.2.4 Network Objects, page 140.
	<b>Deny</b>			
	<b>Pass</b>			
	<b>Redirect</b>	IP address to be redirected (Destination IP)	<b>Create Proxy ARP</b>	Activate if you want a Proxy ARP to be generated by the firewall. If the IP is already in the list, you do not need to activate it, but it does not bother anyway.  <b>Attention:</b> Due to fact that using Proxy ARPs is not without a risk, please consult 2.2.9 Proxy ARPs, page 150, for further information.
	<b>Redirect Object</b>	You may select an already existing network object from the menu or enter an explicit IP address/netmask. The configuration dialogue in this place, is the same as described under 2.2.4 Network Objects, page 140.	<b>Explicit</b>	You may enter an explicit IP address/netmask. The configuration dialogue in this place, is the same as described under 2.2.4 Network Objects, page 140.
	<b>Map</b>	One destination IP or a whole subnet can be mapped to another IP-object of same size. The map is also available the reversed way. The connection type can either be client (destination NAT) or any pre-defined Translation Map (Translation Map, page 149).	<b>Create Proxy ARP</b>	Activate if you want a Proxy ARP to be generated by the firewall. This option does not necessarily have to be activated if the IP is already included in the Proxy ARP list. Ticking the checkbox will not disturb the existing object, though.  <b>Attention:</b> Due to fact that using Proxy ARPs is not without a risk, please consult 2.2.9 Proxy ARPs, page 150, for further information. A referenced translation map will be read from right to the left. Proxy ARPs will be generated only if the netmask is at most 8bit long (phion notation - 255.255.255.0). ( <b>Getting Started</b> - 5. phion Notation, page 25)



List 4-19 Firewall configuration - Destination section

Icon	Action	Destination	Additional parameters	
	<b>Local Redirect</b>	<b>Note:</b> Advanced parameters and timeouts of this type behave like in the local firewall.	<b>Create Proxy ARP</b>	Activate if you want a Proxy ARP to be generated by the firewall. If the IP is already in the list, you do not need to activate it, but it does not bother anyway.  <b>Attention:</b> Due to fact that using Proxy ARPs is not without a risk, please consult 2.2.9 Proxy ARPs, page 150, for further information.
	<b>Local Redirect Object</b>	Traffic is redirected to a network object.  <b>Note:</b> Advanced parameters and timeouts of this type behave like in the local firewall.		
	<b>Broad-Multicast</b>	Traffic is propagated to multiple interfaces (only needed with Bridging, see 9. Bridging, page 187).		
	<b>Cascade</b>	No traffic is yet affected. It is a jump into other parts of the rule set (see 2.5 Cascaded Rule Sets, page 160).	Rule set list	Defines the rule set traffic is cascaded to.
	<b>Cascade Back</b>			
	<b>Execute</b>	Redirects traffic to an executable (std_in - incoming traffic; std_out - outgoing traffic)		

### 2.2.3.5 Redirection Section

Depending on the relative properties of the redirected IP Range and the target IP, there are four types of redirecting:









- The target IP range is as large as the redirected range (for example 10.0.0.128/4 to 192.168.32.0/4). The IP addresses are mapped one to one.
- The target IP range is larger than the redirected range (for example 10.0.0.128/4 to 192.168.32.0/8). The "most fitting" IP address is taken, for example 10.0.0.130 to 192.168.32.130.
- The target IP range is smaller than the redirected range (for example 192.168.32.0/8 to 10.0.0.128/4). The larger range is mapped to the smaller range, for example 192.168.32.2 as well as 192.168.32.130 to 10.0.0.130, and 192.168.32.30 to 10.0.0.142.
- One IP is redirected to several other IPs (for example 192.168.32.3 to [10.0.0.23 10.0.0.68]). Depending on the chosen policy (**Fallback** or **Cycle**) requests are redirected to one of the target IPs.

#### Multiple Redirecting (Failover and/or Load Sharing)

- **Failover:** All IPs from the redirect list are tested and IPs where no connection could be established are marked as unreachable. The process lists for how long the IP was unreachable (**last time**) and how often retries took place. As soon the retry time is smaller than the last time, the IP is considered as reachable and a new connection attempt is started.
- **Load Sharing:** The principle is the same as for failover, except for that the valid index for the connection establishment results from the SRC IPs.

The available settings of this section are depending on the set **Action** type:

List 4-20 Firewall configuration - Redirection section

Icon	Action	Parameter	Description
	<b>Block</b>		not available
	<b>Deny</b>		not available
	<b>Pass</b>		not available
	<b>Redirect</b>	<b>Target List</b>	List of targets that the clients should be redirected to (possible connection IPs). By entering a colon it is possible to define the port.  <b>Attention:</b> When entering a specific port be sure to have the correct service selected. Otherwise it will not work at all.
		<b>List of Critical Ports</b>	By default, the available/unavailable policy considers all ports of the allowed rule services. If a connection to such a port fails the target is marked unavailable and the rest of the targets are used as the new list. If there are entries in the critical ports list, only failed connections to these ports lead to a state change of the respective target from available to unavailable. Separate multiple critical port entries with a space.
	<b>Redirect Object</b>	<b>Target List</b>	List of targets that the clients should be redirected to (possible connection IPs). By entering a colon it is possible to define the port.  <b>Attention:</b> When entering a specific port, be sure to have the correct service selected. Otherwise it will not work at all.
		<b>List of Critical Ports</b>	By default, the available/unavailable policy considers all ports of the allowed rule services. If a connection to such a port fails, the target is marked unavailable and the rest of the targets are used as the new list. If there are entries in the critical ports list, only failed connections to these ports lead to a state change of the respective target from available to unavailable. Separate multiple critical port entries with a space.
	<b>Map</b>	<b>Real IP/Mask</b>	IP to be redirected (Destination IP)
		<b>Referenced Map</b>	Instead of explicit mapping you can also refer to a pre-defined connection object of type translation map.
	<b>Local Redirect</b>	<b>Local Address</b>	Local address the request is redirected to.  <b>Note:</b> Advanced parameters and timeouts of this type behave like in the local firewall.
	<b>Local Redirect Object</b>	<b>Local Address</b>	Local address the network object is redirected to.  <b>Note:</b> Advanced parameters and timeouts of this type behave like in the local firewall.



List 4-20 Firewall configuration - Redirection section

Icon	Action	Parameter	Description
	<b>Broad-Multicast</b>		not available
	<b>Cascade</b>		not available
	<b>Cascade Back</b>		not available
	<b>Execute</b>		not available

### 2.2.3.6 Service Section

This section provides all already configured service objects affected by the rule. The objects describe the used protocol as well as the used port/port range.

You may select an already existing service object from the menu or enter an explicit service object.

The configuration dialogue in this place, is the same as described under 2.2.5 Services Objects, page 143.

### 2.2.3.7 Connection Section

The available settings in this section depend on the configured **Action** type:

List 4-21 Firewall configuration - Connection section

Icon	Action	Description
	<b>Block</b>	not available
	<b>Deny</b>	not available
	<b>Pass</b>	The connection element of a firewall rule defines the bind address. This is the address which is used by the firewall to connect to the target computer.
	<b>Redirect</b>	You may select an already existing service object from the menu or enter an explicit service object.
	<b>Redirect Object</b>	The configuration dialogue in this place, is the same as described under 2.2.6 Connection Elements, page 145.
	<b>Map</b>	A more advanced type of connection is the translation map. Here you can define more sophisticated source-NAT rules. For more information concerning maps have a look at 2.2.6 Connection Elements, page 145.
	<b>Local Redirect</b>	not available
	<b>Local Redirect Object</b>	not available
	<b>Broad-Multicast</b>	The connection element of a firewall rule defines the bind address. This is the address which is used by the firewall to connect to the target computer. You may select an already existing service object from the menu or enter an explicit service object. The configuration dialogue in this place, is the same as described under 2.2.6 Connection Elements, page 145.
	<b>Cascade</b>	not available
	<b>Cascade Back</b>	not available
	<b>Execute</b>	not available

### 2.2.3.8 Authenticated User Section

This section is needed for Firewall Authentication (see 10. Firewall Authentication, page 188) and defines the user(s)/usergroup(s) affected by this rule.

You may select an already existing user/usergroup from the menu or enter an explicit user/group.

The configuration dialogue in this place, is the same as described under 2.2.7 User Groups, page 150.

If the rules requires user authentication at the firewall, the rule is depicted with a icon in the Name column in the rule overview window.

### 2.2.3.9 Source Interface Section / Reverse Interface Section

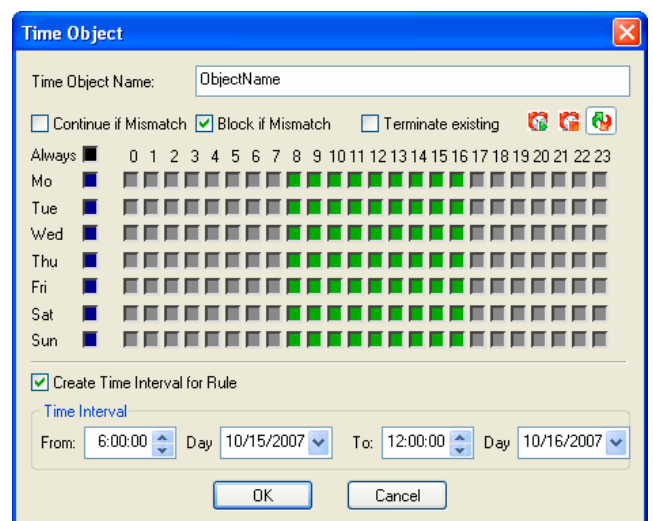
This section specifies, which interfaces should be utilised when the rule is processed. For a description of configuration details see 2.2.8 Interface Groups, page 150.

### 2.2.3.10 Time Objects

**Note:**  
Starting with netfence 3.4, Time Objects have been introduced to configure rules with a time restriction. Select **New Time Object ...** in the **Time Objects** tab from the Object Viewer to create a New Time Object. For netfence gateways configured with a feature level equal to or lower than 3.2 (see Setup, page 135) use the **Time Restriction** (see Time Restriction, page 155) parameter in the Advanced settings to configure rules with a time limitation. Time Objects cannot be combined with a Time Restriction. Either the former or the novel method has to be used.

The granularity of time limitation is 1 hour on a weekly base.

Fig. 4-10 Time Object configuration dialogue



A rule is allowed at all times by default, that is all checkboxes in the **Time Object** dialogue window are unchecked. Checking a box denies a rule for the given time.

List 4-22 Firewall configuration - Time Object

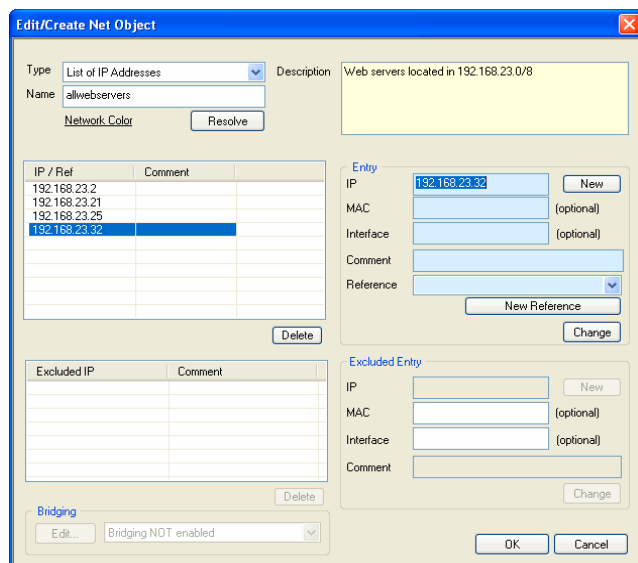
Parameter	Description
<b>Time Object Name</b>	Specify a name for the time object.
Set allow	Select  to clear selected checkboxes.
Set deny	Select  to select checkboxes as disallowed time intervals.
Set Invert	Select  to configure allowed and disallowed time intervals simultaneously.
<b>Continue if mismatch (default)</b>	Process the rule set even if time restriction denies it.
<b>Block if mismatch</b>	Do not allow connection if time restriction denies it.
<b>Terminate existing</b>	If checked an active session is terminated as soon as time restriction applies.
<b>Create Time Interval for Rule checkbox</b>	Select this checkbox to create a time limited interval for the specific rule instead of a validity based on days of the week. Exact dates and times of day may be specified by selection in the calendar list.

## 2.2.4 Network Objects

The **Firewall - Networks** window assort network objects that have been assigned with labels for easier recognition and handling. Network objects are designed to be used for example in the following way:

Instead of itemising single web servers running on the IPs 192.168.23.2, 192.168.23.21, 192.168.23.25, and 192.168.23.32, all servers can be summed up in a network object called **allwebservers**. This network object can be used to define actions applying for all servers. Again, if a further web server is created running on the IP address 192.168.23.34, there is no need to create further rules applying to it. The additional web server simply has to be added to the network object **allwebservers**. It will thus inherit all properties from the existing object.

Fig. 4-11 Creating/editing a net object called allwebservers



Beside the local and forwarding firewall, network objects may reside in the following configuration areas of management centres:

### ➤ Global Firewall Objects

(accessible through **Multi-Range** > **Global Settings**) (**phion management centre** - 6.3.2 Global Settings - Global Firewall Objects, page 411)

### ➤ Range Firewall Objects

(accessible through **Multi-Range** > <rangename> > **Range Settings**) (requires activation of **Own Firewall Objects** in the Range Config file, see **phion management centre** - 6.4 Range Configuration, page 416)

### ➤ Cluster Firewall Objects

(accessible through **Multi-Range** > <rangename> > <clustername> > **Cluster Settings**) (requires activation of **Specific Firewall Settings** in the Cluster Config file, see **phion management centre** - 6.5 Cluster Configuration, page 417)

#### Note:

MC-administered boxes inherit all network objects created in these configuration areas as external objects.

**Networks** objects may consist of the following:::

List 4-23 Net Object configuration parameters

Parameter	Description
<b>Type</b>	<ul style="list-style-type: none"> <li>➤ <b>Generic Network Objects</b> may combine network addresses of all types. All network objects that are available on netfence systems by default are configured as generic network objects.</li> <li>➤ <b>Single IP Address</b> Selecting this type allows inserting a single IP address into the <b>IP / Ref</b> list.</li> <li>➤ <b>List of IP Addresses</b> Selecting this type allows inserting single IP addresses and/or references to other single IP address objects into the <b>IP / Ref</b> list.</li> <li>➤ <b>Single Network Address</b> Selecting this type allows inserting a single network address into the <b>IP / Ref</b> list.</li> <li>➤ <b>List of Network Addresses</b> Selecting this type allows inserting multiple network addresses (networks and IP addresses) and/or references to other network address objects into the <b>IP / Ref</b> list.</li> <li>➤ <b>Hostname (DNS Resolved)</b> Selecting this type allows specifying a DNS resolvable host name as network address.</li> </ul> <p><b>Attention:</b> Network objects of type Hostname come along with a number of specialities and potential security issues when applied wrongly. Pay regard to their attributes with essential care. See 2.2.4.1 Hostname (DNS Resolvable) Network Objects, page 141 for a detailed description of configuration options.</p>

List 4-24 Net Object configuration parameters - section Excluded Entry

Parameter	Description
<b>Excluded Entry</b>	This section allows excluding specific networks from a network object. A preconfigured network object using this feature is the object <b>Internet</b> located in the Local Networks list of every Forwarding Firewall service created on a netfence gateway. The <b>Internet</b> object excludes the networks 10.0.0.0/24, 172.16.0.0/20, and 192.168.0.0/16 from the network object <b>World</b> (0.0.0.0/32), which is the mostly intended use, when creating rules assigned to Internet access.
<b>Note:</b>	For transparency and consistency reasons references are not available in the <b>Excluded Entry</b> section.

List 4-25 Net Object configuration parameters - section Bridging

Parameter	Description
	<p><b>Note:</b> The configuration options in the <b>Bridging</b> section are only applicable for <b>Layer3 Bridging</b>. See 9.3.3 Layer3 Bridging, page 181 for general information and 9.6.2.4 Using Layer3 Bridging, page 186 for exemplary configuration details.</p> <p>When bridging is activated on an interface, host routes and PARPs may automatically be generated by the netfence gateway. This section allows you to specify the information required for this task. The Bridging section is only available in the <b>Local Networks</b> list of the Forwarding Firewall Service. Select <b>Bridging ENABLED (Advanced Settings)</b> from the list (default: <b>Bridging NOT Enabled</b>) if you want to configure bridging details.</p>
<b>Device Addresses Reside</b>	Insert the name of the interface here, on which bridging shall be enabled (for example eth1).
<b>Parent Network</b>	Insert the superordinate network here, from which the bridged interface has been separated (see example setup in 9.6.2.4 Using Layer3 Bridging, page 186).
<b>Introduce Routes checkbox</b>	Select this checkbox if you want the netfence gateway to introduce host routes to the IP addresses to be separated from the superordinate network (IPs enlisted in the network object) automatically.
<b>Restrict PARP to Parent Network checkbox</b>	Select this checkbox if you want the netfence gateway only to answer the automatically introduced ProxyARPs to hosts within the parent (superordinate) network.

Create and make use of network objects to benefit from the following:

- Labelled IP and network addresses can easily be identified and handled by their name.
- Network objects may easily be edited and extended when network addresses in productive environments change.
- Working with network objects instead of explicit IP addresses allows you to construct a consistent hierarchical structure of your network and to implement consistent security policies
- In firewall rule sets that employ references to network objects instead of explicit IP addresses, rule configurations do not have to be edited when IP addresses within objects change.
- Network objects may be referenced in all generic configuration dialogues of the management centre configuration tree in places where IP addresses or networks have to be inserted (IP/network address field flagged with the icons), with the exception of DNS zone configuration, Personal Firewall configuration, MC administrator configuration, and the explicit tunnel override dialogues provided by the VPN GTI. Click the icon to open the **Network Objects** window from which the network object reference can be chosen. Click the icon to delete the reference. This feature protects your from adverse side-effects that may arise from incomplete address changes throughout multiple configuration instances.

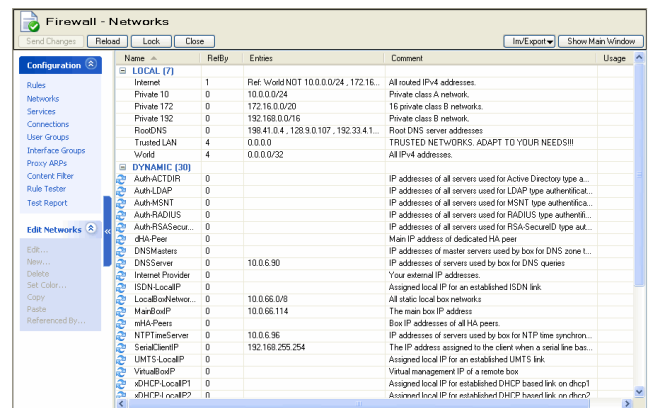
**Note:**  
Creating references to network objects in generic configuration areas is only possible in the management centre configuration tree and not on MC-administered or single boxes.

**Note:**  
Once created, a network object's type may not be changed.

**Note:**  
Character restriction: you may use spaces for the **Name** (figure 4-11, page 140) of your global firewall object. But this object will only be visible within the firewall rule set, it cannot be selected as reference from the **Network Objects** dialogue (figure 18-44, page 418).

**Attention:**  
Network objects may not be deleted, if other objects are referencing to it. They may be deleted when referenced by configuration files, though. Make sure that network objects are not referenced before deleting them. If objects are referenced can be seen in the RefBy column in the Network Objects listing (figure 4-12).

Fig. 4-12 Firewall - Networks window - Listing of Network Objects



### 2.2.4.1 Hostname (DNS Resolvable) Network Objects

**Note:**  
Hostname network objects are available as from netfence 3.6.3. Always use the correct phion.a version when editing Hostname objects.

**Attention:**  
Do not import rule sets containing Hostname network objects on netfence gateways with version numbers 3.6.3 or lower.

Firewall rule sets steer the processing of IP packets. As IP packets only know a destination IP address and not a host name, the allocation of host names to appropriate IP addresses must be managed through the firewall.

Network objects of type **Hostname** allow specifying DNS resolvable host names as network addresses, and in this way make the use of host names in firewall rules possible.

**Note:**  
Note that only explicitly defined host names (for example www.phion.com) but no comprehensive zone names may be used in network objects.

**Note:**  
A DNS Server must be specified in the **DNS Server IP** field in the **Box Settings** file (**Configuration Service - 2.2.3.3 DNS**, page 55), in order to use network objects of type **Hostname**.

Using DNS resolvable host names in firewall rule sets can cause problems because of the following:

- IP addresses that are allocated to DNS host names might change.
- A DNS record might contain multiple IP addresses.

### Creating network objects of type Hostname

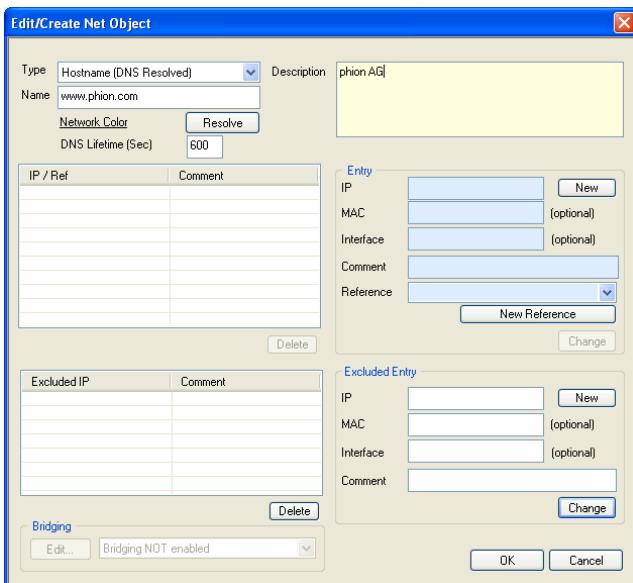
Hostname objects may be created in:

- the Local Firewall rule set
- the Forwarding Firewall rule set
- as Global, Range- or Cluster-specific firewall objects

**Note:**  
Hostname objects **may NOT** be created as explicit source or destination objects in firewall rules.

To create a network object of type **Hostname**, select **Hostname (DNS resolved)** from the **Type** list in the Net Object window. Consider the following detail configuration options:

Fig. 4-13 Network Object - Type Hostname (DNS Resolved)



List 4-26 Network Object - Type Hostname

Parameter	Description
<b>Type</b>	The Type defines specific object characteristics. Network objects of type <b>Hostname</b> expect specification of an explicit DNS resolvable host name in the Name field below. <b>Note:</b> Once the object has been created its type cannot be changed.
<b>Name</b>	Into this field insert the DNS resolvable name the object shall be created for. <b>Note:</b> The specified name is the name of the network object at the same time. The object name may be changed retroactively.
<b>Description</b>	Into this field insert a significant object description.

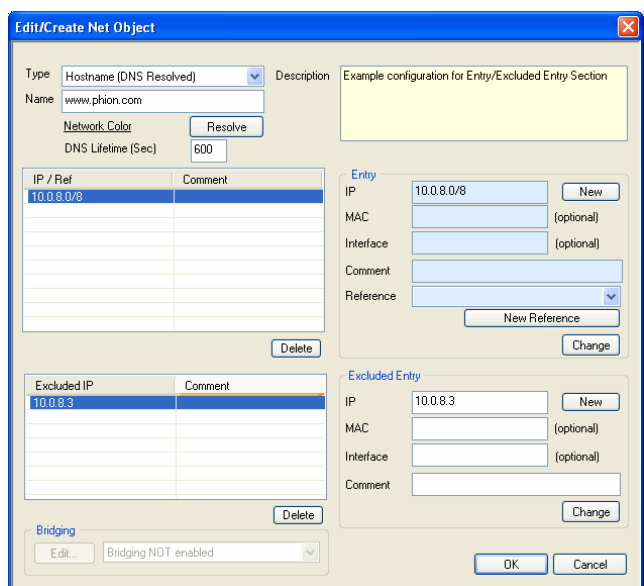
List 4-26 Network Object - Type Hostname

Parameter	Description
<b>Resolve</b>	The functionality of this button is purely informational. Click it to execute a DNS query for the host name inserted into the <b>Name</b> field. The result of the query is displayed in the <b>IP</b> field in the Entry section. Note that the query is executed using the DNS server(s) known to the client running the graphical administration tool phion.a and NOT using the DNS server(s) known to the netfence gateway running the firewall service.
<b>DNS Lifetime (Sec)</b>	The <b>DNS Lifetime</b> defines the interval after which to refresh DNS entries for network objects of type <b>Hostname</b> that are configured for use in currently effective firewall rules (default: <b>600 s</b> ). Setting to a lower value than 30 seconds might cause problems in network object lists containing a huge number of Hostname objects. DNS entries may also be refreshed manually in the Firewall Monitoring GUI > <b>Dynamic</b> tab > <b>Dynamic Rules</b> tab (see 6.5.1 Dynamic Rules, page 176). <b>Attention:</b> The DNS Lifetime has no effect on actively established connections, even if the DNS resolution of a network object that is currently used in a firewall rule changes. In this case to force a refresh terminate the active session in order to enable new connection establishment using the updated DNS entry.

List 4-27 Network Object - Type Hostname - section Entry / Excluded Entry

Parameter	Description
	The fields in the <b>Entry</b> and <b>Excluded Entry</b> sections may be used to restrict a network object and to force a condition to match explicitly or to exclude it from being part of it. For example, if a DNS host name entry <b>www.domain.com</b> matches four DNS A-records pointing to the IP addresses 10.0.6.1, 10.0.8.1, 10.0.8.2 and 10.0.8.3, and it is wanted that connection requests must always point to addresses residing in the 10.0.8.0/8 network, but must never be addressed to the IP address 10.0.8.3, the following values have to be configured in the corresponding fields (figure 4-14): ➤ <b>Section Entry:</b> IP 10.0.8.0/8 ➤ <b>Section Excluded Entry:</b> IP 10.0.8.3  The configuration stated above will be processed as follows, when it is utilised in a firewall rule: Connection requests may be addressed to IP addresses living in the network 10.0.8.0/8, but they may not address the excluded IP address 10.0.8.3.

Fig. 4-14 Hostname Network Object configuration example



### Using network objects of type Hostname

Hostname objects may be used as:

- Source/Destination in rules within the Forwarding Firewall

- Source/Destination in rules within the Local Firewall
- Reference in the Entry list of Generic Network Objects
- Hostname objects **may NOT** be used as reference in the Entry list of all other network object types.

**Attention:**

Hostname objects that cannot be resolved can never match in a rule. Consequently, when a non resolvable object is used in a rule, this rule cannot be processed correctly. Hostname objects will become non resolvable not only if they refer to a non existent host name, but also in case the DNS server queries are addressed to is unavailable.

**Attention:**

Do NOT use Hostname network objects in rules with the policy block.

**Note:**

When the firewall is (re)started, it may take up to 10 seconds until DNS resolution is provided for all configured Hostname network objects. Because the firewall is already active, it might happen that before the actually desired rule becomes active another rule matches a request.

**Note:**

Active sessions are not reevaluated when DNS resolution changes, but only when the rule itself is modified. Persistent sessions might have to be terminated manually in order to enable new connection establishment using the updated DNS entry.

**Monitoring network objects of type Hostname**

DNS queries addressed to the DNS server configured in the Box Settings are triggered as soon as a Hostname network objects is created. The result of these queries is visualised in the following places:

**Note:**

In all views but the *Dynamic Rules* tab, DNS resolution is retrieved using the DNS server(s) known to the client running the graphical administration tool phion.a and **NOT** using the DNS server(s) known to the netfence gateway running the firewall service.

- In the *Entries* column in the Network Object list (figure 4-12, page 141).
- In the Rule Object list when the Hostname object configured in the rule is used (figure 4-7, page 134).
- In the Source/Destination window querying the Rule Object list when the Hostname object is currently used (see Show, page 134).
- In the Rule Tester.
- In the *Dynamic Rules* tab (see 6.5.1 Dynamic Rules, page 176) of the Firewall Monitoring GUI.

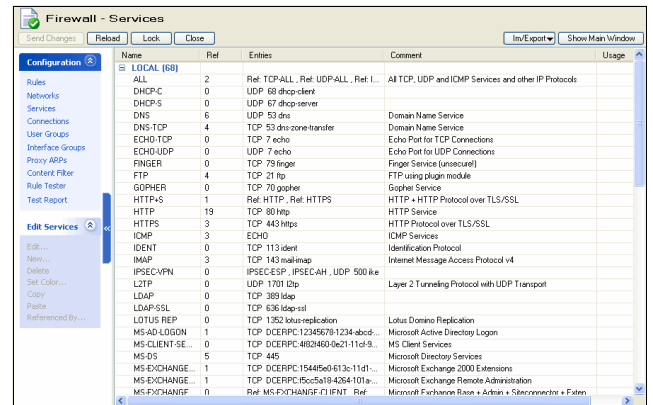
**2.2.5 Services Objects**

Services are terms for the ports involved in a network connection. A service is principally defined by the destination port. Nevertheless, it also defines the permitted client range and some other parameters.

Services objects can be simply put together as net objects. The only difference is that a service object has more properties than just a set of one or more ports, the succession of the individual sub-objects that build up a service object is important.

The default rule set of the phion firewall has a large list of predefined service objects. We will discuss the principal structure of a service object by dealing with the TCP-ALL example.

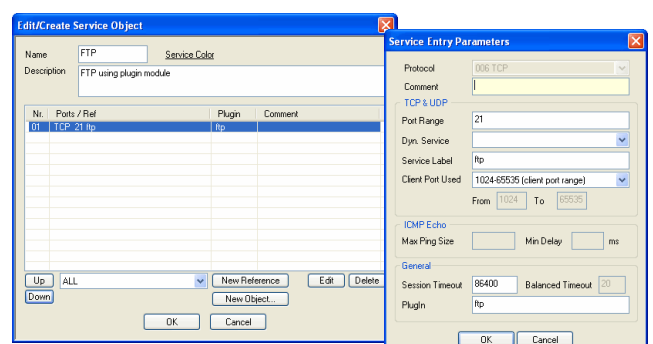
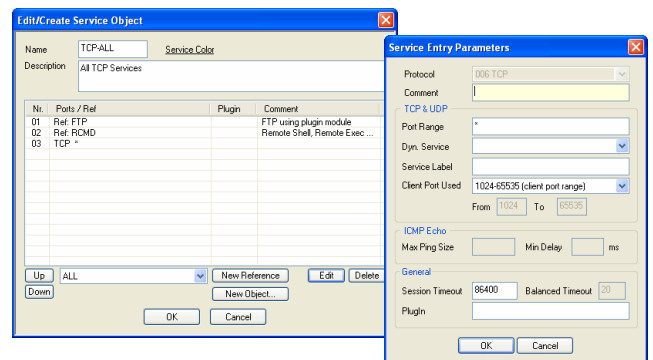
**Fig. 4-15** Part of the predefined services for the phion firewall



The service object TCP-ALL (figure 4-15) consists of five elements, though one would think that TCP-ALL simply means what the fifth element is: all ports for a TCP connection. There are two reasons for this. Two of them (ftp and rcmd) have different settings in the parameter section than TCP \* has. The presence of HTTP+S and SMTP only have administrative functions.

If you want the statistics to resolve the services it performs down to the lowest matching object. In this case this means that the statistics for a rule using TCP-ALL would resolve the traffic for the service objects FTP, RCMD, HTTP, HTTPS (because HTTP+S itself is a composite of HTTP and HTTPS), SMTP and the rest of TCP.

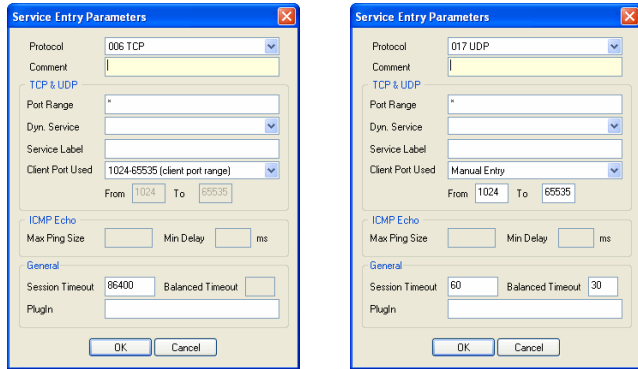
**Fig. 4-16** Service objects TCP-ALL and FTP





### 2.2.5.1 Parameters of Services

Fig. 4-17 Parameter section for TCP and UDP



List 4-28 Firewall configuration - Service Objects parameters - section TCP & UDP

Parameter	Description
<b>Port Range</b>	Port or port range the service is running on.
<b>Dyn. Service</b>	This parameter is required in conjunction with ONCRPC (see 11. RPC, page 193).
<b>Service Label</b>	Here you may enter certain labels. Leaving this parameter blank causes that well-known service names (available in <code>/etc/services</code> ) are used. <b>Attention:</b> It is highly recommended to use this parameter only for defining service names that are not "well-known ones" (for example, Oracle521, ...).
<b>Client Port Used</b>	Port range the firewall uses to build up the connection between itself and the destination. This port range is only used if a dynamic port allocation is required, as f.e. for the proxy dynamic connection type. Selecting Manual Entry enables the parameters From and To below, where you may enter a custom port range. <b>Note:</b> This parameter does not state a condition for rule-evaluation.

List 4-29 Firewall configuration - Service Objects parameters - section ICMP Echo

Parameter	Description
<b>Max Ping Size</b>	Defines the maximum allowed ping size.
<b>Min Delay</b>	Defines the minimum allowed delay for ping. <b>Note:</b> With eventing activated, the event <b>FW Flood Ping Protection Activated</b> [4002] is generated if this limit is under-run (see <b>Flood Ping</b> , page 130).

List 4-30 Firewall configuration - Service Objects parameters - section General

Parameter	Description
<b>Session Timeout</b>	Time in seconds a session may remain idle until it is terminated by the firewall (default values: TCP: <b>86400</b> , UDP: <b>60</b> , ICMP: <b>20</b> , all other protocols: <b>120</b> ). This timeout applies as only value for all TCP connections thereby counting the time that has passed in a session without traffic processing. Additionally, it applies as initial timeout for all session-like connections established through non-connection oriented protocols (for example, UDP or ICMP) thereby counting the time that has passed from the source's yet unanswered initial datagram. As soon as this datagram has been answered, the <b>Balanced Timeout</b> (see below) comes into effect. <b>Note:</b> This parameter is only executable in the forwarding firewall. Setting this parameter in the local firewall takes no effect.

List 4-30 Firewall configuration - Service Objects parameters - section General

Parameter	Description
<b>Balanced Timeout</b>	Time in seconds a session-like connection established through a non-connection oriented protocol (all protocols except TCP) may remain idle until it is terminated by the firewall (default values: UDP: <b>20</b> , ICMP: <b>10</b> , all other protocols: <b>120</b> ). The balanced timeout comes into effect, after the initial datagram sent by the source has been answered and the "session" has been established. Generally, the balanced timeout should be shorter than the session timeout, because it will otherwise be overridden by the session timeout and never come into effect. The balanced timeout allows for keeping non-connection oriented "sessions" short and minimising the amount of concurrent sessions. The larger initial session timeout guarantees that late replies to initial datagrams are not inevitably dropped. <b>Note:</b> This parameter is only executable in the forwarding firewall. Setting this parameter in the local firewall takes no effect.
<b>Plugin</b>	Name and parameters of the used plug-in (see 2.2.5.2 Plugin Modules, page 144).

### 2.2.5.2 Plugin Modules

There are some applications which do not use just simple communication between two predefined IPs over one or a few well defined ports.

A well known example is **FTP**: After an initial control dialogue over port 21, the client and the server use another random port from 1024 through 65535 to send and receive data. The firewall has two possibilities to handle this: either it opens all higher ports, which is not really suitable for a secure firewall, or it listens to the two FTP partners and opens the data channel just for this connection. In order to do this, you must use a so-called module.

Table 4-4 Currently available modules

Application/Protocol	Protocol family	Syntax with parameters	Description
FTP	TCP	ftp	
FTP	TCP	ftp samePort	Indicates that no PAT (Port Address Translation) is performed for ftp data sessions even if the firewall session is NATed. This way one can guarantee that the source port for an active FTP data session remains port 20.
RSH	TCP	rsh	Ensures that rsh works properly
ICA Browser	UDP	ica ip-address-1 ip-address-2 ip-address-3 ... ip-address-n	Used for the ICA browser application (mapping, redirecting). The pairs of IPs are mapped IP/real IP. If no NAT is involved, you have to declare the IPs as pairs as well.
Oracle SQL*Net	TCP	ora hostname=ip-address	Needed when the Oracle SQL*Net application uses dynamic ports. Also used in the context of destination NAT (mapping, redirecting). The Oracle server usually uses domain name resolution. Hence you have to give the IP/name pair to the module.
Trivial FTP	UDP	tftp	<b>Attention:</b> Inherently insecure. Read the explanation below.
ONCRPC	UDP & TCP	oncrpc	Use only with port 111 (RPC Port Mapper); in conjunction with 11. RPC, page 193.

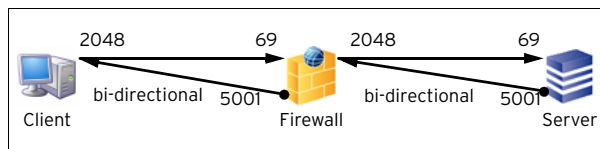
**Table 4-4** Currently available modules

Application/Protocol	Protocol family	Syntax with parameters	Description
DCERPC	UDP & TCP	dcerpc	Use only with port 135 (Endpoint Mapper); in conjunction with 11. RPC, page 193.
Skinny	TCP	---	The plugin monitors the skinny signalling connection between phone and Cisco call manager; use only with port 2000 (default port for signalling); for configuration details see <b>Voice over IP</b> - 2. SCCP, page 356.

➤ **Trivial FTP module**

The trivial ftp module can be used for all UDP applications, which maintain their connection on a different port than their initial starting port; trivial FTP is the most common example.

**Fig. 4-18** Connection situation for a UDP connection of tftp kind

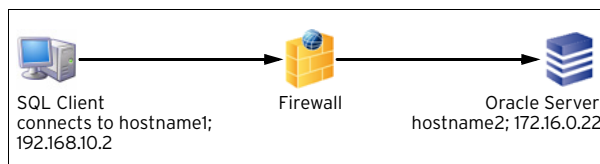


After an initiating request on port 69, the server for example answers with port 5001, and all subsequent traffic uses port 5001.

➤ **Oracle SQL\*Net module**

The SQL\*Net client by OracleTM uses IP and hostname to establish a connection to the server. Since these parameters can be different behind the firewall, it has to translate this information. The ora plugin module analyses the data stream of sqlnet sessions. The purpose of the plugin is to detect server responses during the initial sqlnet handshake that redirect the client to a different port on the server or even to another SQL server in a cluster. The redirection is communicated to the client by sending port numbers and hostname/IP-Addresses to the client. The plugin must create an acceptor for the expected dynamic session, and also must rewrite the hostnames or IP addresses to proper values, if destination address translation is used. Therefore, the plugin can be configured with hostname rewriting parameters that allow replacement of hostnames or IP address in the server response. The plug-in syntax (see above) allows various patterns which may be replaced with the intended addresses. Optional, a target address may be specified if a specific target IP address where is SQLNET session is to be connected to is required (SQLNET load balancing between oracle servers).

**Fig. 4-19** Connection situation for a SQL client connecting to an Oracle server



In the situation shown in figure 4-19 the plug-in settings have to be `ora hostname2=192.168.10.2`.

Since TNS structures can operate with different servers and hostnames you can use patterns for the hostname. Since the communication also involves a port change the plugin has to be used in any case. The `hostname2=hostname1` or `hostname2=hostname1,IP1` part is mandatory and must not be omitted. If database farms are used, the `hostname=IP` or `hostname2=hostname1,IP` entries have to be a space separated list.

## 2.2.6 Connection Elements

The connection element of a firewall rule defines the bind address. This address is used by the firewall to connect to the target computer.

There are essentially three ways of connecting the bind IP to the original Source IP.

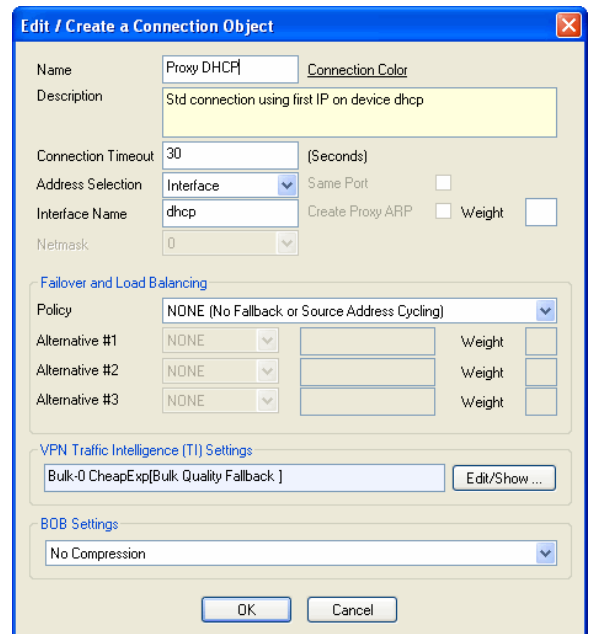
- Client - Source IP = Bind IP
- Proxy - Fixed Bind IP for all Clients (also called Masquerading or Source NAT)
- Explicit NAT - Explicit rule; assigns a bind IP to every source IP (Commonly called Source NAT)

To cover even the most complex network environments, the phion firewall allows for a large set of detailed connection types.

### 2.2.6.1 Standard Connections

To enter a new standard connection, click **New Standard ...** in the **Edit Connections** navigation bar.

**Fig. 4-20** Standard Connections - Edit / Create a Connection Object



The following options are available for configuration of a standard connection object:

**List 4-31** Firewall configuration - Service Objects - General settings

Parameter	Description
<b>Name</b>	Name of the connection object.
<b>Description</b>	Significant connection object description.
<b>Connection Color</b>	Choose a color, in which you want the connection object to be displayed in the Firewall - Connections window.

List 4-31 Firewall configuration - Service Objects - General settings

Parameter	Description
<b>Connection Timeout</b>	This general option for all connection types is the timeout for trying to establish a connection. The default value is <b>30</b> seconds. Increasing this value can be useful for very protracted connection partners. Decreasing this value can be useful for faster failover mechanisms.
<b>Address Selection</b>	This parameter specifies the Bind IP. The following options are available:
<b>Proxy Assigned</b>	Reserved for future use to implement policy routing based on administrative scope (organisational unit a host belongs to).
<b>Proxy First</b>	First IP address of server under which firewall service is operating. May be used to restrict the bind address or when policy routing is activated.
<b>Proxy Second</b>	Second IP address of server under which firewall service is operating. May be used to restrict the bind address or when policy routing is activated.
<b>Proxy Dynamic (default)</b>	Dynamically chosen according to firewall routing tables. This is a General purpose option.
<b>Client</b>	IP Address of the Client. Source IP = Bind IP
<b>Explicit</b>	Explicitly specified IP address. May be used to restrict the bind address to a specific address. Selecting <b>Explicit</b> activates further options below and in section Firewall configuration - Service Objects - General settings - section Failover and Load Balancing:
<b>Same Port</b>	Ticking this checkbox enforces to use the same client port when establishing the connection.
<b>Explicit IP</b>	Here the specific IP address is to be entered.
<b>Create Proxy ARP</b>	If the explicitly defined IP address does not exist locally, an appropriate ProxyARP entry may be created by selecting this checkbox
<b>Interface</b>	Explicitly specified interface. May be used to restrict the bind address to a specific interface. Selecting <b>Interface</b> activates further options below and in section Firewall configuration - Service Objects - General settings - section Failover and Load Balancing:
<b>Interface Name</b>	Here the name of the affected interface is to be entered.
<b>Map</b>	Source NAT for a complete subnet. In order to avoid dramatic misconfiguration, the netmask is limited to up to 16 bits. Otherwise, a Proxy ARP with 10.0.0.0/24 would "blank out" the whole internal network for example. <b>Attention:</b> If you define a map, you will have to make sure that the source range using this connection is equal or smaller than the map range. If not, the firewall will wrap the larger source net into the smaller bind net.
<b>Map to Network</b>	Here the specific mapping network is to be entered.
<b>Netmask</b>	Here the corresponding netmask is to be entered.
<b>Proxy ARP</b>	This parameter is needed by a router if the addresses live in its local network (2.2.9 Proxy ARPs, page 150).

**Note:**

The section **Failover and Load Balancing** is only available with parameter **Address Selection** set to **Explicit** or **Interface**.

List 4-32 Firewall configuration - Service Objects - General settings - section Failover and Load Balancing

Parameter	Description
<b>Policy</b>	This parameter allows you to specify what should happen if the connection cannot be established. Especially when having multiple providers and policy routing this parameter comes handy because it allows you to specify which IP address/interface has to be used for backup reasons. Otherwise, connecting via the backup provider using the wrong IP address in conjunction with the backup provider would make routing back quite impossible. Available policies are: <ul style="list-style-type: none"> <li>➤ <b>NONE</b> (No Fallback or Source Address Cycling) [default setting] Selecting this option deactivates the fallback feature</li> <li>➤ <b>Fallback</b> (Fallback to alternative Source Addresses) Causes use of the alternative IP addresses/interfaces specified below.</li> <li>➤ <b>SEQ</b> (Sequentially Cycle Source Addresses) Causes cycling of the IP addresses/interfaces specified below.</li> <li>➤ <b>RAND</b> (Randomise Source Addresses) Causes randomised usage of the IP addresses/interfaces specified below.</li> </ul> Configuration examples related to <b>multipath routing</b> are described below in more detail (see 2.2.6.2 netfence Multipath Routing, page 147).
<b>Alternative/Type</b>	Here up to three Alternative IP addresses or interfaces can be configured for use with the selected policy. <b>Note:</b> Usage of alternative interfaces is recommended when no permanently assigned IP address exists on an interface.
<b>Weight</b>	Assigns a weight number to the IP address or interface. Lower numbers mean higher priority.

List 4-33 Firewall configuration - Service Objects - General settings - section VPN Traffic Intelligence (TI) Settings

Parameter	Description
	Settings configured in this section only apply to Traffic Intelligence configuration in combination with TINA tunnel VPN technology. See 2.7.1.2 Traffic Intelligence (TI) and List 5-45, page 224 for details.

List 4-34 Firewall configuration - Service Objects - General settings - section BOB Settings

Parameter	Description
<b>BOB Settings</b>	This setting specifies if traffic should be processed compressed or not and in which direction to utilise compression. To compress traffic, parameter <b>Enable FW Compression</b> has to be set to <b>Yes</b> (see page 128). <b>Note:</b> Firewall compression is only applicable between firewalls operating on netfence gateway. When activated, option <b>Enable FW Compression</b> (see page 128) <b>MUST</b> be set to <b>yes</b> on all systems participating in compressed traffic. <b>Attention:</b> Do not enable firewall compression on gateways situated at the rim of untrustworthy networks in order to avoid DoS attacks based on bulk sending of compressed data packets. An attacker might forward IPCOMP packet copies originating from the compressed session to the firewall, thus forcing it to load consuming decompression tasks. If compressed traffic is required at the perimeter, make use of compressed VPN traffic. Authentication mechanisms included in VPN technology prevent the DoS exploit stated above (VPN - 2.7.1.2 Traffic Intelligence (TI), page 223).

**List 4-34** Firewall configuration - Service Objects - General settings - section BOB Settings

Parameter	Description
<b>BOB Settings</b> (continuation)	<p><b>Note:</b> Traffic compression only applies in the span from firewall to firewall. The firewall automatically uncompresses the traffic before forwarding it to the actual destination.</p> <p>Settings will be interpreted in the following way:</p> <ul style="list-style-type: none"> <li>➤ <b>No Compression</b> Traffic is always forwarded uncompressed (default).</li> <li>➤ <b>Compression in FORWARD Direction</b> Traffic is compressed in direction from <b>source</b> to <b>destination</b> address.</li> <li>➤ <b>Compression in REVERSE Direction</b> Traffic is compressed in direction from <b>destination</b> to <b>source</b> address. This compression mode thus only applies to traffic returned as response to a connection request.</li> </ul> <p><b>Attention:</b> Be careful when creating rules using the "2-way" option as this will only work when the destination address is a firewall as well.</p> <p><b>Note:</b> Have a look at the example setups below to understand the mode of action of compression configuration.</p>

**Effect of Firewall Compression Directions**

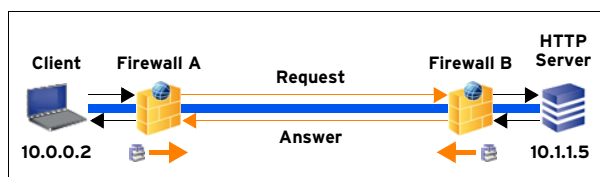
➤ **Example Setup 1**

A LAN client and an intranet web server constantly interchange huge amounts of data. The wanted setup therefore aims at bidirectional compressed traffic between these two endpoints (figure 4-21). It can hereby generally be assumed, that the connection is always initiated by the client. Two rules have to be introduced to achieve the wanted result:

**Table 4-5** Example Setup 1 - Rule configuration firewalls A and B

Rule configuration	Firewall A	Firewall B
<b>Action</b>	Pass	Pass
<b>Source</b>	10.0.0.2	10.0.0.2
<b>Destination</b>	10.1.1.5	10.1.1.5
<b>Service</b>	HTTP+S	HTTP+S
<b>Connection</b>	Client	Client
<b>Compression</b>	Forward	Reverse

**Fig. 4-21** Standard Connections - Example Setup 1



**Description:**  
Client requesting a connection to a web server. Firewall A is configured to compress traffic in forward direction, firewall B is configured to compress traffic in reverse direction. Data transmitted between client to HTTP server will thus always be compressed.

➤ **Example Setup 2**

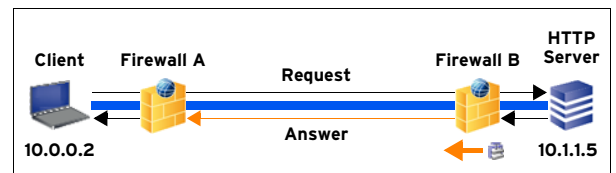
The following situation does not afford traffic compression from client to HTTP server but only vice versa, as the client rarely does anything else than requesting data. Compression is thus only needed in reverse direction.

The following rules have to be introduced to achieve the wanted result:

**Table 4-6** Example Setup 2 - Rule configuration firewalls A and B

Rule configuration	Firewall A	Firewall B
<b>Action</b>	Pass	Pass
<b>Source</b>	10.0.0.2	10.0.0.2
<b>Destination</b>	10.1.1.5	10.1.1.5
<b>Service</b>	HTTP+S	HTTP+S
<b>Connection</b>	Client	Client
<b>Compression</b>	none	Reverse

**Fig. 4-22** Standard Connections - Example Setup 2



**Description:**  
Client requesting a connection to a web server. Firewall A is configured without compression, firewall B is configured to compress traffic in reverse direction. Connection requests from client to web server will thus be uncompressed, returning traffic will be compressed.

**2.2.6.2 netfence Multipath Routing**

netfence 4.2 offers two possibilities to introduce Multipath Routing.

- Linux Standard Multipath routing
- ACPF Assisted Multipath routing

Additionally, the firewall rule set is extended to allow **Source Address Cycling**. This enables to configure rules where the source IP for different sessions is cycled.

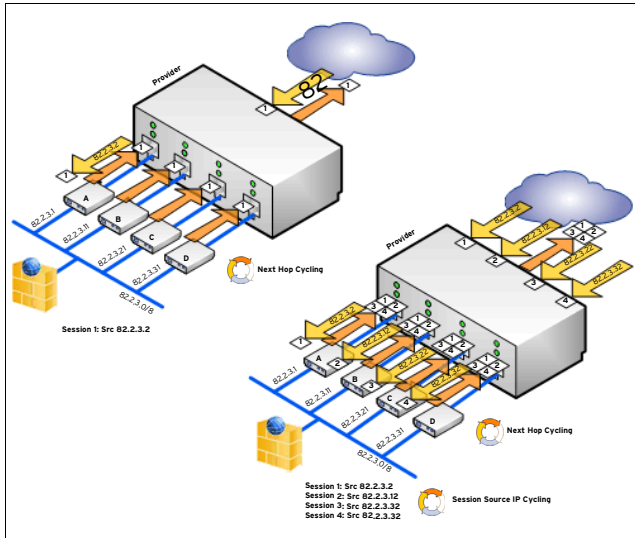
The capabilities of netfence multipath routing are noted below.

**Linux Standard Multipath - How Linux Standard Multipath routing is handled**

- Source IP Based balancing between Next Hops.  
Once the source destination combination is in the routing cache this combination will stay on the selected next hop IP
- No dead next hop detection
- No per session packet balancing

Simple redundancy by next hop detection could be provided by adding multiple routing entries with different route preference numbers.

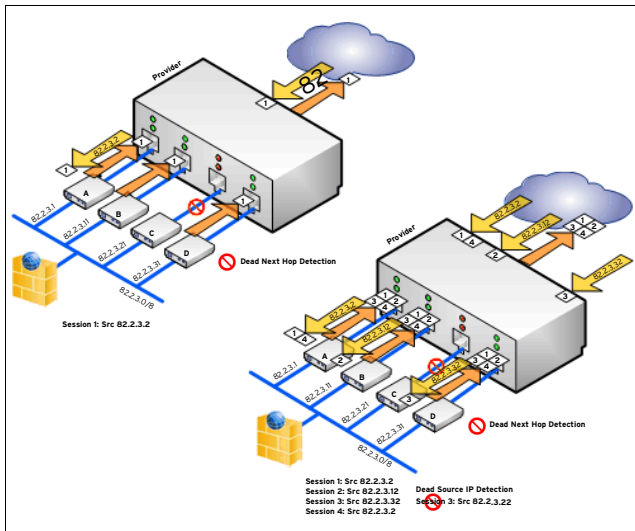
Fig. 4-23 Simple redundancy through next hop detection



**ACPF Assisted Multipath - How ACPF Assisted Multipath routing is handled**

- Per packet balancing between Next Hops
- Dead Next Hop Detection (Missing ARP reply)
- Associated source for each next hop for dead source address detection

Fig. 4-24 Handling of assisted multipath routing



**Source Address Cycling**

For cycling through the individual source IPs Connection Objects in the Firewall Rule Set are extended by the following entries.

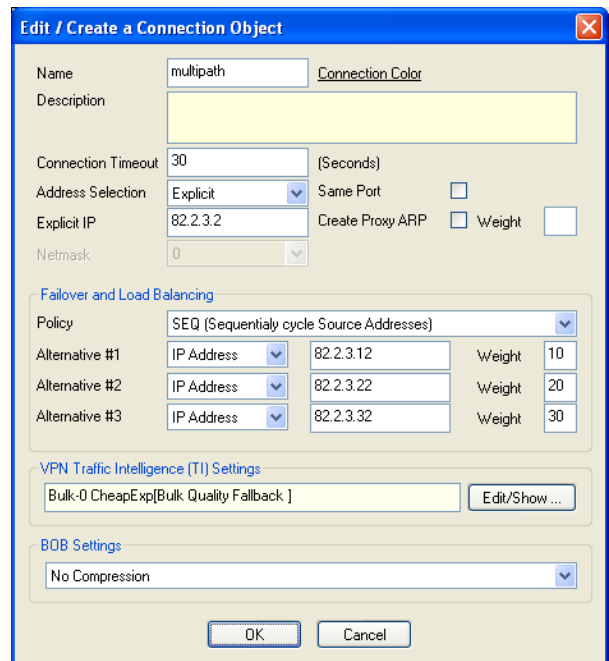
**Source Address Fallback and Cycling - Policy**

- NONE  
No fallback or source address cycling
- FALLBACK  
Fallback to alternative source addresses
- SEQ - Sequentially cycle source addresses  
for example,  
first session - Explicit IP,  
second session - Alternative #1;  
third session - Alternative #2;  
fourth session -Alternative #3  
fifth session - Explicit IP, ...
- RAND  
Randomise source addresses

**Examples:**

- **Source Address Cycling**  
To create a new Connection Object change to the **Connections** tab and add a new standard connection object by clicking the **New Standard** button. Select **Explicit IP Address** and add the first IP. Alternative IP Addresses are specified in the section **Source Address Fallback and Cycling**.

Fig. 4-25 Configuration example for Source Address Cycling



➤ **Linux Standard Multipath routing**

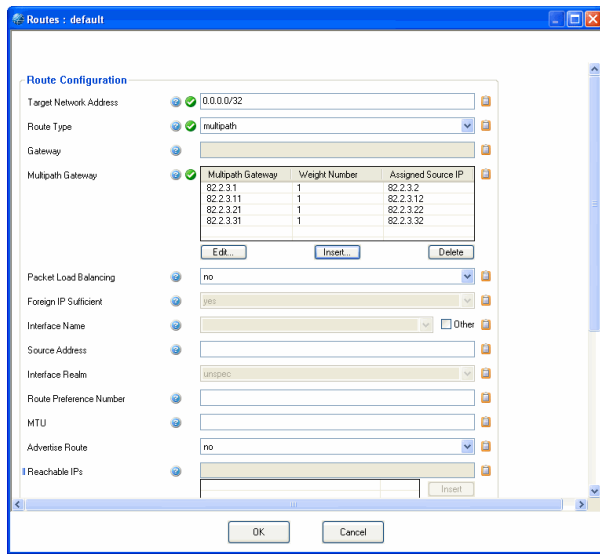
Add a default route in **Box - Network - Routing**. Change Route Type to **multipath**. Add multipath gateways by clicking **Insert** and provide the following Information

- Multipath Gateway - next hop IP address of the multipath route
- Weight Number - weight number of path (valid range from 0 - 10)



➤ Assigned Source IP

**Fig. 4-26** Configuration example for multipath routing (Packet Load Balancing is set to 'No')



Together with the described source address cycling the configuration shown above performs session based load balancing by

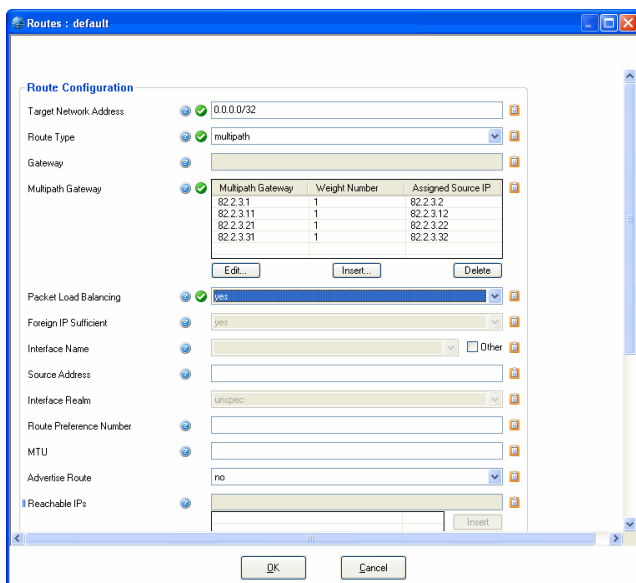
- Sequentially cycling the source addresses for each session
- Linux standard multipath routing does a routing lookup for the first session (Source IP 82.2.3.2) and keeps the next hop IP 82.2.3.1 in its routing cache. So all packets of the first session are routed via 82.2.3.1. The next session gets the source IP 82.2.3.12 assigned and thus is routed via 82.2.3.11.

➤ **ACPF Assisted Multipath routing**

Add a default route in **Box - Network - Routing**. Change Route Type to **multipath**. Add multipath gateways by clicking **Insert** and provide the following Information

- Multipath Gateway - next hop IP address of the multipath route
- Weight Number - weight number of path
- Assigned Source IP

**Fig. 4-27** Configuration example for ACPF Assisted Multipath routing (Packet Load Balancing is set to 'Yes')



Together with the described source address cycling the configuration shown above performs packed based load balancing by

- a) Sequentially cycling the source addresses for each session so that the first session gets the source IP 82.2.3.2 assigned, etc
- b) ACPF Assisted Multipath routing perform packet based load balancing for each session, so that the first datagram of session one is routed via 82.2.3.1, the second datagram of session one is routed via 82.2.3.11 and so on.
- c) The first packet of session two is routed via 82.2.3.1, the second packet via 82.2.3.11 and so on.
- d) Furthermore ACPF Assisted Multipath routing performs dead Next Hop Detection by detecting missing ARP replies from the next hop IP address.

If for example the next hop with the IP address 82.2.3.21 does not respond to ARP requests anymore further datagrams are cycled through the next hops 82.2.3.1, 82.2.3.11 and 82.2.3.31. The Source Address 82.2.3.22 is not used anymore for new session requests.

**2.2.6.3 Translation Map**

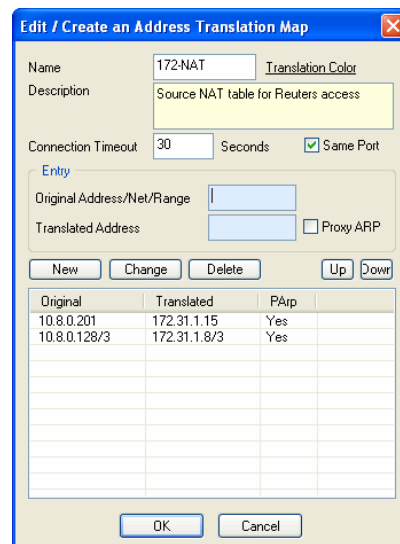
Translation maps define rewriting of source and/or destination addresses of IP packets as they pass the firewall. Source address translation (**source NAT**) involves rewriting of the source address originating from the *natted* network. The reverse operation applies to returning reply packets. Destination address translation (**destination NAT**) involves rewriting of the destination address of packets destined to the *natted* network.

You may define multiple source NAT conditions in one connection object if this does not conflict with the object's utilisation in multiple rules.

**Attention:**  
Pay attention to the succession of data sets in the translation map object. The first matching entry will be used when a rule is processed.

To create a new translation map, click **New Translation Map ...** in the **Edit Connections** navigation bar.

**Fig. 4-28** Address Translation Map configuration



The object created in figure 4-28 defines source NAT translation of the IP address 10.8.0.201 to 172.31.1.15 and of IP address 10.8.0.28 (from a 3-Bit network sub-class) to the address 172.31.1.8 (from a 3-Bit network sub-class).

As soon as this translation map is interpreted as destination NAT map it will be read in reverse order, thus a request to the IP address 172.31.1.15 will be redirected to the real destination address 10.8.0.201.

## 2.2.7 User Groups

This tab is used in conjunction with Firewall Authentication. For a detailed description, please have a look at 10.1.2.1 Firewall - User Window, page 189.

## 2.2.8 Interface Groups

Processing of a rule does not necessarily have to be invariantly associated with the physical network environment on a box, which is configured on box level. On machines equipped with multiple network interfaces, usage of a specific interface may be explicitly defined when a rule comes into action.

For each rule an interface may be assigned to origin and destination of the connection request. The **Source Interface** specifies the interface, the source address is allowed to use. The **Reverse Interface** specifies the interface, which the destination address is allowed to use. Latter is only available for passing and mapping actions with selected checkbox **2-Way**.

The following predefined network interface objects are available for selection:

### ➤ **Any**

With this setting the first interface matching the request is utilised for the connection in accordance with routing configuration. The packet source is not verified. Reply packets might be forwarded through another interface, if multiple interfaces capable of doing so are available. Not to check the physical source of packets might sometimes be needed in very special configurations with combinations of screened host and multi-homed topologies.

#### **Attention:**

For security reasons do not use this setting without explicit need.

### ➤ **Matching** (default)

This setting ensures that arriving packets are processed through the same interface, which will forward the corresponding reply packets. Source and destination addresses are thus only reversed. This method aims at preventing a network attack, in which an attacker might try using internal addresses from outside the internal network (IP spoofing).

#### **Note:**

With eventing activated (parameter **IP Spoofing** set to **yes**, see page 130), IP spoofing identification will trigger the events **FW IP Spoofing Attempt Detected** [4014] and **FW Potential IP Spoofing Attempt** [4015].

### ➤ **RAM, ADSL, DHCP, ISDN, SERIAL, UMTS**

Explicitly restricts rule processing to the specified dynamic network interface (if installed and configured).

### ➤ **Continue on Mismatch** checkbox

Select this checkbox, if you want rule processing to continue even if no matching interface can be found. The next rule in succession will then be "tried".

### ➤ **Disable Interface Check** checkbox

Select this checkbox, if you want to disable interface check (only available for rules applying both ways).

#### **Attention:**

Checkbox **Disable Interface Check** affects both sections, source **AND** reverse, and disables the settings of parameter **Send TCP RST for OOS Pkts.** (see 2.1.1.4 Operational).

## 2.2.9 Proxy ARPs

The Address Resolution Protocol (ARP) is primarily used to map IP addresses to MAC addresses. ARP takes an IP address as input, and by propagating this address it tries to retrieve the MAC address of the interface featuring it. ARP requests are broadcasted and can only be understood by hosts placed within the same subnet class.

Proxy ARP is a technique utilising the nature of the Address Resolution Protocol in order to connect two physically separated networks. The netfence gateway may be configured to answer ARP requests on behalf of the requested interface itself, accept packets and thus overtake responsibility for forwarding them to the actual destination correctly. This configuration is done via Proxy ARP objects. Proxy ARPs can thus be regarded as additional IP addresses the firewall responds to when it receives an ARP request.

Proxy ARP addresses may be utilised for redirecting and mapping in firewall rule sets, if they are in the same address space as

the source of a connection request. Additionally, Proxy ARP objects are utilised in bridging setups (9. Bridging, page 180).

#### **Note:**

You may define up to 256 Proxy ARP entries per box. This limitation exists for the numbers of entries, not for the number of IP addresses.

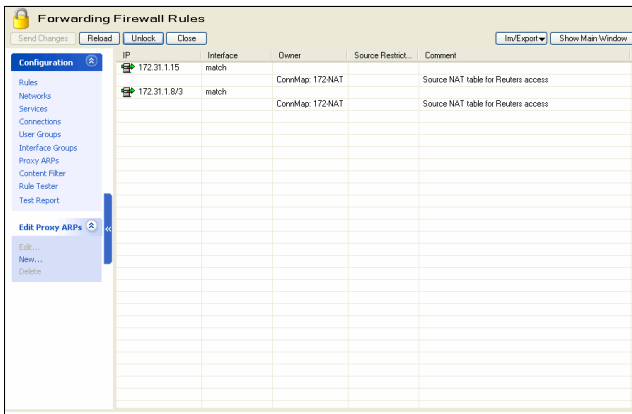
#### **Note:**

It is not recommended to create Proxy ARPs in address spaces, in which the firewall IP is configured as gateway IP.

**Table 4-7** Recommendation for creation of Proxy ARPs

Localnet	Firewall IP	Default Gateway IP	Redirected IP	Create Proxy ARP
10.0.0/8	10.0.0.100	none	10.0.0.10	yes
10.0.0/8	10.0.0.100	10.0.0.100	10.0.1.10	no

Fig. 4-29 Proxy ARPs tab of the firewall configuration window



In most cases proxy ARPs will be created, when the checkbox **Proxy ARP/Create Proxy ARP** has been selected next to a specific configuration parameter's properties in other configuration areas (rule configuration window, connection object dialogue, ...). These proxy ARPs may not exist without concurrent existence of the objects they have been created for, and will be deleted, as soon as the object referring to them is deleted.

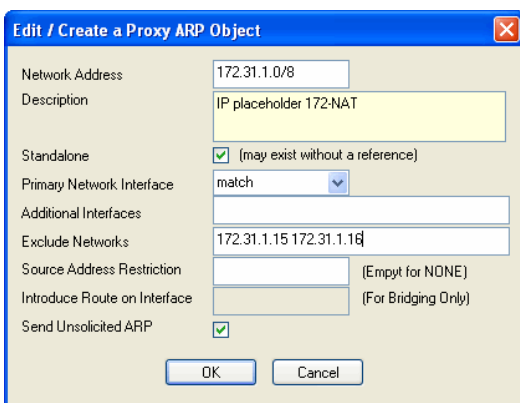
**Attention:**

If you are additionally using referenced proxy ARPs for another purpose than the one they have been created for, select the **Standalone** checkbox in the Proxy ARP object window. The proxy ARP object will then remain functional, even if the originally referring object is deleted.

Nonetheless, you might sometimes want to create proxy ARPs that are not dependent on rules or NAT tables, for example for "filling up" a net to prevent someone else from taking a local address. In this case make use of the Proxy ARPs window.

A proxy ARP takes the following configuration values:

Fig. 4-30 Create a Proxy ARP Object dialogue



List 4-35 Proxy ARP object configuration values

Parameter	Description
<b>Network Address</b> field	This field either takes a single IP address or specification of a complete network.
<b>Description</b> field	Enter a significant description of the proxy ARP object in this place.
<b>Standalone</b> checkbox	This checkbox always has to be selected when a proxy ARP object is created without a referring object (selected by default). The proxy ARP object will be deleted when the checkbox is unselected.

List 4-35 Proxy ARP object configuration values

Parameter	Description
<b>Primary Network Interface</b> pull-down menu	This field specifies the interface, which is going to be utilised when responding to an ARP request. The following predefined choice is available: <ul style="list-style-type: none"> <li>➤ <b>match</b> (default) ARP requests will be answered via the interface that hosts the network.</li> <li>➤ <b>any</b> ARP requests will be answered via any interface.</li> <li>➤ <b>noext</b> If an ARP request arrives from an external interface, it will not be answered.</li> <li>➤ Alternatively, a specific network interface may be entered into the field (for example eth1).</li> </ul>
<b>Additional Interfaces</b> field	Through this field additional interfaces may be specified, which should respond to ARP requests. Be careful only to specify interfaces, which cannot conflict with the primary network interface. Separate multiple entries with space.
<b>Exclude Networks</b> field	If a complete network has been specified in the <b>Network Address</b> field (see above), specific network addresses may now be excluded from proxy ARP creation. Separate multiple entries with space.
<b>Source Address Restriction</b> field	This field limits responding to an ARP request to the network addresses entered in this place. Separate multiple entries with space.
<b>Introduce Route on Interface</b> read-only field	This value is dependant on bridging configuration and only filled (read only) if a bridging interface route is created (9. Bridging, page 180).
<b>Send Unsolicited ARP</b> checkbox	Activating this checkbox causes that the firewall does not only answer ARP requests but also propagates the specified IP addresses through ARPs unsolicitedly (checkbox selected by default).  <b>Note:</b> Unsolicited ARPs can only be sent if the corresponding network interface has an active IP address. The evaluation of the interface's IP address happens only on startup of the forwarding firewall, in case of a HA takeover or when the firewall rule set changes. No automatic evaluation is performed if the network interface changes into state "up" or if a pending route becomes active (example: in case of a newly introduced server-IP). In this case only the ProxyARP is introduced to answer incoming ARP requests.

## 2.2.10 Rule Tester & Test Report

Due to their complexity, these two windows are described in a separate chapter (see 4. Testing and Verifying of Rule Sets, page 163).

## 2.3 Advanced Options for Firewall Rules

### 2.3.1 Content Filter (Intrusion Prevention)

The content filter is used for blocking Internet worms and exploit attacks. A set of predefined filters, which can be referenced by the firewall rule set, is provided with the phion netfence. The possibility of defining custom filters enables the administrator to react to new threats.

The phion content filter can detect network based attacks, and protects the network by terminating the offending IP connection.

All type of network connections (for example SMTP) that are defined in the referenced service object are checked for the configured patterns of the content filter to detect attacks.



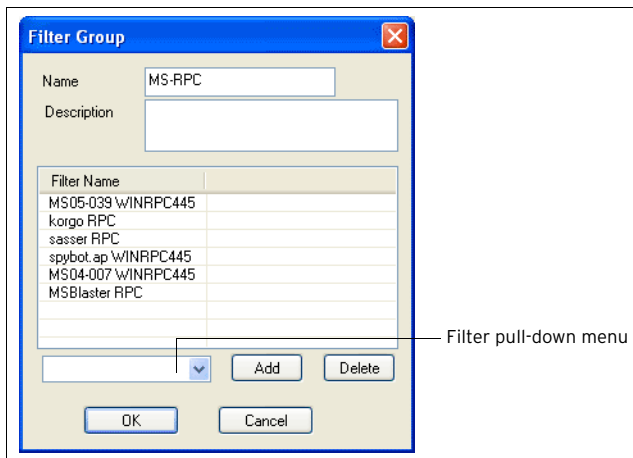
### 2.3.1.2 Creating/Editing Filter Groups

To open the configuration dialogue for filters, click **New ...** in the **Edit Filter Group** navigation bar. The configuration dialogue consists of a field **Name** used for entering the name of the filter. The field **Description** can be used for any additional information concerning/describing the filter group.

The list **Filter name** displays all filters that are part of this filter group. These filters are implemented by selecting them from the filter pull-down menu and clicking **Add**.

To delete an entry, select it from the list and click the **Delete** button.

Fig. 4-34 Creating/Editing Filter Groups



### 2.3.1.3 Referencing within the Corresponding Rules

Enter the **Rule** configuration dialogue, click **Content/IPS** in the **Views** navigation bar and choose the desired filter from the **Content Filter** pull-down menu.

## 2.3.2 Peer-to-Peer Detection

netfence gateway 3.6.2 and later provide additional layer-7 deep packet inspection technology to detect and control applications such as Instant Messaging, peer-to-peer based file sharing, and Skype. The above mentioned applications usually cannot be detected by pattern based intrusion prevention mechanisms. All these applications have in common that they use peer-to-peer (**P2P**) mechanisms instead of a client-server architecture. Thus, we will refer to this kind of software as peer-to-peer clients, even if their primary purpose is Instant Messaging (IM) or Voice-over-IP (Skype).

P2P-software uses multiple technologies like port hopping and protocol obfuscation to circumvent firewalls and proxy servers. Skype and up-to-date BitTorrent or eDonkey clients already make use of encryption; further protocols will switch to encrypted communication in the near future.

Pattern based detection mechanisms will fail due to the above mentioned reasons. Instead, netfence provides sophisticated behavioural analysis to detect and manipulate traffic generated by these applications. For

example, multiple criteria like packet length, packet timing, flow behaviour, and bit patterns are taken into account to determine if a connection is likely to origin from an IM or Skype client.

The current netfence version supports three traffic handling modes regarding P2P forwarding traffic. Traffic can be reported only, blocked, or throttled. The upcoming netfence release will allow more granulated rules for individual categories or applications.

**Note:**

Behaviour based analysis does not give full protection against P2P applications.

The reason for this is that behavioural analysis requires initial packets to pass through the firewall (of course only if the packets are allowed by all other criteria of a firewall rule) and that only as soon as the P2P module has enough information to classify a flow as P2P traffic, the configured netfence action can take place.

Beyond this, the P2P module can only detect behaviour of known applications. Newer versions of a specific protocol or a completely new protocol can only be detected as soon as their behaviour is known and detection mechanisms are implemented. phion will notify their customers if a new P2P module is available (usually in form of patch or release notes).

**Note:**

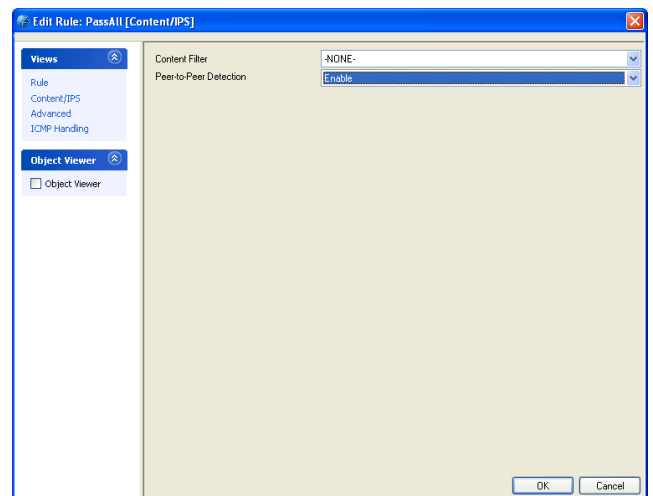
netfence P2P detection requires purchase of an additional license. Please contact your phion sales representative for detailed information.

**Note:**

P2P-detection can only be used in the forwarding firewall rule set and is assigned per firewall rule.

It has to be enabled globally through parameters in the **Firewall Settings** (see 2.1.1.1 Peer-to-Peer Detection, page 126) and a global policy applies whenever P2P traffic is detected.

Fig. 4-35 Assigning P2P-detection



To assign P2P-detection to a firewall rule, click **Content/IPS** in the Rule window and set option **Peer-to-Peer** Detection to **Enable**.



### 2.3.3 Advanced Rule Parameters

Usually, a connection request matches a rule as soon as source, service, and destination match. Situations exist in which you might want to ascertain that no rule allows bypassing a configured rule set.

Example: Two machines in your LAN have access to a database server on a critical port (for example, telnet). You want to make sure that no other rule accidentally allows access for another source than the configured two clients. In this case, select **Block on (Source) Mismatch** in the **Rule Mismatch Policy** section of the Advanced Rule Parameters window.

Clicking **Advanced** in the navigation bar of the rule window opens the following dialogue:


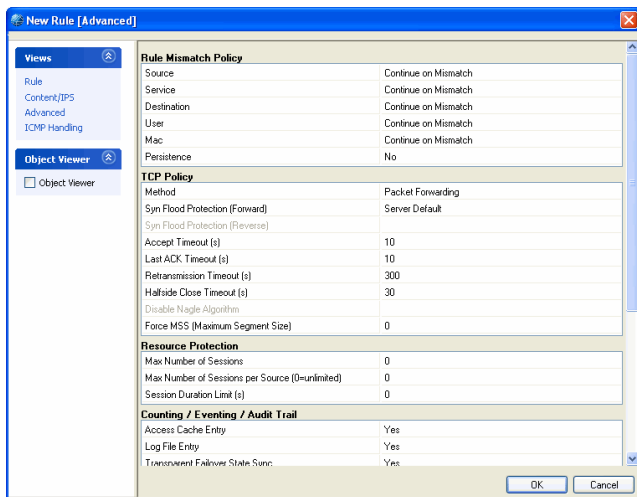
**Note:**  
The following icon  is displayed in the rule view of the rule configuration window as soon as the default data has been modified. Changed values are highlighted in yellow.


Fig. 4-36 Advanced Rule Parameters



List 4-37 Firewall configuration - Advanced Rule Parameters - section Rule Mismatch Policy

Parameter	Description
<b>Source / Service / Destination / User / Mac</b>	Defines the behaviour on mismatch. The following options are available: ➤ <b>CONTINUE on Mismatch</b> - processes the subsequent rule ➤ <b>BLOCK on Mismatch</b> - see 2.2.3.3 Action Section, page 136 ➤ <b>DENY on Mismatch</b> - see 2.2.3.3 Action Section, page 136 <b>Attention:</b> The effect of these options is cumulative. If you check two options you blank out the remaining values for all subsequent rules. If you check all three options, this rule is the effective end of your rule set.
<b>Persistence</b>	If set to <b>yes</b> , the session is not reevaluated when rule set or authentication settings change (default: <b>No</b> ).

List 4-38 Firewall configuration - Advanced Rule Parameters - section TCP Policy

Parameter	Description
<b>Method</b>	<p><b>Packet Forwarding</b> (Application Controlled Packet Forwarding) The firewall engine is capable of two TCP forwarding methods. If you want to avoid any direct TCP connection between two TCP-partners transverseing the firewall you will use stream forwarding which actually builds two distinct TCP connections and hence the destination will not get any packet which is not generated by the firewall TCP stack itself. Since the ACPF engine filters any malformed packet too, the security advantage of stream forwarding is not that important as it was years ago when the filtering engines were not that powerful.</p> <p><b>Stream Forwarding</b> (Transparent Application Proxying; yellow background) With <b>Stream Forwarding</b> the performance of the firewall is significantly reduced (400-500 MBit maximum). For detailed performance data contact phion support.</p> <p><b>Note:</b> The icon  is added to the Action column of the rule set overview window, if Stream Forwarding is configured as data transfer Method</p>
<b>Syn Flood Protection (Forward)</b>	<p><b>Note:</b> For a description of access policy handling see 2.3.3.3 Accept Policies.</p> <p><b>Server Default</b> The value configured in 2.1.1.4 Operational, page 128 is used as default.</p> <p><b>Outbound</b> The firewall immediately tries to establish a connection to the requested destination. If successful, it then establishes the connection between itself and the client.</p> <p><b>Inbound</b> The firewall first tries to establish a connection to the requesting source and then establishes the connection between itself and the requested destination.</p>
<b>Syn Flood Protection (Reverse)</b>	<p>Only activated if option "<b>2-way</b>" has been chosen in section <b>Action</b>.</p> <p><b>Note:</b> For a description of access policy handling see 2.3.3.3 Accept Policies.</p> <p><b>Outbound</b> Same as above. Policy applies for the reverse connection direction.</p> <p><b>Inbound</b> Same as above. Policy applies for the reverse connection direction.</p>
<b>Accept Timeout (s)</b>	Time the firewall waits until the destination has to answer. After this timeout the firewall sends a TCP RST packet to both partners (default: <b>10</b> ).
<b>Last ACK Timeout (s)</b>	Time the firewall waits after an ACK until the connection is terminated (default: <b>10</b> ).
<b>Retransmission Timeout (s)</b>	Time the firewall waits until the source has to retransmit packets before the firewall registers this as a hijacking attempt (default: <b>300</b> ).
<b>Halfside Close Timeout (s)</b>	Time the firewall waits after conscious termination of the connection until the socket is closed (default: <b>30</b> ).
<b>Disable Nagle Algorithm (No Delayed ACK)</b>	This parameter enables/disables the Nagle Algorithm. This option is only available when using Stream Forwarding.
<b>Force MSS (Maximum Segment Size)</b>	When setting a MSS TCP in a rule the SYN and SYN-ACK TCP packets are checked for a MSS larger than the configured one. If the MSS TCP attribute is smaller, the packet is rewritten with the configured MSS. Use the feature for VPN to force a TCP MSS that fits the MTU of the VPN tunnel device.

**List 4-39** Firewall configuration - Advanced Rule Parameters - section Resource Protection

Parameter	Description
<b>Max. Number of Sessions</b>	Maximum accepted concurrent connections for this rule on a global basis. <b>Note:</b> With eventing activated (parameter <b>Rule Limit Exceeded</b> (see page 129), the event <b>FW Rule Connection Limit Exceeded</b> [4016] is generated when the limit is exceeded.
<b>Max. Number of Sessions per Source</b>	Maximum accepted concurrent connections for this rule on a per source address basis (default: 0 = unlimited). <b>Attention:</b> Choosing these values too small can have unexpected effects. Use this parameters only if you are a preferred victim of Denial of Service (DoS) attacks. <b>Note:</b> With eventing activated (parameter <b>Source/Rule Limit Exceeded</b> (see page 129), the event <b>FW Rule Connection per Source Limit Exceeded</b> [4018] is generated when the limit is exceeded.
<b>Session Duration Limit (s)</b>	Allows setting a maximum keep alive time for an established session. The value 0 means unlimited, that means the session never dies. <b>Note:</b> This parameter is only executable in the forwarding firewall. Setting this parameter in the local firewall takes no effect.

**List 4-40** Firewall configuration - Advanced Rule Parameters - section Counting / Eventing / Audit Trail

Parameter	Description
	Defines whether such events should be logged, written to the access cache, ...
<b>Access Cache Entry</b>	Set to <b>yes</b> (default) to obtain access cache entries.
<b>Log File Entry</b>	Set to <b>yes</b> (default) to obtain log file entries.
<b>Transparent Fallover State Sync</b>	Setting to <b>yes</b> (default) causes that a session that is controlled by this rule is synchronised on a HA system ( <b>High Availability</b> , page 375).
<b>Statistics Entry</b>	Set to <b>yes</b> (default) to obtain statistics files. <b>Note:</b> Set to <b>no</b> causes that also no global firewall statistics will be generated.
<b>Log Session State Change</b>	Set to <b>yes</b> (default: <b>no</b> ) to log changes of session states.
<b>Own Log File</b>	If set to <b>yes</b> (default: <b>no</b> ) All log events belonging to this rule are logged into an extra log file.
<b>Service Statistics</b>	Set to <b>yes</b> (default: <b>no</b> ) to generate service statistics for this rule.
<b>Eventing</b>	Specify a severity level for generation of event log entries every time a request matches the rule. Possible settings generating the corresponding events are: <ul style="list-style-type: none"> <li>➤ <b>None</b> (default) - no event generation</li> <li>➤ <b>Normal - FW Rule Notice</b> [4020]</li> <li>➤ <b>Notice - FW Rule Warning</b> [4021]</li> <li>➤ <b>Alert - FW Rule Alert</b> [4022]</li> </ul> <p>Within the event settings (<b>Eventing - 2</b>. Event Configuration, page 306) each of these events can be assigned with different actions. <b>Note:</b> Local rules are not affected by the rules advanced 'eventing' setting. The behaviour is fixed to "none".</p>

**List 4-41** Firewall configuration - Advanced Rule Parameters - section Miscellaneous

Parameter	Description
<b>Authentication</b>	Via this menu the required user authentication for HTTP and HTTPS connections (Inline Authentication) can be defined (see 10. Firewall Authentication, page 188). The following options are available: <ul style="list-style-type: none"> <li>➤ <b>No Inline Authentication</b> (default)</li> <li>➤ <b>Login+Password Authentication</b></li> <li>➤ <b>X509 Certificate Authentication</b></li> <li>➤ <b>X509 Certificate &amp; Login+Password Authentication</b></li> </ul>

**List 4-41** Firewall configuration - Advanced Rule Parameters - section Miscellaneous

Parameter	Description
<b>Policy</b>	<b>Default Policy</b> This option is the default one and takes the interface realm settings into consideration that are assigned in the network configuration for the local networks and interface routes ( <b>Configuration Service - 2.2.5.5 Network Routes</b> , page 68, <b>Interface Realm</b> , page 69). Depending on the specified realm, the Source or Destination IP counts. <b>Count Source IP</b> <b>Count Destination IP</b> These two parameters allow you to specify explicitly what type of IP address is counted ( <b>Licensing - 6.2 Policy No. 2: Rule Explicit</b> , page 509).
<b>Time Restriction</b>	<b>Note:</b> Use this parameter to apply a time restriction to rules configured with a feature level lower or equal 3.2 (see Setup, page 135). For a description of the time restriction dialogue see 2.3.3.2 Time Restriction below.
<b>Clear DF Bit</b>	The DF ( <b>Don't Fragment</b> ) bit is a bit within an IP header that determines whether a packet may be fragmented or not (0 = fragmentation allowed, 1 = do not fragment). In networks where packet size is limited to a Maximum Transmission Unit (MTU), packet fragmentation may become vital when packets sent to this network exceed the MTU (for example, as may frequently occur with SAP applications). This parameter determines if the original DF bit setting in an IP header may be overridden. When set to <b>no</b> (default) the packet's specification is observed. Normally, the sending clients determine if fragmentation is required. When the DF bit is set and the target network's MTU specification requires fragmentation, the firewall responds with an ICMP Destination Unreachable message (Code 4: Packet too large. Fragmentation required but DF bit in the IP header is set). As the firewall may not override the DF bit setting, fragmentation is up to the client. If the client for any reasons does not understand the answer code, data transmission will fail and data loss might occur in network transports where packet sizes exceed the MTU of the network.
<b>Clear DF Bit (continuation)</b>	When set to <b>yes</b> , the DF bit will be cleared from the IP header and packets will be fragmented if necessary regardless of the setting in the packet's IP header. Note that fragmentation and packet reassembling process might lead to significant performance loss at high traffic rates. <b>Note:</b> Appropriate handling of this parameter is essential in conjunction with VPN tunnels, as encapsulating packets reduces the available MTU size. The DF bit is automatically cleared from traffic, which is forwarded towards a VPN interface. <b>Note:</b> It is recommended only to change the default setting when experiencing transport problems clearly associated with packet size restrictions.
<b>Set TOS Value</b>	In networks the <b>Type of Service (ToS)</b> information may be utilised to define the handling of the datagram during transport. The <b>TOS Value</b> thus specifies how to deal with the ToS information in packets' IP headers for all traffic forwarded by the particular rule. By default the value is set to 0 ( <b>TOS unchanged</b> ). Another fixed size may be specified instead even if originally the ToS flag has not been set.
<b>Prefer Routing over Bridging</b>	This parameter controls routing behaviour of bridges that are configured as Routed Transparent Layer2 Bridges (see), and thus act as routers and bridges at the same time. When set to yes (default: no), traffic is routed that by configuration would actually traverse the bridges, which are available on a netfence gateway directly. Use this setting in scenarios, where an external router connects bridges that are configured on a netfence gateway, and where it should be avoided that traffic is directed to the router. When directed to the external router first, traffic would attempt to pass the gateway twice and be rejected by the firewall. When activated, the routing functionality of the bridge itself is used.
<b>Color</b>	Allows defining a colour in which the rule is displayed in the rule set overview window.

**List 4-42** Firewall configuration - Advanced Rule Parameters - section Quarantine Policy

Parameter	Description
<b>LAN Rule Policy</b>	Matching Policy for a session to be evaluated destined or originated from a non Quarantine net. ➤ <b>Match.</b> The rule matches ➤ <b>Block.</b> The rule blocks the request ➤ <b>Deny.</b> The rule denies the request ➤ <b>Continue.</b> Rule evaluation continues with next rule in ruleset
<b>Quarantine Class 1 Rule Policy</b>	Matching Policy for a session to be evaluated destined or originated from a Quarantine class 1 net. ➤ <b>Match.</b> The rule matches ➤ <b>Block.</b> The rule blocks the request ➤ <b>Deny.</b> The rule denies the request ➤ <b>Continue.</b> Rule evaluation continues with next rule in ruleset
<b>Quarantine Class 2 Rule Policy</b>	Matching Policy for a session to be evaluated destined or originated from a Quarantine class 2 net. ➤ <b>Match.</b> The rule matches ➤ <b>Block.</b> The rule blocks the request ➤ <b>Deny.</b> The rule denies the request ➤ <b>Continue.</b> Rule evaluation continues with next rule in ruleset
<b>Quarantine Class 3 Rule Policy</b>	Matching Policy for a session to be evaluated destined or originated from a Quarantine class 3 net. ➤ <b>Match.</b> The rule matches ➤ <b>Block.</b> The rule blocks the request ➤ <b>Deny.</b> The rule denies the request ➤ <b>Continue.</b> Rule evaluation continues with next rule in ruleset

### 2.3.3.1 Multiple Rules Editing

When feature level 3.4.0, 3.6.0, 4.0.0 or 4.2.0 applies, it is possible to select multiple rules for editing. Select the rules you want to edit together and click **Edit ...** in the main navigation bar or **Edit Multiple Rules ...** in the right-click context menu to open the rules for modification.

**Note:**

The option **Edit Multiple Rules** is not available if the view is set to **Show in Sections** and a section is selected. Select "real" rules only.

The rule window opens displaying the advanced parameters view.

**Note:**

The register of available configuration parameters has been expanded compared to the the one in single rule editing mode (see list 4-37, page 154).

The following values have been added to the listing:

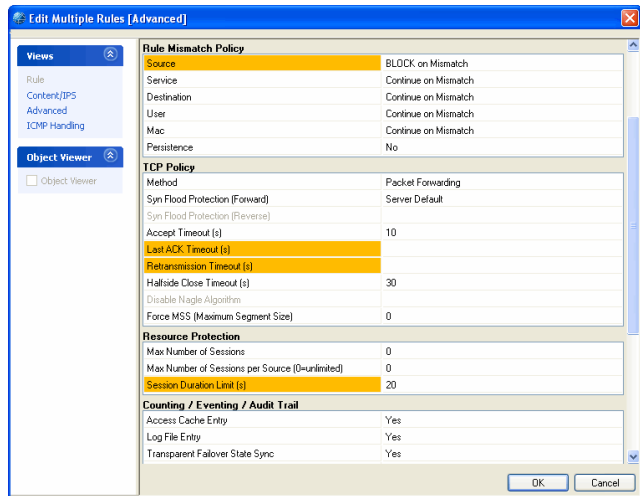
**List 4-43** Firewall configuration - Enhanced Advanced Rule Parameters - section Rule Settings

Parameter	Description
<b>Timed</b>	see 2.3.5 Dynamic Activation, page 159
<b>Inactive</b>	see inactive checkbox, page 136
<b>Time Object</b>	see 2.2.3.10 Time Objects, page 139
<b>Band</b>	see Forward Band, page 136
<b>Authenticated User</b>	see 2.2.3.8 Authenticated User Section, page 139

Again, modified default values are displayed highlighted in yellow when they have been changed uniformly. As soon as the parameter has been configured differently in each

particular rule, it is highlighted in red, leaving the field with the parameter value empty.

**Fig. 4-37** Advanced Rule Parameters - Multiple Rules Editing



**Attention:**  
Use this feature with great care. Editing of multiple rules without the necessary wariness can cause severe misconfiguration.

**Note:**  
Multiple rules editing as well applies to Content Filter and ICMP Handling characteristics. Rules cannot be edited together in the rule view, though.

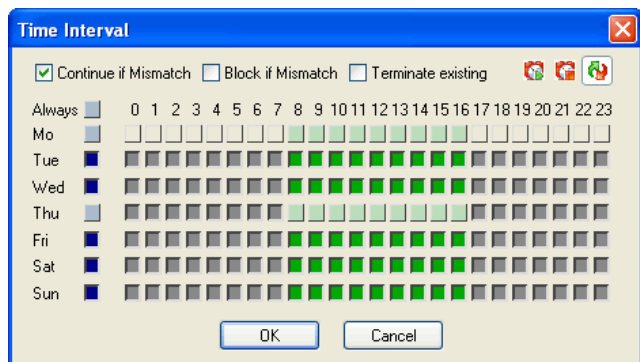
### 2.3.3.2 Time Restriction

Using the **Always** button in the Advanced rule parameters window, each rule configured within a feature level equal or lower than 3.2 (see Setup, page 135) can be equipped with a time restriction.

Clicking the button opens the **Time Interval** configuration window. If time restriction applies to a rule, the label of the button changes to **Restricted! ...**

The granularity of time restriction is 1 hour on a weekly base.

**Fig. 4-38** Time restriction dialogue



A rule is allowed at all times by default, which means all checkboxes in the **Time Interval** dialogue window are unchecked. Checking a box denies a rule for the given time. Figure 4-38 shows a time interval setting for a rule which

has been set to disallowed on Monday and on Thursday from 08:00 to 16:00.

**List 4-44** Firewall configuration - Time Restriction

Parameter	Description
<b>Continue if mismatch</b> (default)	Process rule set even if time restriction denies it.
<b>Block if mismatch</b>	Do not allow connection if time restriction denies it.
<b>Terminate existing</b>	If checked an active session is terminated as soon as time restriction applies.
Set allow	Select  to clear selected checkboxes.
Set deny	Select  to select checkboxes as disallowed time intervals.
Set Invert	Select  to configure allowed and disallowed time intervals simultaneously.

### 2.3.3.3 Accept Policies

The firewall offers a choice of two different accept policies on a per rule basis which are intended to offer varying levels of protection against TCP SYN flooding attacks. Only upon successful establishment the TCP session is governed directly by the two communicating network entities.

- **Outbound Accept Policy** - "Trusted clients accessing untrusted networks"  
TCP session requests (SYN packets) are immediately forwarded to the target address if the session is allowed by the rule set. The TCP handshake occurs between source and destination.
- **Inbound Accept Policy** - "Server protection against untrusted networks"  
TCP session requests (SYN packets) are NOT immediately forwarded to the target address even if the session is allowed by the rule set. The firewall rather establishes a complete TCP handshake with the requesting source first, assuring that the requestor is authentic (no IP spoofing) and really intends to establish a TCP session. Only after a complete TCP handshake is established, the handshake with the target is caught up and traffic will be forwarded to the target address.

**Note:**

The different accept policies only apply to the TCP family.

Additionally, as safeguard against DoS/DDoS attacks from the internet for instance, the netfence firewall allows configuration of two resource limits on a per rule basis to protect against resource exhaustion of the firewall gateway (**Max. Number of Sessions/Max. Number of Sessions per Source**).

The following options are configurable on a per rule basis in the Advanced parameter window of the rule configuration window:

**List 4-45** Firewall configuration - Accept Policy section - section Firewall configuration - Advanced Rule Parameters - section Resource Protection

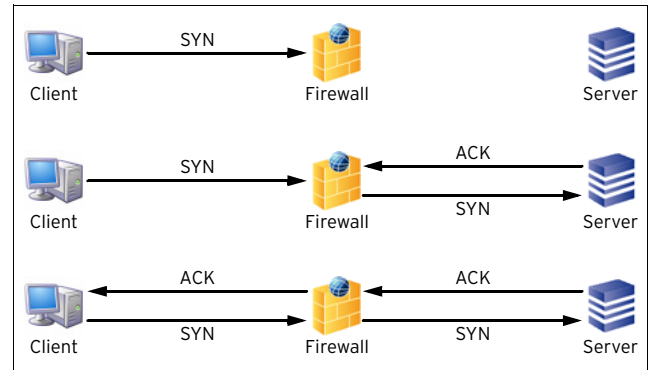
Parameter	Description
<b>Max. Number of Sessions</b>	see list 4-37, page 154
<b>Max. Number of Sessions per Source</b>	

**List 4-46** Firewall configuration - Accept Policy section - section Firewall configuration - Advanced Rule Parameters - section TCP Policy

Parameter	Description
<b>Syn Flood Protection (Forward)</b>	see list 4-37, page 154
<b>Syn Flood Protection (Reverse)</b>	

The scenario depicted in the figures below explains how SYN flooding and protection by the netfence firewall work:

**Fig. 4-39** Building up a connection with outbound accept policy.



The main characteristic of the **outbound policy** is that the client will only receive an ACK when the requested server is really up. This is important for many applications such as a browser when it tries to connect to a server with many IP addresses for the same hostname (DNS round robin). The browser tries to connect to the first IP it gets from the DNS server, and, if it is not successful, it tries the next one and so on. Hence, it would be fatal if the firewall sent an ACK to the client even if the server was not reachable because then the browser would never get the chance to try any further IP.

On the other hand this accept policy opens the door to a simple attack illustrated in figure 4-40.

**Step 1** The unfriendly host fakes its IP address and gives itself an address, which is already in use in another network. This way it never gets any answer.

**Step 2** It then sends innumerable SYN packets to the protected server.

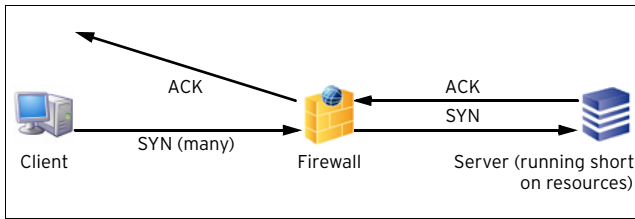
**Step 3** The firewall builds up a connection for every SYN, thus using up own and protected server's resources.

**Step 4** After a certain number of unanswered ACKs the firewall possibly recognises the unfriendly activity and no longer accepts SYNs from the source

**Note:**

If the unfriendly host is able to change its IP address fast enough it will be able to do this very often without a chance for the firewall to differentiate between the attack and ordinary requests.

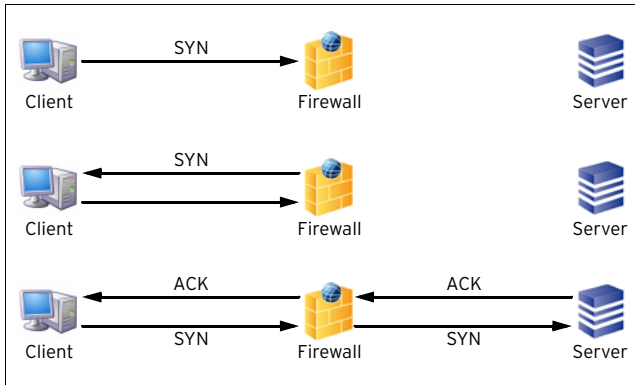
**Fig. 4-40** Simple SYN flooding attack with faked IP addresses on a firewall with outbound accept policy



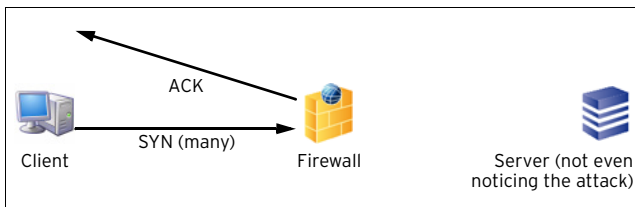
**Solution:**

To avoid exhausting a protected server with faked requests, the **Accept Policy** of the rule should be set to **Inbound**. This means the firewall first returns an ACK to the clients IP, thus verifying its real wish for a connection. Only if the ACK is confirmed, the firewall will build up a connection to the protected server.

**Fig. 4-41** Building up a connection with inbound accept policy



**Fig. 4-42** Simple SYN flooding attack with faked IP addresses on a firewall with inbound accept policy



**Note:**

A SYN request matching a rule with inbound policy is neither logged nor appears in real time status nor in the access cache until it is validated as a real request. That means that SYN flooding attacks do not affect resources of the firewall system. As soon as a SYN flooding attack is detected a cumulative log entry and the event **FW Potential IP Spoofing Attempt [4015]** are generated.

**2.3.4 ICMP Handling**

Click on **ICMP Handling** in the **Views** navigation bar to access this configuration section allowing you to define which IP address is used within ICMP (Internet Control Message Protocol) messages.

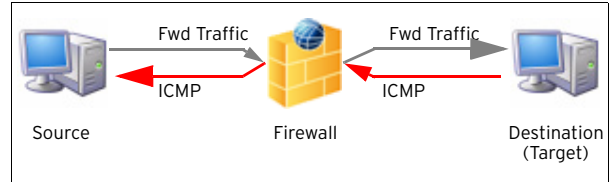
**2.3.4.1 Theory**

Let us have a look at the phion terminology:

➤ **Forward Policy**

The Forward Policy affects ICMP messages that are caused by traffic from Source to Destination.

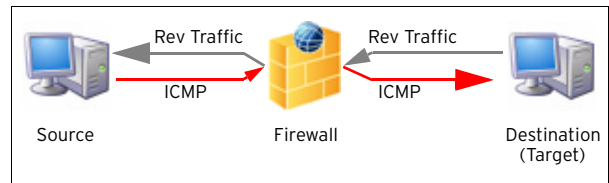
**Fig. 4-43** Forward Policy



➤ **Reverse Policy**

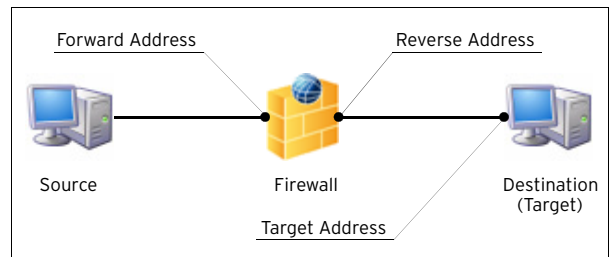
The Reverse Policy affects ICMP messages that are caused by traffic from Destination to Source.

**Fig. 4-44** Reverse Policy



➤ **Addresses (Forward / Reverse / Target)**

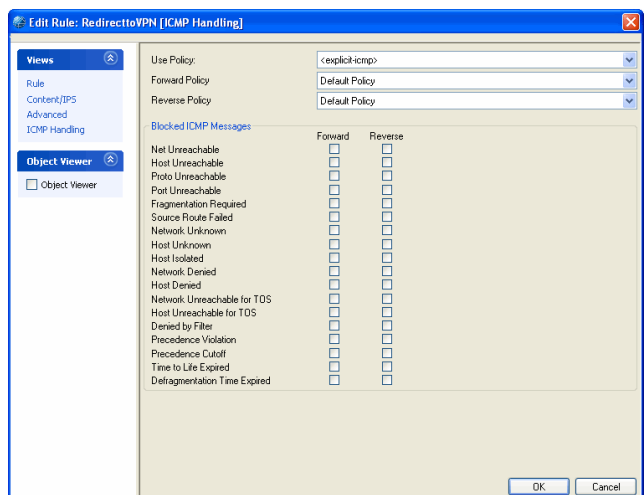
**Fig. 4-45** Forward / Reverse / Target Address



**2.3.4.2 Configuration**

ICMP handling policy is configurable per rule. The following options are available:

**Fig. 4-46** ICMP Handling parameters



**Forward Policy / Reverse Policy** menu



➤ **Default Policy**

The **Default Policy** decides automatically whether to use forward or target address:

- with NAT the forward address is used (no internal IP address is visible)
- without NAT the target address is used

**Note:**

This setting will fit in most cases.

➤ **NO ICMP AT ALL**

This setting causes that all ICMP messages are blocked by the firewall.

➤ **Use Forward Address**

This setting causes that the Forward Address is used for ICMP messages.

➤ **Use Reverse Address**

This setting causes that the Reverse Address is used for ICMP messages.

➤ **Use Target Address**

This setting causes that the Target Address is used for ICMP messages.

The section **BLOCKED ICMP Messages** offers configuration options additional to the selected policies. This means you may define whether certain ICMP messages are blocked in either forward, reverse, or forward & reverse direction.

**Note:**

To configure a policy template select **New ICMP Param Object** in the **ICMP** tab of the Object Viewer.

**2.3.4.3 Example**

In order to get a more practical way for understanding this topic, let us have a look at the following example:

Fig. 4-47 ICMP Handling - Example

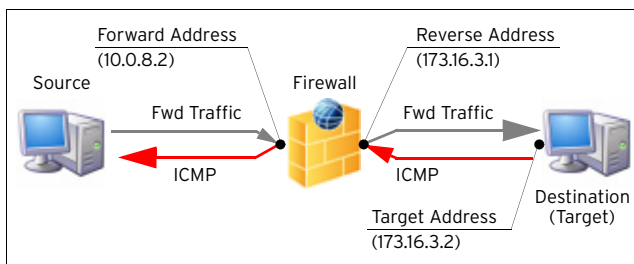


Table 4-8 Forward policy comparison

Fwd Policy set to	IP address used
Use Forward Address	10.0.8.2
Use Reverse Address	173.16.3.1
Use Target Address	173.16.3.2

**Note:**

Assuming that you use NAT for 173.16.3.2 via 10.0.8.3, selecting **Use Target Address** causes IP address 10.0.8.3 to be used instead of 173.16.3.2.

**2.3.5 Dynamic Activation**

By chance every rule may become a dynamic rule. Therefore, simply select the checkbox **Timed** in the rule configuration window.

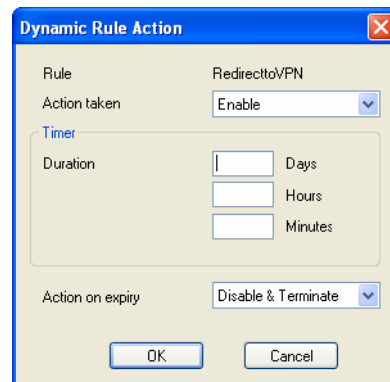
This is a singular capability of the phion firewall. It was developed to close one of the most dangerous gaps in firewall administration: the forgotten service access holes.

If a rule is subject to **Dynamic Activation**, it is inactive by default. It is switched on by demand and thereafter automatically switched off after some time.

Dynamically activated rules are flagged by the icon. To alter the state of a dynamic rule, change from the firewall configuration tab to the **Dynamic** tab ( **Firewall**).

Double-clicking a dynamic rule opens the **Change Dynamic Rule** dialogue.

Fig. 4-48 Change Dynamic Rule dialogue



Possible actions:

- **Enable**  
enable rule
- **Disable**  
disable rule
- **Disable & Terminate**  
disable rule and terminate all existing connections based on this rule
- **Block**  
block all traffic matching this rule explicitly
- **Block & Terminate**  
block all traffic matching this rule and terminate all existing connections based on this rule explicitly
- **None**  
none

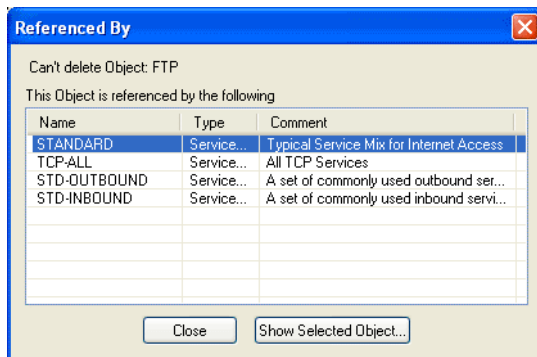
## 2.4 Delete, Copy and Paste within the Firewall Configuration

Since the rule set is built up of objects which can refer to each other, the data transfer actions like copy, paste, and delete are not as simple as they usually are. Several actions are forbidden to maintain consistency to the rule set as a whole.

### 2.4.1 Deleting

It is not permitted to delete an object which is referenced by another object. Otherwise, the other object would become invalid. If you try to delete a referenced object, the following window will appear.

Fig. 4-49 Warning dialogue when trying to delete a referenced object



By clicking **Show Selected Object ...** you can go directly to the referenced object, to see whether the reference is necessary. For some references this does not work, since they are not real objects of their own. This holds especially true for connection objects that are usually referenced by an action which is not a GUI-visible object by itself.

### 2.4.2 Copy and Paste

It is generally possible to copy objects from one firewall configuration to another, or simply duplicate objects for subsequent editing. Again, we face the problem of referenced objects. If you copy and paste objects with references to other objects, you are asked to transfer these objects as well.

#### Attention:

Copying objects across firewall configurations can result in unwanted and inconsistent rule sets. Use with caution.

## 2.5 Cascaded Rule Sets

The phion firewall comprises the unique feature of so-called cascaded rule sets. Usage of cascaded rule sets can contribute to improved rule management. The following two cascading methods exist:

- **Cascaded Rule Lists**
- **Cascaded Rule Sets**

Cascaded rule lists are included into a rule set. They share the rule set's properties, such as network objects and

service objects, and are stored in one file together with the rule set.

Cascaded rule sets, just like ordinary rule sets, are directly related to specific objects they own. Each cascaded rule set is saved to a separate file. To work together, these files are put together later on the operative system. Since cascaded rule sets are saved to distinct files, they can be assigned with specific administrative rights. With repository technology it is furthermore possible to share parts of the rule set with multiple firewall services.

For details of that concept consult **phion management centre** - 6.5.1.2 Creating a Shared Service, page 418 and 6.11 Supplement - Configuring the Cascaded Firewall (cfirewall), page 425.

There are two action types called **Cascade** and **Cascade Back**.

The process of applying a cascaded rule set is the following: the firewall starts to go through the master rule set. If a rule with **Cascade** action matches, it hands the request over to the rule set where the cascade rule points to. With the **Cascade Back** action it is just the other way around.

### 2.5.1 Cascaded Rule Lists

Clicking **New Rulelist** below the **Edit Rulelist** navigation bar item opens a window where the name of the new rule list has to be entered. Confirming by clicking **OK** opens a new tab next to the **Main Rules** tab labelled with the name entered.

#### Note:

The usage of the action type **Cascade** is limited to the main rule list and **Cascade Back** is limited to the sub-lists. It is not allowed to cascade between sublists.

#### Attention:

Rule set names may contain a maximum of 10 characters and digits.

### 2.5.2 Cascaded Rule Sets

The logical structure of a cascaded rule set is simple. Each part of the rule set is a complete rule set with its own net objects, service objects, and rules.

To avoid overcomplexity and because of limitations of overall rule name length, usage of cascaded rule lists is limited to the global rule set of a cascaded rule set.

#### Attention:

Use cascading with diligence and caution. Cascading can simplify your rule set. If applied wrong it will mess it up.

Cascading of rules is allowed in the following places:

- **Forwarding Firewall:**
  - in the main rule set between the main rule list and its sublists.

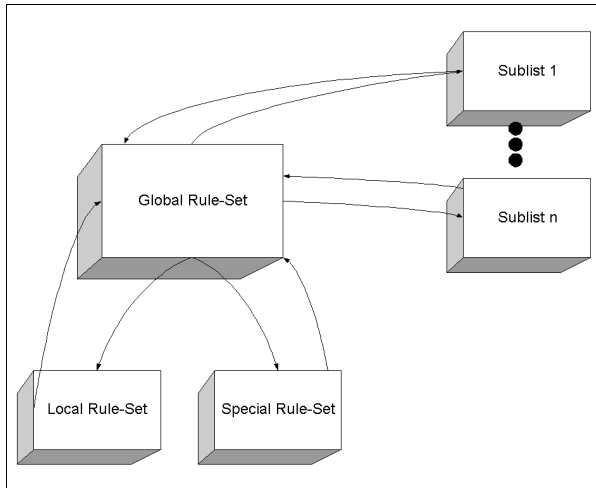
#### Note:

Cascading is not allowed from a rule-sublist to the other.

- **Cascaded Firewall**

- in the Global Rule Set between the main rule list and its sublists.
- from the Global Rule Set to Local Rule Set and Special Rule Set (see 6.11 Supplement - Configuring the Cascaded Firewall (cfirewall), page 425).

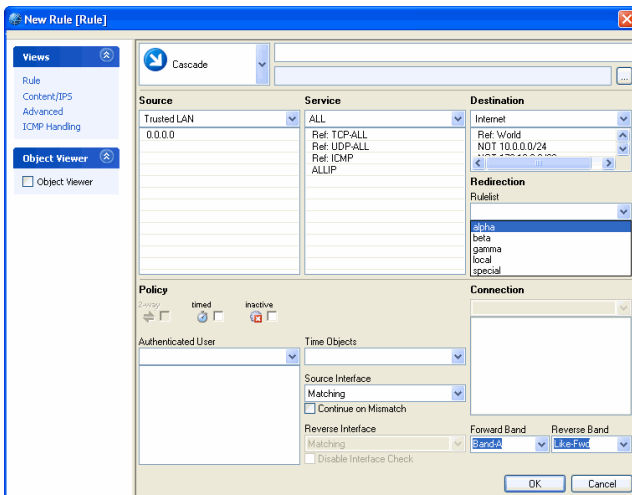
Fig. 4-50 Cascading of rules



### 2.5.2.1 View

The cascaded rule sets are shown by own top tabs in the firewall window next to the **Main Rules** tab. Here we have the master rule set with the three subsets called **alpha**, **beta**, and **gamma**.

Fig. 4-51 Rule for cascading into a rule-sublist

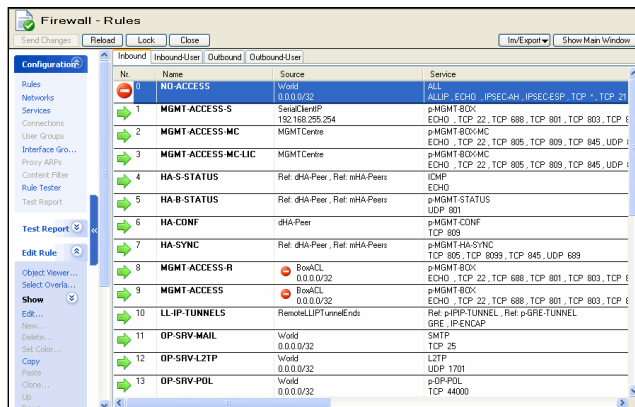


## 3. Local Rules

### 3.1 General

The rules for local traffic (which means traffic to the box and traffic generated by processes on the system itself (figure 4-2, page 126), are separated from the forwarding rules.

Fig. 4-52 Local rules



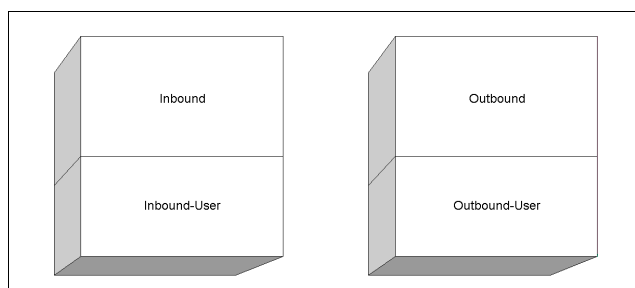
No.	Name	Source	Service
0	NO-ACCESS	World 0.0.0.0/32	ALL, ECHO, IPSEC-AH, IPSEC-ESP, TCP, UDP
1	MGMT-ACCESS-S	ServiceIP 193.169.255.254	pMGMT-BOX ECHO, TCP, 22, TCP, 688, TCP, 801, TCP, 803, TCP, 809
2	MGMT-ACCESS-MC	MGMT-Centre	pMGMT-BOX-MC ECHO, TCP, 22, TCP, 688, TCP, 801, TCP, 803, TCP, 809
3	MGMT-ACCESS-MC-LIC	MGMT-Centre	pMGMT-BOX-MC ECHO, TCP, 22, TCP, 688, TCP, 801, TCP, 803, TCP, 809
4	HA-S-STATUS	Ref: dHA-Peer, Ref: mHA-Peers	ICMP ECHO
5	HA-B-STATUS	Ref: dHA-Peer, Ref: mHA-Peers	pMGMT-STATUS UDP, 801
6	HA-CONF	dHA-Peer	pMGMT-CONF TCP, 809
7	HA-SYNC	Ref: dHA-Peer, Ref: mHA-Peers	pMGMT-HA-SYNC TCP, 805, TCP, 8099, TCP, 845, UDP, 689
8	MGMT-ACCESS-R	BoxACL 0.0.0.0/32	pMGMT-BOX ECHO, TCP, 22, TCP, 688, TCP, 801, TCP, 803, TCP, 809
9	MGMT-ACCESS	BoxACL 0.0.0.0/32	pMGMT-BOX ECHO, TCP, 22, TCP, 688, TCP, 801, TCP, 803, TCP, 809
10	LL-IP-TUNNELS	RemoteLLIP-TunnelEnds	Ref: pIP-TUNNEL, Ref: pGRE-TUNNEL GRE, IPENCAP
11	OP-SRV-MAIL	World 0.0.0.0/32	SMTP TCP, 25
12	OP-SRV-L2TP	World 0.0.0.0/32	L2TP UDP, 1701
13	OP-SRV-POL	World 0.0.0.0/32	pGRP-POL TCP, 4000

The rule set governing local traffic is one set, but internally divided into **four** parts:

- **Inbound** tab  
Predefined rule set with the most important rules for protection of management access and rules to identify the activities.
- **Inbound-User** tab  
Bound to the **Inbound** set. The default set contains a **Pass All** rule. Change this to restrict any traffic to the box. The ACL which protects the management access is not affected. It is handled by the Inbound rule set.
- **Outbound** tab  
Predefined rule set with the most important rules for protection of management access and rules to identify the activities.
- **Outbound-User** tab  
Bound to the **Outbound** set. The default set contains a **Pass All** rule. Change this to restrict any traffic leaving the box.

The rule set consists of two separated parts, the inbound and the outbound part. Each is divided into a standard set and an individual set, which are bound to one another.

Fig. 4-53 Local Rule scheme



### 3.2 Restrictions of Local Action and Connection Types

#### 3.2.1 Inbound Rule Set

Many features of the forwarding rule set are not needed for local traffic or are not applicable at all. The most important restrictions regard the Action and Connection types.

Available action types (see 2.2.3.3 Action Section, page 136):

- **Block**
- **Deny**
- **Pass**

#### 3.2.2 Outbound Rule Set

Available action types (see 2.2.3.3 Action Section, page 136):

- **Block**
- **Deny**
- **Pass**
- **Redirect**

#### Note:

Multiple Redirects (load sharing) is not possible. Available connection types (2.2.6 Connection Elements, page 145):

- **Client**
- **Proxydyn**
- **Explicit**

## 4. Testing and Verifying of Rule Sets

### 4.1 General

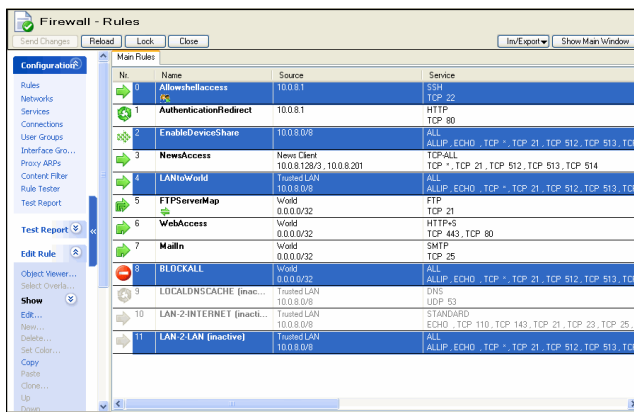
The phion firewall configuration appliance knows three tools, which assist in keeping firewall rules consistent:

- An overlap checker reveals interferences between rules.
- A rule tester explicitly applies a rule set to a given connection request.
- The most comprehensive part is a set of example connections which can be used to keep the rule set working as you want.

### 4.2 Overlapping Rules

Principally, a connection request can match with several rules of a rule set. Hence the succession of the configured rules is very important. To help the administrator avoiding mistakes, the phion firewall configuration includes a navigation bar item called **Select Overlapping ...** Use of this menu item in conjunction with selection of a rule will result in highlighting those rules possibly interfering with the selected one. In most cases the overlap is a harmless outcome of the use of very openly defined objects such as **World**.

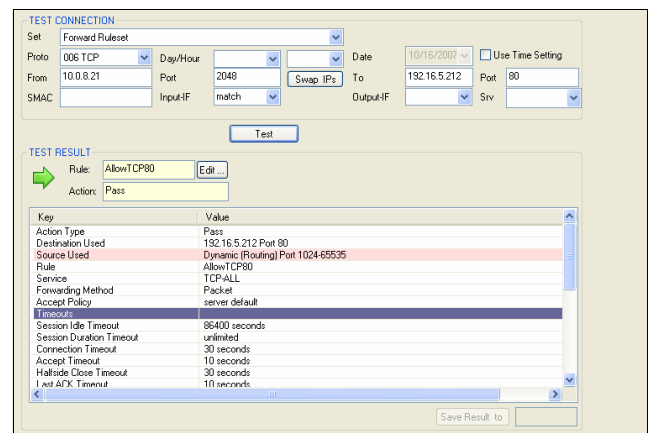
Fig. 4-54 Example for overlapping rules



### 4.3 Rule Tester

The rule tester allows testing rule sets for consistency.

Fig. 4-55 Rule tester window with all information of consequences of the matching rule



#### 4.3.1 Section Test Connection

The following entities are available for rule testing:



- Protocol
- Day of Week/Date/Time (optional)
- Source-IP
- Source-Port (default 2048)
- Destination-IP
- Destination-Port
- Source MAC Address
- Incoming Interface
- Outgoing Interface
- Service
- The button **Swap IPs** interchanges the source/destination IPs of the tested connection. Note that only the IPs and not the port information is swapped.
- Click the **Test** button to test the connection. The test result is then displayed in the section below.



### 4.3.2 Section Test Result

The following icons depict if a connection attempt would have succeeded or failed under given conditions.

**Table 4-9** Rule Tester - Test Result icons

Icon	Description
	A rule has applied and the connection attempt has succeeded.
	No matching rule has applied or the connection attempt has been blocked explicitly.

The **Rule** field displays the name of the rule which has been responsible for the result of the connection attempt. If a configured rule has applied you may click on the button **Edit ...** to open and modify it. If no rule has applied, the field will take the value **No matching rule found**.

#### ➤ **Save Result to** button

Enter a name into the field right of the button and click it to save the result of the test. The output of the connection test is then written to the Test Report window and stored as part of the rule set.

#### **Note:**

The rule set has to be in locked (that is read-write) state to save a test report.

## 4.4 Test Report

Usually a rule set has the aim to allow and/or steer a set of abstract policies. The test report utility is a tool to create a set of connection requests, which are critical for a security policy.

Test reports are saved on a first come first served basis. Valid test results are indicated by a ■ green symbol. Changing any rule parameter, which influences the result of a test report (for example object naming and details, changing rule succession), leads to a status icon change in the overview window - green icons become ● red. Furthermore, currently active values are added to the column listing, former ones are displayed embraced by brackets.

Test reports flagged with a red symbol are not valid anymore, as the new conditions first have to be applied to them. To do so, select the test report and click the **Rectify ...** entry in the context menu. Rectified test reports are again flagged with a ■ green status icon.

Double-clicking a test report or selecting **Edit ...** in the context menu opens the test report window, with all entries pre-filled, which have been responsible for the test result. This feature is very useful, as you may now use this window as template for further tests or you may even directly open the rule, which has been responsible for the handling of this connection attempt by clicking the **Edit ...** button next to the **Rule** field.

#### **Note:**

Test Reports are only saved temporarily. If you want to save them permanently, click **Send Changes** and **Activate** in the Test Report window.

# 5. Example Configuration

## 5.1 General

To move towards a comprehensive description of the possibilities of creating rules for the phion netfence firewall, we consider a setup with a LAN, the internet, and two demilitarised zones.

**Note:**

The rules described in this section are for principle informational purposes only. They are not at all recommended as an example of secure setup.

Fig. 4-56 Example for firewall configuration

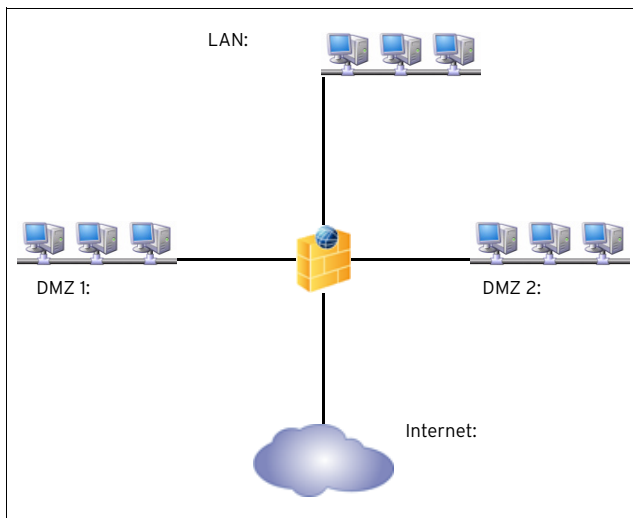


Table 4-10 Exemplary LAN scenario

IP / mask	Description
10.0.8.0/8	LAN, considered secure
10.0.8.34 10.0.8.110	Machines of the internal support team
10.0.8.128 - 10.0.8.134 10.0.8.201	Client PCs with access to news content provider (for example Reuters)
172.16.0.50	Public FTP server with automatic routing
172.16.0.143	Mail server for uncritical accounts, accessible via webmail
172.16.0.2 172.16.0.21 172.16.0.25 172.16.0.32	Internal IP addresses of the web servers
172.17.0.100	Terminal server and gateway to my-news provider (for example Reuters)
172.17.0.8 - 172.17.0.15	Addresses with access rights to the terminal server
105.8.23.64/3	External address space provided by my ISP
105.8.23.65	External address of www.myexample.com, at the same time mail exchanger for myexample.com
105.8.23.66	External address of ftp.myexample.com
105.8.23.67	External address of the firewall to be used as proxy address^
10.0.8.100	External address of the firewall (default gateway of my LAN)
172.16.0.100	DMZ 1 address of the firewall (default gateway of DMZ 1)
172.17.0.99	DMZ 2 address of the firewall (default gateway of DMZ 2)

Let us consider the following security policies to be implemented.

- All computers in the LAN should have full access to the internet.
- All news-service client PCs should have access to the news service.
- The FTP server should act as if it has an official IP and should communicate with others via FTP (as a server and a client).
- The mailserver should be accessible for everyone via secure webmail and should also be used as SMTP server for the webmail users.
- The webservers run server-side java and are usually under heavy load. Traffic should be distributed to them.
- The external support for the webservers has only ssh access to one webserver. From there it has to hop to the next one.
- The internal support team should have access to the DMZ.

We therefore have to handle six different situations that are to be translated into phion firewall rule language. In the next section we want to extend them with some sophisticated additional properties.

Since the rule set is sensitive to the succession of the rules, we want to give a general hint for starting to build up such a set.

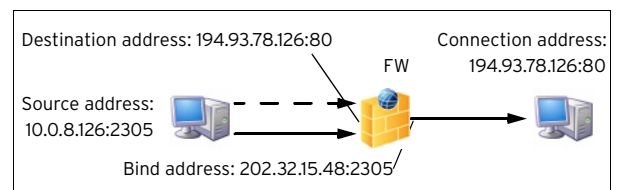
**Note:**

In most situations, start with the redirections followed by maps and end with the pass rules. This is almost always true.

We start by figuring out, what the security policies mean in networking language:

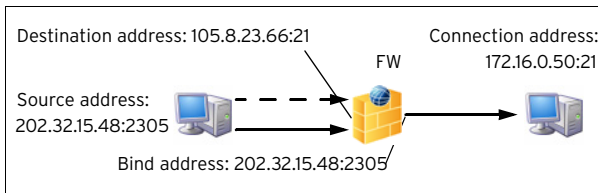
- Destination address is identical to the connection address, whereas the source address is translated to a different bind address. All LAN machines get the same bind address: "proxying, masquerading". The connection from the sysadmin's machine to the DMZ looks just the same.

Fig. 4-57 Network situation for a typical LAN to Internet connection



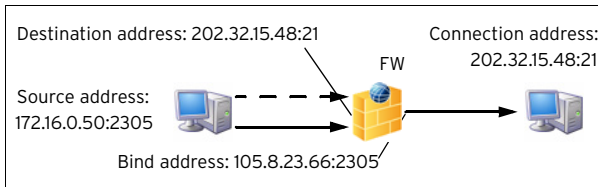
- Source address is the same as the bind address, whereas the destination address is translated to the internal IP of the FTP server.

**Fig. 4-58** Network situation for a ftp connection to our FTP server.



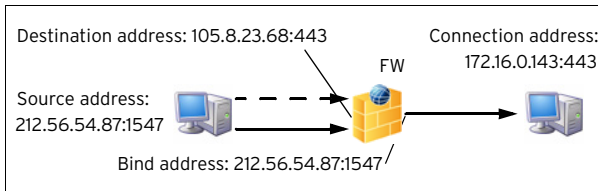
- Destination address is identical to the connection address, whereas the source address is translated a different bind address. The bind address is used only for the FTP server: explicit source NAT.

**Fig. 4-59** Network situation for a ftp connection from our FTP server to another FTP server



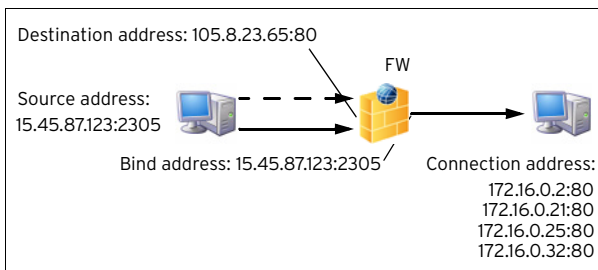
- Source address is the same as the bind address, whereas the destination address is translated to the internal IP of the webmail server: Redirecting

**Fig. 4-60** Network situation for a secure connection to the webmail server



- Source address is the same as the bind address, whereas the destination address is translated to the one of the internal IP addresses of the www servers: Redirecting with cycling

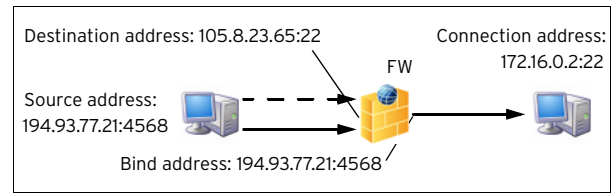
**Fig. 4-61** Network situation for a client connection to our webserver farm



- Source address is the same as the bind address, whereas the destination address is translated to the internal IP of the mail server: Redirecting. Note that although the destination address for the client is the same as when connecting to the

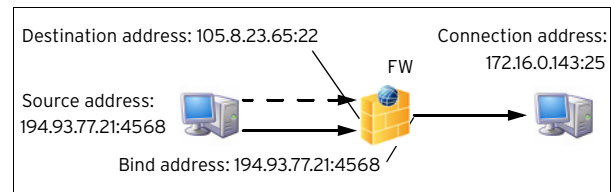
webservers via http, the internal destination is completely different (Service dependent NAT).

**Fig. 4-62** Network situation for remote web server support



- Source address is the same as the bind address, whereas the destination address is translated to the internal IP of the mail server: Redirecting. Note that although the destination address for the client is the same as when connecting to the web server, the internal destination is completely different (Service dependent NAT).

**Fig. 4-63** Network situation for sending a mail to the mail server

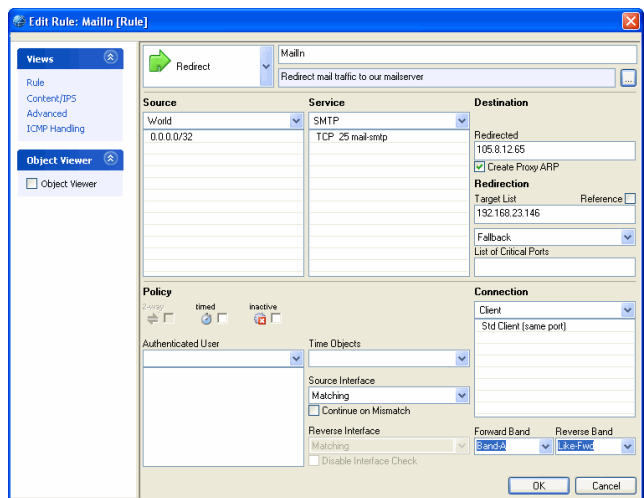


**Step 1** Open the rule set via **Config > Box > Virtual Servers > <servername> > Assigned Services > <servicename> (firewall) > Forwarding Rules.**

Lock the rule set by clicking the **Lock** button and select **New** from the context menu (right-click in the configuration window).

With the information above (figure 4-63), we are able to define a rule set which lets the firewall act exactly as we want it to. We will start with the redirection rules as mentioned above. Allow the first one to function as mail traffic to the mail server.

**Fig. 4-64** Rule for redirection of mail traffic to internal mailserver



**Step 2 The rule for external support for the webservers is almost the same.**

Therefore, we will go on to the next interesting rule, the redirection of an external IP to the web server farm (figure 4-61, page 166).

HTTP access to one IP, namely 105.8.23.65, is redirected to four other IPs. The redirection algorithm is the following: the client address in binary form is divided by the number of redirection targets. The remainder now decides to which target the client is redirected (0 to the first, 1 to the second, 2 to the third, ...). Since the IP address space is approximately equally distributed, this method provides an almost perfect load balancing for all practical purposes.

Introduce two rules of the following type:

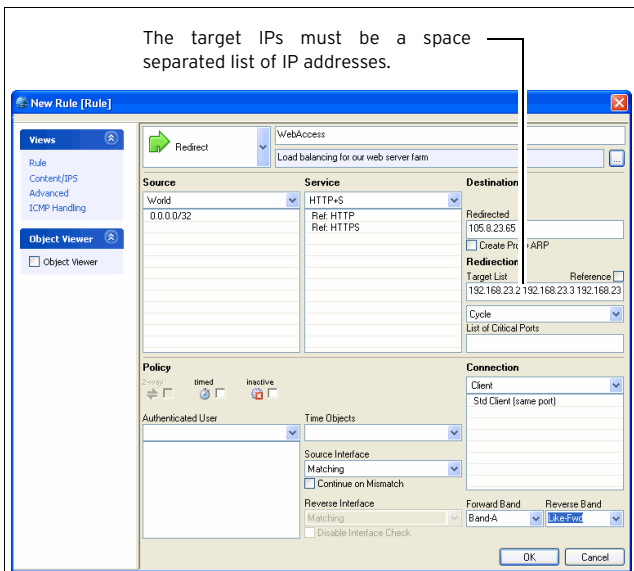
**Table 4-11** Exemplary rule configuration in comparison

Source	Service	Action	Connection type	Destination
World	ftp	Redirect	Client	105.8.23.66 redirected to 172.16.0.50
172.16.0.50	ftp	Pass	Proxy explicit: 105.8.23.66	World

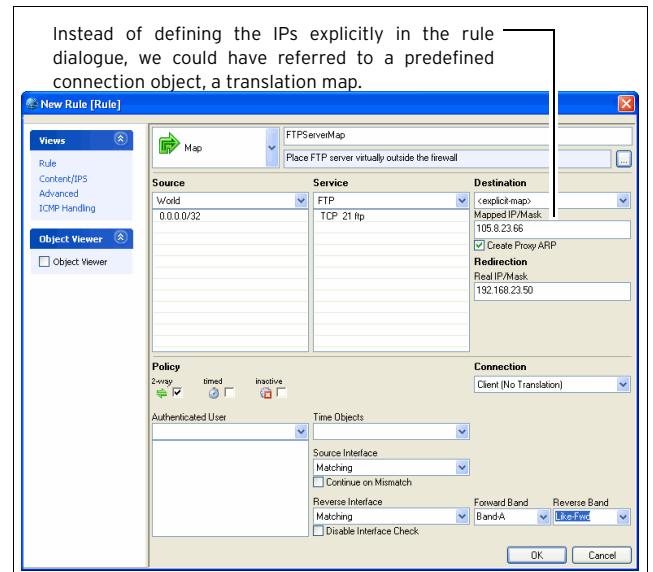
These two rules do not seem to have much in common. But if we have a look at figure 4-58 and figure 4-59, it becomes clear that the rules are just mirrors of each other. Since this is a frequent situation in networking life, the phion firewall has a single action to handle this - **Map**.

One key advantage of mapping is that it can be applied in both ways. Just like in the case of the FTP server.

**Fig. 4-65** Rule which implements load balancing for the web server farm



**Fig. 4-66** Rule which maps the ftp server to the internet

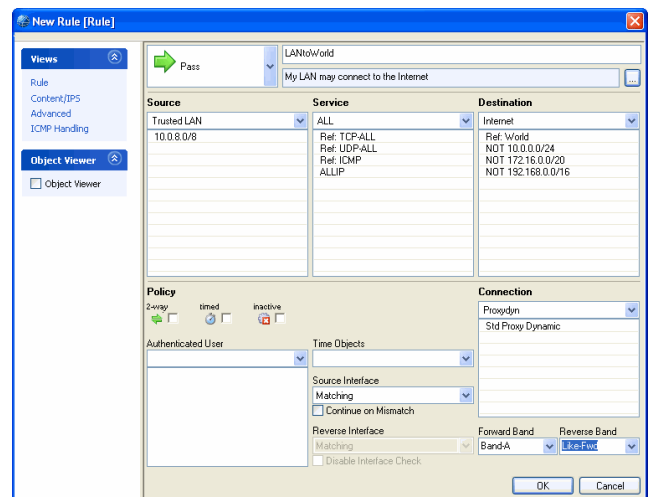


**Step 3 The last rules to be created are the one from LAN to DMZs and internet (figure 4-57, page 165).**

We use the action **Pass**, because the destination IP is identical to the connection IP.

**Note:** Allowing access to the world includes access to the DMZs. If you want to give DMZ access to selected nodes only you have to insert a rule which blocks access from the LAN to the DMZs. This rule has to be placed after the rules which allow access for the selected nodes and before allowing access to the world.

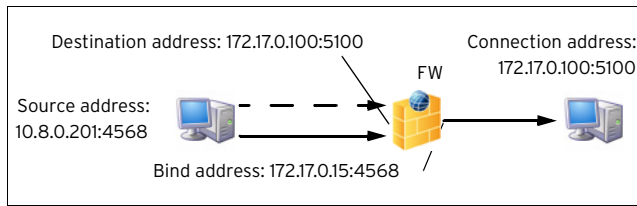
**Fig. 4-67** Rule for LAN access to the whole world



Finally, we want to give certain clients of the LAN access to the news gateway in DMZ 2. The network environment is a little more complicated, because each of the clients is mapped to a certain bind address. To avoid the introduction of an own rule for each client, we define a new connection object, a **translation map**.

In this map, we define which source IP should get which bind IP if the rule uses this connection object.

Fig. 4-68 Network situation for a typical LAN to Internet connection



The destination address is identical to the connection address, whereas the source address is translated into a different bind address. Each client gets a different bind address: "explicit source NAT".

Fig. 4-69 Connection object dialogue window for translation map

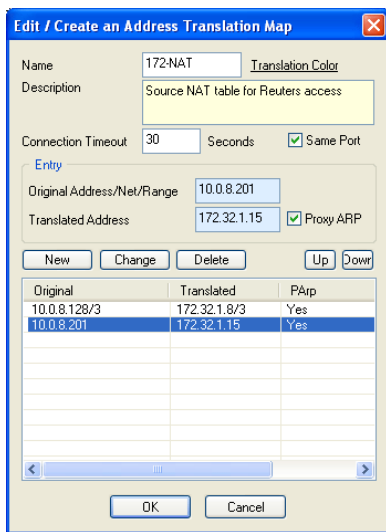
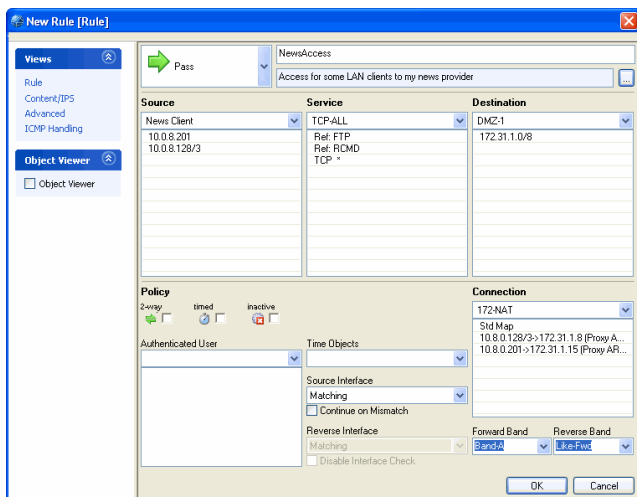


Fig. 4-70 Rule dialogue for the news access rule via explicit source NAT



We now end up with a rule set that implements our general security policy. There are however some pending improvements. Before we refine the rule set, we will go on with a detailed description of the rule in general.

A last attention we care to the FTP server rule. Since it works in both ways, we have given a DMZ server ftp access to our LAN, too. THIS IS SURELY NOT WHAT WE INTENDED. Hence we fill in another rule, which blocks all traffic from the DMZs to the LAN.

## 5.2 Advanced Settings in the Example Setup

With the knowledge of the advanced part of rule configuration one would suggest the following improvements for this example.

Table 4-12 Improved rule configuration

Rule	Improvement
Web-support	Inbound, Dynamic activation
Web-in	Inbound
Mail-in	Inbound
Webmail	Inbound
FTPServerMap	Inbound, Reversed Policy: Outbound
Admin2DMZ	Outbound
NewsAccess	Outbound
LAN2world	Outbound



# 6. Real Time Information and Manipulation

## 6.1 GUI Elements

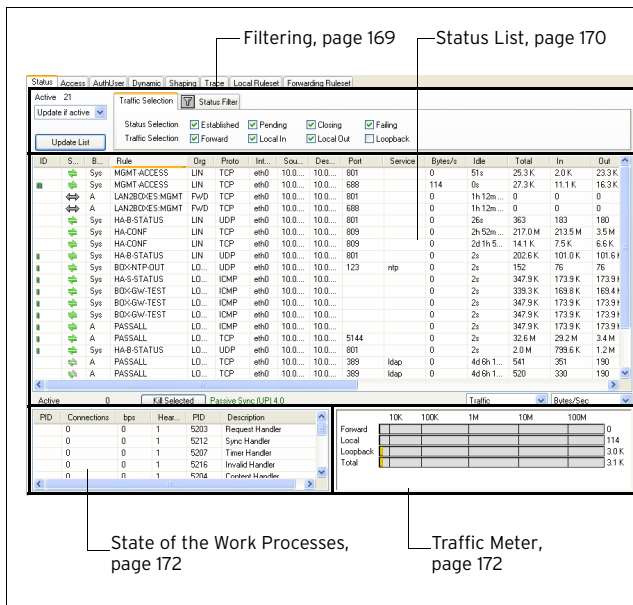
The operative firewall GUI consists of the following parts/tabs:

- **Status** - 6.2 Real Time Status, page 169
- **Access Cache** - 6.3 Access Cache, page 173
- **AuthUser** - 6.4 Authenticated User, page 176
- **Dynamic** - 6.5 Dynamic Rules and Data, page 176
- **Shaping** - 6.6 Shaping, page 177
- **Trace** - 6.7 Tracing Connections, page 177
- **Audit Log** - 6.8 Audit Log, page 178
- **Local Rule Set** - 3. Local Rules, page 162
- **Forwarding Rule Set** - 2. Firewall Configuration, page 126

## 6.2 Real Time Status

In the **Status** tab of the firewall GUI traffic going through your firewall can be watched in realtime.

Fig. 4-71 Status tab



The tab **Traffic Selection** (top, right) is used for regulating the shown information. Therefore, the options (checkboxes) in the two lines **Status Selection** and **Traffic Selection** are used:

### Status Selection line

- **Established**  
displays all established connections
- **Pending**  
displays all connections that are establishing right now
- **Closing**  
displays all connections that are closing
- **Failing**  
displays all connections that could not be established

### Traffic Selection line

- **Forward**  
displays the traffic on the Forwarding FW
- **Local In**  
displays the incoming traffic on the box firewall
- **Local Out**  
displays the outgoing traffic from the box firewall
- **Loopback**  
traffic over the loopback interface

### 6.2.1.2 Status Filter

The tab **Status Filter** allows you to constrain the view to very specific properties.

- **Rule**  
allows setting a filter for a specific rule
- **Proto.**  
allows setting a filter for a specific protocol
- **Source**  
allows setting a filter for a specific source IP address/range
- **Dest.**  
allows setting a filter for a specific destination IP address/range
- **Interface**  
allows setting a filter for a specific interface (for example eth0)
- **Addr.**  
allows to setting a filter for a specific IP address
- **Srv.**  
allows setting a filter for a specific service
- **Port**  
allows setting a filter for a specific port
- **Src-Interface**  
allows setting a filter for a specific source interface
- **Dest-Interface**  
allows setting a filter for a specific destination interface

## 6.2.1 Filtering

**Note:**

To activate the defined view it is necessary to click **Update List.**

### 6.2.1.1 Traffic Selection

The pull-down menu (top, left) serves to define the number of shown entries.

By ticking the corresponding checkboxes it is possible to combine multiple fields in order to improve the filter sequence.

**Note:**






All fields except the pull-down menu **Proto.** allow the use of the \* and ? wild cards.

## 6.2.2 Status List

**Note:**

Double-clicking an entry opens a window called **Details** that contains all information concerning the entry in one view.

The list itself consists of the following columns:

- **ID**  
Icons indicating the amount of traffic ( ) and the unique access ID for each active connection
- **State**
  -  One-way traffic
  -  Connection established (TCP) - Both way traffic (all other)
  -  Connection could not be established
  -  Closing connection
- **Band**  
Traffic band (**SYS, A, B, C, D, E, F, G**)
- **Rule**  
Name of the affected rule
- **Org**  
Origin:  
LIN: **Local In**; equals incoming traffic on the box firewall  
LOUT: **Local Out**; equals outgoing traffic from the box firewall  
LB: **Loopback**; equals traffic via the loopback interface  
FWD: **Forwarding**; equals outbound traffic via the forwarding firewall  
IFWD: **Inbound Forwarding**; inbound traffic to the firewall  
PXY: **Proxy**; equals outbound traffic via the proxy  
IPXY: **Inbound Proxy**; equals inbound traffic via the proxy  
TAP: **Transparent Application Proxying**; equals traffic via stream forwarding
- **Proto**  
Used protocol; for example TCP, UDP, ICMP
- **Interface**  
Shows the affected interface
- **Source**  
Source IP:Port
- **Destination**  
Destination IP
- **Port**  
Destination port (or internal ICMP ID)
- **Service**  
Name of dynamic service
- **Bytes/s**  
Bytes per second (during the last second)

- **Idle**  
time passed since last data transfer
- **Total**  
Total number of bytes transferred over this connection
- **In**  
Total number of bytes transferred over this connection from the source
- **Out**  
Total number of bytes transferred over this connection to the source
- **Start**  
Time passed since connection has been established
- **Bind**  
IP and port of the bind address
- **Conn**  
IP and port of the connection address
- **Out-IF**  
Outgoing interface
- **Status**  
Status of active connections

**Note:**

Connections can be terminated by using **Terminate Session** from the right mouse-button context menu. Do not use this feature for fun.

The following status types exist:

**Table 4-13** Status types and their origin

Status name	Origin	Description
FWD-NEW	TCP Packet Forwarding Outbound	Session is validated by the firewall rule set, no traffic was forwarded so far.
FWD-FSYN-RCV	TCP Packet Forwarding Outbound	The initial SYN packet received from the session source was forwarded
FWD-RSYN-RS V	TCP Packet Forwarding Outbound	The session destination answered the SYN with a SYN/ACK packet
FWD-EST	TCP Packet Forwarding Outbound	The SYN/ACK packet was acknowledged by the session source. The TCP session is established.
FWD-RET	TCP Packet Forwarding Outbound	Either source or destination are re transmitting packets. The connection might be dysfunctional.
FWD-FFIN-RCV	TCP Packet Forwarding Outbound	The session source sent a FIN datagram indicating to terminate the session
FWD-RLACK	TCP Packet Forwarding Outbound	The session destination answered the FIN packet with a FIN reply and awaits the last acknowledgement for this packet
FWD-RFIN-RCV	TCP Packet Forwarding Outbound	The session destination sent a FIN datagram indicating to terminate the session
FWD-FLACK	TCP Packet Forwarding Outbound	The session source answered the FIN packet with a FIN reply and awaits the last acknowledgement for this packet
FWD-WAIT	TCP Packet Forwarding Outbound	The session was reset by one of the two participants by sending a RST packet. A wait period of 5 seconds will silently discard all packet belonging to that session
FWD-TERM	TCP Packet Forwarding Outbound	The session is terminated and will shortly be removed from the session list.
IFWD-NEW	TCP Packet Forwarding Inbound	Session is validated by the firewall rule set, no traffic was forwarded so

**Table 4-13** Status types and their origin

Status name	Origin	Description
IFWD-SYN-SND	TCP Packet Forwarding Inbound	A SYN packet was sent to the destination initiating the session (Note that the session with the source is already established)
IFWD-EST	TCP Packet Forwarding Inbound	The destination replied the SYN with a SYN/ACK. The session is established.
IFWD-RET	TCP Packet Forwarding Inbound	Either source or destination are re transmitting packets. The connection might be disfunctional.
IFWD-FFIN-RCV	TCP Packet Forwarding Inbound	The session source sent a FIN datagram indicating to terminate the session
IFWD-RLACK	TCP Packet Forwarding Inbound	The session destination answered the FIN packet with a FIN reply and awaits the last acknowledgement for this packet
IFWD-RFIN-RCV	TCP Packet Forwarding Inbound	The session destination sent a FIN datagram indicating to terminate the session
IFWD-FLACK	TCP Packet Forwarding Inbound	The session source answered the FIN packet with a FIN reply and awaits the last acknowledgement for this packet
IFWD-WAIT	TCP Packet Forwarding Inbound	The session was reset by one of the two participants by sending a RST packet. A wait period of 5 seconds will silently discard all packet belonging to that session
IFWD-TERM	TCP Packet Forwarding Inbound	The session is terminated and will shortly be removed from the session list.
PXY-NEW	TCP Stream Forwarding Outbound	Session is validated by the firewall rule set, no traffic was forwarded so far.
PXY-CONN	TCP Stream Forwarding Outbound	A socket connection to the destination is in progress of being established
PXY-ACC	TCP Stream Forwarding Outbound	A socket connection to the source is in progress of being accepted.
PXY-EST	TCP Stream Forwarding Outbound	Two established TCP socket connection to the source and destination exist.
PXY-SRC-CLO	TCP Stream Forwarding Outbound	The socket to the source is closed or is in the closing process.
PXY-DST-CLO	TCP Stream Forwarding Outbound	The socket to the destination is closed or is in the closing process.
PXY-SD-CLO	TCP Stream Forwarding Outbound	The source and the destination socket are closed or in the closing process
PXY-TERM	TCP Stream Forwarding Outbound	The session is terminated and will shortly be removed from the session list.
IPXY-NEW	TCP Stream Forwarding Inbound	Session is validated by the firewall rule set, no traffic was forwarded so far.
IPXY-ACC	TCP Stream Forwarding Inbound	A socket connection to the source is in progress of being accepted.
IPXY-CONN	TCP Stream Forwarding Inbound	A socket connection to the destination is in progress of being established
IPXY-EST	TCP Stream Forwarding Inbound	Two established TCP socket connection to the source and destination exist.

**Table 4-13** Status types and their origin

Status name	Origin	Description
IPXY-SRC-CLO	TCP Stream Forwarding Inbound	The socket to the source is closed or is in the closing process.
IPXY-DST-CLO	TCP Stream Forwarding Inbound	The socket to the destination is closed or is in the closing process.
IPXY-SD-CLO	TCP Stream Forwarding Inbound	The source and the destination socket are closed or in the closing process
IPXY-TERM	TCP Stream Forwarding Inbound	The session is terminated and will shortly be removed from the session list.
UDP-NEW	UDP Forwarding	Session is validated by the firewall rule set, no traffic was forwarded so far.
UDP-RCV	UDP Forwarding	Traffic has been received from the source and was forwarded to the destination
UDP-REPL	UDP Forwarding	The destination replied to the traffic sent by the source
UDP-SENT	UDP Forwarding	The source transmitted further traffic after having received a reply from the destination
UDP-FAIL	UDP Forwarding	The destination or a network component on the path to the destination sent an ICMP indicating that the desired request cannot be serviced.
ECHO-NEW	ECHO Forwarding	Session is validated by the firewall rule set, no traffic was forwarded so far.
ECHO-RCV	ECHO Forwarding	Traffic has been received from the source and was forwarded to the destination
ECHO-REPL	ECHO Forwarding	The destination replied to the traffic sent by the source
ECHO-SENT	ECHO Forwarding	The source sent more traffic after racing a reply from the destination
ECHO-FAIL	ECHO Forwarding	The destination or a network component on the path to the destination sent an ICMP indicating that the desired request cannot be serviced.
OTHER-NEW	OTHER Protocols Forwarding	Session is validated by the firewall rule set, no traffic was forwarded so far.
OTHER-RCV	OTHER Protocols Forwarding	Traffic has been received from the source and was forwarded to the destination
OTHER-REPL	OTHER Protocols Forwarding	The destination replied to the traffic sent by the source
OTHER-SENT	OTHER Protocols Forwarding	The source sent more traffic after receiving a reply from the destination
OTHER-FAIL	OTHER Protocols Forwarding	The destination or a network component on the path to the destination sent an ICMP indicating that the desired request cannot be serviced.
LOC-NEW	Local TCP Traffic	A local TCP session was granted by the local rule set
LOC-EST	Local TCP Traffic	The local TCP session is fully established.
LOC-SYN-SND	Local TCP Traffic	A Local-Out TCP session is initiated by sending a SYN packet.
LOC-SYN-RCV	Local TCP Traffic	A Local-In TCP session is initiated by receiving a SYN packet.
LOC-FIN-WAIT1	Local TCP Traffic	An established local TCP session started the close process by sending a FIN packet
LOC-FIN-WAIT2	Local TCP Traffic	A local TCP session in the FIN-WAIT1 state received an ACK for the FIN packet
LOC-TIME-WAIT	Local TCP Traffic	A local TCP session in the FIN-WAIT1 or in the FIN-WAIT2 state received a FIN packet.

Table 4-13 Status types and their origin

Status name	Origin	Description
LOC-CLOSE	Local TCP Traffic	An established local TCP session is closed.
LOC-CLOSE-WAIT	Local TCP Traffic	An established local TCP session received a FIN packet.
LOC-LAST-ACK	Local TCP Traffic	Application holding an established TCP socket responded to a received FIN by closing the socket. A FIN is sent in return.
LOC-LISTEN	Local TCP Traffic	A local socket awaits connection request (SYN packets)
LOC-CLOSING	Local TCP Traffic	A local socket in the FIN_WAIT1 state received a FIN packet.
LOC-FINISH	Local TCP Traffic	A local TCP socket was removed from the internal socket list.

### ➤ Policy

The following entries are possible:

Table 4-14 Overview of possible access cache entries

Entry	Description
NO_MATCH_IIF	Received packet (Forward Direction) must NOT match initial input interface
NO_MATCH_OIF	Received packet (Reverse Direction) must NOT match initial output interface
INBOUND	Session is set to accept policy Inbound ( <b>Firewall - 2.3.3.3 Accept Policies</b> , page 157)
FWD_FILTER	Content filter is applied for forward traffic
REV_FILTER	Content filter is applied for reverse traffic
TRACE	Session is being traced
NOTIFY_CONNECT	Session will notify the Firewall Service upon successful or failing TCP establishment. Needed for multiple redirection status
PROXYDYN	Bind IP is determined by the routing table
NOLOG	Session will not generate log file entries
NOSTAT	Session will not generate statistics
NOCACHE	Session will not generate an access cache entry
NONAGLE	Nagle algorithm is turned OFF
LOG_STATE	Session will log each state change / Every state change of this session is logged
OWN_LOG	Session will log to firewall rule log file
SRVSTAT	Session will resolve service object names when generating statistics
DYNAMIC_PORT	Session is dynamically NATed. The outgoing source port will differ from the original client port
NOSYNC	Session will not be synchronised for transparent failover
CLEAR_ECN	Session will clear any ECN bits in the IP header

### ➤ TI Classification

Transport rating setting (Bulk, Quality, or Fallback with IDs 0-7 each)

### ➤ FWD Shape

Shows you the actual shape connectors used in forward direction. There are possibly two shape connectors involved, one for ingress and one for egress shaping respectively. Ingress shaping in forward direction takes place at the inbound interface, egress shaping at the outbound interface.

The first shape connector displayed is the one used for ingress and the second one is used for egress shaping.

### ➤ REV Shape

Shows you the actual shape connectors used in reverse direction. There are possibly two shape connectors involved, one for ingress and one for egress shaping respectively. Ingress shaping in reverse direction takes place at the outbound interface, egress shaping at the inbound interface.

The first shape connector displayed is the one used for ingress and the second one is used for egress shaping.

## 6.2.3 State of the Work Processes

In the lower left of the Status tab a display for the workers state is integrated.

The entry **Active** displays the currently active worker processes.

The button **Kill Selected** is used for terminating single workers.

The entry on the right of the **Kill Selected** button shows the status of the synchronisation in case of active Transparent Failover (**High Availability**, page 375) and consists of the following possible states:

#### ➤ Active Sync (UP)

shown on active HA partner; synchronisation works

#### ➤ Active Sync (DOWN)

shown on active HA partner; sync would work, but BoxFW is down

#### ➤ Passive Sync (UP)

shown on passive HA partner; synchronisation works

#### ➤ Passive Sync (DOWN)

shown on passive HA partner; sync would work, but BoxFW is down

The window provides the following information about the processes:

#### ➤ PID

System process ID

#### ➤ Connections

Number of connections handled by worker

#### ➤ bps

bytes per second (during the last second)

#### ➤ Heartbeat

Time in seconds the process stopped to answer, should never be more than 2.

#### ➤ PID

System process ID; allows view on PID and full extended description column

#### ➤ Description

Role description of worker

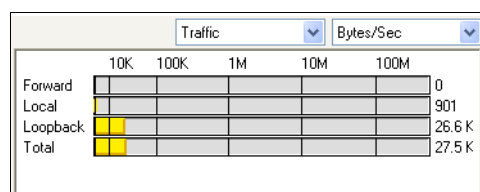
## 6.2.4 Traffic Meter

In the lower right of the **Status** tab a traffic meter is integrated.

The firewall engine samples the amount of traffic over 10 seconds and the traffic meter shows it either based on bands (**SYS**, **A** to **G**) or on traffic origin (**Forward**, **Loopback**, **Local**, **Total**).

Both traffics are available as **Bytes/sec** or **Packets/sec**.

Fig. 4-72 Traffic meter



The third available view is called **TF Sync** and contains detailed information concerning the Transparent Failover function of a HA Forwarding Firewall. The pull-down menu for the statistics type (with the options **Bytes/sec** and **Packets/sec**) has no function for this type of view.

The display consists of the following entries:

- **My Sync Addr**  
IP address and connection port for synchronisation of this box
- **Partner Sync Addr**  
IP address and connection port for synchronisation of the HA partner box
- **Synced Sessions**  
Number of sessions successfully synchronised
- **Pending Sessions**  
Number of not synchronised sessions

## 6.3 Access Cache

The access cache is the most powerful tool for troubleshooting.

Fig. 4-73 Access Cache

AID	Dst	Dev	Src	Dst	Proto	Port	Service	Count	Last	Rule	Info	MAC	Br
253	LOUT	ppp1	62.4...	80.6...	TCP	80	http	1	2d 21h...	PASSALL		40.0...	62
150	LOUT	ppp1	62.4...	80.7...	TCP	80	http	6	2d 23h...	PASSALL		40.0...	62
245	LOUT	ppp1	62.4...	80.1...	TCP	80	http	4	2d 21h...	PASSALL		00.0...	62
B-17	LIN	ppp1	80.1...	80.1...	ICMP			1	13h 51...	<no-match>	Block...	00.0...	
B-16	LIN	ppp1	80.1...	80.1...	ICMP			1	13h 55...	<no-match>	Block...	00.0...	
B-15	LIN	ppp1	80.1...	80.1...	ICMP			1	15h 43...	<no-match>	Block...	00.0...	
285	LOUT	ce01	62.4...	80.2...	TCP	80	http	3	2d 21h...	PASSALL		40.0...	62

### 6.3.1 Available Filter Options

#### 6.3.1.1 Global Viewing Options

The area on the top left side of the Access Cache tab is used to define viewing preferences.

Use the pull-down menu on the top to set the maximum to be shown cache entries.

Activate the checkbox **Show Hostnames**, if you want source and destination IPs to be translated to hostnames as far as possible.

**Note:**

IP addresses will only be resolved to hostnames, if this function has been enabled in the firewall settings (see Resolve Access Cache IPs, page 129).

**Note:**

Click **Update List** to activate any newly defined view.

#### 6.3.1.2 Cache Selection

The tab **Cache Selection** (top, right) is used for regulating the shown information. Therefore, the options (checkboxes) in the two lines **Traffic Selection** and **Cache Selection** are used:

**Traffic Selection** line

- **Forward**  
displays the traffic on the Forwarding FW
- **Local In**  
displays the incoming traffic on the box firewall
- **Local Out**  
displays the outgoing traffic from the box firewall
- **Loopback**  
traffic over the loopback interface

**Cache Selection** line

- **Access**  
displays all allowed and successfully established connections
- **Rule Block**  
displays all connections matching Deny Reasons, page 174/Block Reasons, page 175.
- **Packet Drop**  
displays all connections matching the Drop Reasons, page 175.
- **Fail**  
displays all connections matching the Fail Reasons, page 176.
- **ARP**  
displays all ARP requests
- **Scan**  
displays all SCAN tasks

#### 6.3.1.3 Cache Filter

The tab **Cache Filter** allows you to constrain the view to very specific properties.

- **Rule**  
allows setting a filter for a specific rule
- **Proto.**  
allows setting a filter for a specific protocol
- **Source**  
allows setting a filter for a specific source IP address/range
- **Dest.**  
allows setting a filter for a specific destination IP address/range
- **Interface**  
allows setting a filter for a specific interface (for example eth0)
- **Addr.**  
allows to setting a filter for a specific IP address
- **Srv.**  
allows setting a filter for a specific service
- **Port**  
allows setting a filter for a specific port
- **Src-Interface**  
allows setting a filter for a specific source interface
- **Dest-Interface**  
allows setting a filter for a specific destination interface



By ticking the corresponding checkboxes it is possible to combine multiple fields in order to improve the filter sequence.

**Note:**

All fields except the pull-down menu **Proto**, allow the use of the \* and ? wild cards.

The size of the caches is configured in the Firewall Settings and requires a service restart.

## 6.3.2 Access Cache List

**Note:**

Double-clicking an entry opens a window called **Details** that contains all information concerning the entry in one view.

The list itself consists of the following columns:

- **AID**  
Access ID including an icon for blocked connections (🔴), an icon for established connections (🟢) and consecutive numbering for both blocked and established connections. The AID contains also the letter **B** to indicate blocked connection.
- **Org (Origin)**  
LIN: **Local In**; incoming traffic on the box firewall  
LOUT: **Local Out**; outgoing traffic from the box firewall  
LB: **Loopback**; traffic via the loopback interface  
FWD: **Forwarding**; outbound traffic via the forwarding firewall  
IFWD: **Inbound Forwarding**; inbound traffic to the firewall  
PXY: **Proxy**; outbound traffic via the proxy  
IPXY: **Inbound Proxy**; inbound traffic via the proxy  
TAP: **Transparent Application Proxying**; traffic via virtual interface  
LRD: **Local Redirect**; redirect traffic configured in forwarding rule set
- **Interface**  
Incoming interface
- **Source**  
Source IP of the requesting client
- **Destination**  
IP of the requested destination
- **Proto**  
Used protocol; for example TCP, UDP, ICMP
- **Port**  
Port of the requested destination
- **Service**  
Assigned (dynamic) service
- **Count**  
Number of tries
- **Last**  
Time passed since last try
- **Rule**  
Name of the matching rule
- **Info**

Reason why things happen (see 6.3.3 Reasons, page 174).

**Note:**

Entry **TF-sync** means that the session is synced (shows up on the backup machine where the firewall service is on standby).

- **MAC**  
MAC address of the interface
- **Bind**  
Bind address
- **Conn**  
IP of the connection address
- **Out-IF**  
Outgoing interface; tunnel and transport is visualized.
- **OutRoute**  
unicast or local
- **Next Hop**  
Gateway

**Note:**

There may show up a **Next Hop** address in a **Local Redirect** action. This routing information comes from the reverse direction lookup (how packets will be routed from loopback to client).

### 6.3.2.1 Context Menus

Right-clicking into the listing makes the following context menus available:

- The standard context menu accessible through the item **Tools** (see 4.2 Standard Context Menu, page 395).
- **Remove Selected**  
This entry is only available with one or multiple item(s) selected. Executing it removes all selected access cache entries from the listing.
- **Flush Cache**  
Removes all entries from the access cache.
- **Save Cache Selection Policy**  
Permanently saves settings defined through the section Cache Selection (see 6.3.1.2 Cache Selection) in the phion.a administration tool.
- **Group by**  
For better lucidity, access cache entries may be grouped by their essential attributes such as Rule, Interface, Origin, ... Grouped entries are arranged in pop-up menus topped by a labelled title bar.

## 6.3.3 Reasons

### 6.3.3.1 Deny Reasons

**Table 4-15** Reasons for connections denials

Deny Reasons	Description
Deny by Dynamic Rule	The session request was matched by a dynamic rule, which is set to be denied.
Deny by Rule	A rule denies a session request explicitly.
Deny by Rule Destination Mismatch	A rule with the 'DENY on Destination Mismatch' option selected, matched and resulted into a deny action.

**Table 4-15** Reasons for connections denials

Deny Reasons	Description
Deny by Rule Service Mismatch	A rule with the 'DENY on Service Mismatch' option selected, matched and resulted into a deny action.
Deny by Rule Source Mismatch	A rule with the 'DENY on Source Mismatch' option selected, matched and resulted into a deny action.
Deny by Rule Time Mismatch	A rule with the 'DENY on Time Mismatch' option selected, matched and resulted into a deny action due to the mismatch in time.
Deny Local Loop	A passing rule matched, but the destination is a local system IP address. Targeted local IP addresses must be redirected.
Deny No Address Translation possible	The matching rule contains a address translation table which does not specify how to translate the particular source IP address.

### 6.3.3.2 Block Reasons

**Table 4-16** Reasons for connection blocks

Block Reasons	Description
Block Broadcast	Broadcasts are not propagated.
Block by Dynamic Rule	The session request was matched by a dynamic rule, which is set to be blocked.
Block by Rule	A rule blocks a session request explicitly.
Block by Rule Destination Mismatch	A rule with the 'BLOCK on Destination Mismatch' option selected, matched and resulted into a blocking action.
Block by Rule Interface Mismatch	A rule with the 'BLOCK on Interface Mismatch' option selected, matched and resulted into a blocking action due to the mismatch in time.
Block by Rule Service Mismatch	A rule with the 'BLOCK on Service Mismatch' option selected, matched and resulted into a blocking action.
Block by Rule Source Mismatch	A rule with the 'BLOCK on Source Mismatch' option selected, matched and resulted into a blocking action.
Block by Rule Time Mismatch	A rule with the 'BLOCK on Time Mismatch' option selected, matched and resulted into a blocking action due to the mismatch in time.
Block Echo Session Limit Exceeded	The number of total Echo sessions was exceeded for a request.
Block Local Loop	A passing rule matched, but the destination is a local system IP address. Targeted local IP addresses must be redirected. Use action type 'Local Redirect' for IP redirection to a local IP.
Block Multicast	Multicasts are not propagated.
Block No Address Translation possible	The matching rule contains a address translation table which does not specify how to translate the particular source IP address.
Block no Rule Match	No rule matched for the requested session. The default action is to block the request.
Block Other Session Limit Exceeded	The number of total OTHER protocol sessions was exceeded for a request.
Block Pending Session Limit Exceeded	The source IP address has to many pending sessions. Further request which would lead to more pending sessions are blocked.
Block Rule Limit Exceeded	The total number of allowed session for the matched rule was exceeded.
Block Rule Source Limit Exceeded	The number of allowed session per source IP address for the matched rule was exceeded.
Block Size Limit Exceeded	A packet which exceeds the specified size limit (for ICMP-Echo) was received.
Block Source Echo Session Limit Exceeded	The number of total ECHO sessions per source IP was exceeded for a request.
Block Source Session Limit Exceeded	The number of total sessions per source IP was exceeded for a request.
Block UDP Session Limit Exceeded	The number of total UDP sessions was exceeded for a request.
Forwarding is disabled	A forwarding firewall service does not exist or is inactive.

### 6.3.3.3 Drop Reasons

**Table 4-17** Reasons for connection drops

Drop Reasons	Description
Forwarding not Active	A packet could be assigned to an active session, but the forwarding firewall service is block resulting into temporarily dropping all forwarding traffic.
ICMP Header Checksum is Invalid	The ICMP header checksum did not verify
ICMP Header is Incomplete	The ICMP header of the packet is shorter that the minimum ICMP header length (8 bytes) or shorter than the indicated ICMP header length.
ICMP Packet is Ignored	An ICMP packet contains a type other than UNREACHABLE or TIME_EXCEEDED and is ignored.
ICMP Reply Without a Request	A ICMP-Echo-Reply packet was received by no associated Echo session was found.
ICMP Type is Invalid	The ICMP header contained an unknown ICMP type.
IP Header Checksum is Invalid	The IP header checksum did not verify.
IP Header Contains Source Routing	The source routing IP option is set.
IP Header has Invalid IP Options	The IP option encoding is malformed or contains unknown IP options.
IP Header is Incomplete	The packet is shorter than the minimum IP header length (20 bytes) or shorter than the indicated header length.
IP Header Version is Invalid	The IP version is different than 4.
IP Packet is Incomplete	The packet is smaller that the indicated total packet length.
No socket for packet	An outgoing TCP or UDP packet could not be assigned to an active socket on the system (RAW socket sending)
Packet Belongs to no Active Session	A received ICMP could not be assigned to a active session and is therefore dropped.
Rate Limit Exceeded	A Echo-Request packet could be assigned to an existing Echo session but was found to result into a too fast request rate.
Reverse Routing Interface Mismatch	The reverse routing path differs from the path the packet was received. (Receiving interface differs from sending interface) IP-Spoofing protection.
Size Limit Exceeded	A Echo-Request/Reply packet could be assigned to an existing Echo session but was found to exceed the configured size limit.
Source is an Invalid IP Class	IP addresses 240-255.x.x.x are not allowed
Source is Broadcast	The source address is a broadcast address
Source is Local Address	The source address is an IP address which is active on the local system and therefore not expected as a sender address.
Source is Loopback	The source address is a loopback address 127.x.x.x
Source is Multicast	The source address is a multicast address
TCP Header Checksum is Invalid	The TCP header checksum did not verify.
TCP Header has Invalid TCP FLAGS	TCP header contains useless combinations of TCP flags (SYN+RST, SYN+FIN).
TCP Header has Invalid TCP Options	TCP options encoding is malformed.
TCP Header is Incomplete	The TCP header of the packet is shorter that the minimum TCP header length (20 bytes) or shorter than the indicated TCP header length.
TCP Packet Belongs to no Active Session	A received TCP packet could not be assigned to an active TCP session and is not an initial TCP packet (SYN packet).
UDP Header Checksum is Invalid	The UDP header checksum did not verify.

**Table 4-17** Reasons for connection drops

Drop Reasons	Description
UDP Header is Incomplete	The UDP header of the packet is shorter than the minimum UDP header length (8 bytes) or shorter than the indicated UDP header length.
Unknown ARP Operation	The 'operation' field for an ARP packet is either a request nor a reply.
Session Creation Load Exceeded	A packet, triggering a new session evaluation, was dropped, because the actual CPU usage for session creation/evaluation has exceeded its limit.

### 6.3.3.4 Fail Reasons

**Table 4-18** Reasons for connection failures

Fail Reason	Description
Accept Timeout	The accept timeout for TCP session establishment was exceeded (TCP only). Possible IP spoofing attempt.
Connect Timeout	The connection timeout for TCP session establishment was exceeded (TCP only). The destination IP address was found not to be reachable.
Denied by Filter	A next hop denied forwarding by a filter rule.
Fragmentation Needed	The destination cannot be reached with the used MTU size without fragmentation. Only occurs if Path-MTU-Discovery is used by the source or the destination.
Host Access Denied	Access to the destination address was denied by on of the next hops.
Host Unreachable	The destination is accessed through a direct route but does not respond to an ARP request.
Host Unreachable for TOS	The requested IP address is not reachable for the used Type of Service.
Network Access Denied	Access to the destination network was denied by on of the next hops.
Network Unreachable	The network for the destination of a request is not reachable (No routing entry on one of the next hops)
Network Unreachable for TOS	The requested network is not reachable for the used Type of Service.
No Route to Host	The local system has no routing entry for the requested destination.
Port Unreachable	The destination system does not service the requested port number.
Protocol Unreachable	The destination system does not support the requested protocol.
Routing Triangle	Happens if a SYN followed by an ACK is registered without a SYN-ACK of the destination. This is an indication of a triangle route in the network.
Source Route Failed	Source Routing was requested but could not be performed. Will not occur, since source routed packets are dropped.
Unknown Network Error	Default network error

## 6.4 Authenticated User

This tab provides information concerning Firewall Authentication (see 10.3 Monitoring, page 192).

## 6.5 Dynamic Rules and Data

The **Dynamic** tab of the firewall GUI is the part where information about dynamic processes within the rule set lives.

There are mainly three things which happen dynamically during normal operation, counting of protected IPs, redirection, and dynamic rule activation.



To refresh the displayed information, click the **Update List** button.

### 6.5.1 Dynamic Rules

This tab provides information about use of dynamic rules and network objects of type **Hostname** (see 2.2.4.1 Hostname (DNS Resolvable) Network Objects, page 141).

Data regarding use of dynamic rules is arranged in the following columns in the upper section of the tab:

**Table 4-19** Columns available in the upper section of the Dynamic Rules tab

Column	Description
Rule	Icon visualising the rule status (inactive  ; active  ) and the name of the dynamic rule.
Status	Current state of the rule ( <b>Disabled</b> - inactive; <b>Enabled</b> - active).
Expires	Interval until the current state expires.
Expire Action	Action that is taken as soon as the dynamic activation expires.

Data regarding **Hostname** network objects is arranged in the following columns in the lower section of the tab:

**Table 4-20** Columns available in the lower section of the Dynamic Rules tab

Column	Description
Index	Progressional ID number of the <b>Hostname</b> network object. The index number is determined by the combination of the <b>Max. DNS Entries</b> value (page 127) and the percental breakdown of DNS queries allowed for network objects in use by the local and forwarding firewall rule sets. Index numbers start with <b>0</b> for network objects used by the forwarding firewall. The initial index number for network objects used in the local firewall is 75 % of the Max. DNS Entries value, that is <b>384</b> with the default of <b>512</b> Max. DNS Entries configured. <b>Note:</b> Keep in mind that MC-administered boxes inherit global, cluster- and range-specific Hostname objects. These objects are automatically added to the memory space of the forwarding firewall rule set.
DNS Name	DNS resolvable host name configured in the network object.
Status	Current state of the network object. The following states are available: <b>New</b> , <b>Pending</b> , <b>Resolved</b> .
Addresses	Result of the DSN query.
Last Update	Time that has passed since the currently active DNS entry was last retrieved by the netfence gateway.
Lifetime	Lifetime that is configured in the network object.

#### Note:

To update the DNS resolution of currently used network objects manually, select one or multiple list entries, then right-click and then click **Refresh selected DNS entries** in the context menu.

### 6.5.2 Protected IPs

This tab provides information concerning the number of active licensed IPs (so-called protected IPs).

The firewall license contains a parameter that limits the number of IP addresses that are "protected" by the firewall. For licensing see page 509. To monitor the number of protected addresses the firewall has a count algorithm that defines which addresses are to be considered as a protected address.

The firewall enters a valid IP address into the list of protected IPs as soon as network activity occurs. Once an



address is entered, but no network activity occurs for that particular address for more than an hour, the address will be set to obsolete and does not count as protected address any more. Periodic checking of the status of protected IPs happens every 30 minutes. Thus it may occur that IP addresses are counted as active for up to 1 hour and 30 minutes.

Clicking the **Update List** button reloads the display.

To the right of the **Update List** button, general info concerning the license of your netfence gateway is shown.

The following columns are available:

**Table 4-21** Columns in the protected IPs tab

Column	Description
ID	Icon visualising the protected IP status (obsolete  , licensed  ) and a progressional ID number.
Status	Status of each protected IP address ( <i>licensed</i> or <i>obsolete</i> ).
Last	Expired time since the IP address was counted the last time.
Address	Address of the protected IP.

### 6.5.3 Dynamic Services

This tab provides information concerning protected IPs and is used in conjunction with ONCRPC (see 11. RPC, page 193 and 11.4 Monitoring, page 198).

### 6.5.4 Redirect Availability

Redirecting an address to many others on a cycle or fallback policy is a dynamic process. The firewall decides on the fly what to do if one or more target addresses are not available.

The state of such rules is displayed here and uses the following columns:

**Table 4-22** Rule state overview

Column	Description
Rule	Name of the rule.
Address	Target Address.
Used	Number of connection requests re-directed to target address.
Unreach Since	Time since the target is unavailable.
Last Retry	Time since last retry.
Count Retry	Number of retries since target was marked unavailable.
Bad Port	Unreachable port; important when the rule is sensitive on more than one critical port.

### 6.5.5 SIP

This tab provides information about voice media connections (**Voice over IP** - 5. Monitoring, page 362).

### 6.5.6 Bridging ARPs

This tab provides information about connections, which have been established over bridging interfaces (9.6.3 Visualisation, page 187).

## 6.6 Shaping

This tab provides information about enterprise traffic shaping. For details see Enterprise Shaping, Realtime Information, page 87.

## 6.7 Tracing Connections

Connection tracing is a powerful tool for firewall management. The phion firewall is able to record every data byte which takes its way through the firewall engine. This ability is most important to detect errors in network based applications fast, and thus a definite need for network administrators who have to deal with an ever changing environment.

Connection tracing is configurable in the following two ways:

- A current connection may be selected in the **Status** tab of the firewall monitoring GUI and monitored from the moment tracing is activated.
- Tracing conditions may be defined in the **Conditions** section within the **Trace** tab of the firewall monitoring GUI and monitored from the moment a corresponding connection is initiated.

### 6.7.1 Tracing of Active Connections

In the **Status** tab of the firewall control window you can select a set of active connections and press the right mouse button and select Toggle Trace. From that moment on the selected connections are traced and you will be able to see all data transferred within these connections in the trace view.

The traced connections get an additional -Trace entry in the **Org** column.

To stop tracing simply select the traced connections and press the right mouse button and select Toggle Trace again.

### 6.7.2 Tracing of Connections Matching Defined Conditions

In the upper left part of the trace view window precise conditions can be defined under which a connection will be traced.

**Attention:**  
If you choose the tracing conditions too general, you will suffer a decrease in performance. Furthermore, it will be very difficult to find the connection you actually need to trace.

**Note:**  
Tracing conditions are only evaluated if the so-called **User space rule set** is used. Thus tracing conditions are only available if the parameter **Use Kernel Rule Set** is set to **no**, see 2.1.1.4 Operational, page 128).

**Note:**

Trace conditions are only evaluated for forwarding firewall traffic. Thus trace conditions cannot be applied for local traffic.

Tracing of local traffic is only available for active connections (see above).

**Note:**

The introduction of a new trace condition has no effect on already established sessions.

**Table 4-23** Possible tracing conditions

Column	Description
Rule	Name of the rule to be traced.
Source Address	IP address of the source; single IPs or netmasks allowed.
Source Port	Port of the source address.
Destination Address	IP address of the destination; single IPs or netmasks allowed.
Destination Port	Port of the destination address.
Maximum Counts	Only the first n packets are recorded. 0 is the service default, which can be set in the firewall service parameters. The default is 512.
Maximum Bytes	Only the first n kilobytes are recorded. 0 is the service default, which can be set in the firewall service parameters. The default is 256 KB.
Active	You can keep a list of predefined trace conditions and switch them on/off by settings this flag.

### 6.7.3 Tracing Window

On the left side is the list of all available tracing sessions.

The notion is

rule\_sourceIP\_sourcePORT\_destIP\_destPORT.dbg.

The corresponding files are located in `/var/phion/debug/trans`.

The maximum number of recorded tracing sessions can be set in the firewall basic configuration. The default is 512.

Double-clicking on a trace session opens the session in the right hand side. The connection traffic is depicted in the following style:

- Green: Data sent by source
- Blue: Data sent by destination
- Yellow: Messages from firewall (closing of connections)

The following checkboxes are used for filtering the view:

- **Binary**  
Show traffic in binary notation
- **Text**  
Show traffic in text notation
- **Source**  
Show traffic generated by source
- **Destination**  
Show traffic generated by destination
- **Header**  
Show traffic header

#### ➤ **Header Info**

Show header information

**Note:**

The depicted time stamp is that of the firewall system time in the time zone of the phion.a computer. If, for example, the firewall is on UTC and your workstation is on Central European Summer Time you will get the system time of the firewall +2 hours.

## 6.8 Audit Log

The Firewall Audit service may be activated on every netfence box without additional licensing. You need to activate the generation of Firewall Audit data within the configuration dialogue **Box > Infrastructure Services > General Firewall Configuration > Reporting > Audit Info Generation > Settings** by setting the parameter **Audit Delivery** to **Local File**.

Firewall Audit data is by default stored locally, but may be forwarded to the management centre or to separate netfence boxes running the Firewall Audit Service for central collection.

More information about provided functionality is available in **phion management centre - 12.MC Firewall Audit Viewer**, page 457.



## 7. Firewall Rule Sets

### 7.1 Direct Modification and Activation

Beside the standard way via the configuration tool it is possible to edit a firewall rule set directly within the operative firewall GUI. This is not allowed if the system is managed by a management centre.

Firewall rule sets are standard ASCII files and can be exported and imported. The configuration engine, however, checks whether the rule set to activate originates from the active one or not. This check is not performed during the standard configuration process.

## 8. Log Files

The firewall service generates several log files in `/var/phion/logs`.

As the firewall engine as well as a box service operates it logs into the box part of the log tree. This is the main log file.

In addition, it logs all to forwarding traffic related entries into a service specific log file.

All standard logs are in the main log file. Additionally administrative logs and logs regarding changes of the rule set are logged twice in separate log files.

### 8.1 Standard Log Files

- `box_Firewall.log`  
Main log file. All log entries are in this file. Information about tunnel and transport is only visualized on active kernel rule set.
- `srv_servername_servicename.log`  
Service log file. All forwarding rules related entries are in this file.
- `srv_servicename_rulename.log`  
Generated when own log file is chosen for a certain rule. All traffic is logged in the main log file and in this one.
- `srv_servername_servicename_Content.log`  
This log file contains all log entries created by the content filter (see 2.3.1 Content Filter (Intrusion Prevention), page 151).

## 9. Bridging

### 9.1 General

Bridging is commonly used to separate LAN segments in a flatly structured network. Bridging can easily be implemented into a network retroactively, if physical segmentation of a flat structure becomes necessary. Typical bridging application areas are commercial Internet services provider's environments, where physical segmentation of diverse customers' machines is necessary.

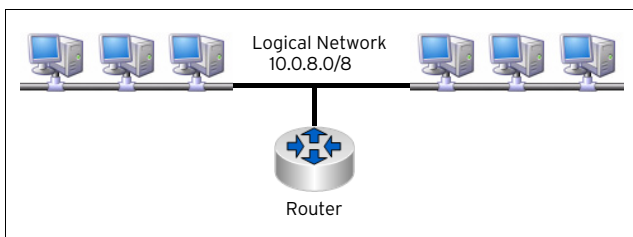
### 9.2 Bridging Goals and Benefits

The netfence bridging concept particularly aims at easy setup and configuration. One of its demands is to achieve stealth mode, that means nodes should not be aware of any active bridging involved.

The following are the main benefits of netfence bridging:

- Bridging allows for physical segmentation of network nodes within a logical network.
- There is no need for client configuration change.
- Full network transparency (down to Layer 2) can be achieved.
- Firewalling can be implemented between LAN segments.

Fig. 4-74 Flat network structure before segmentation



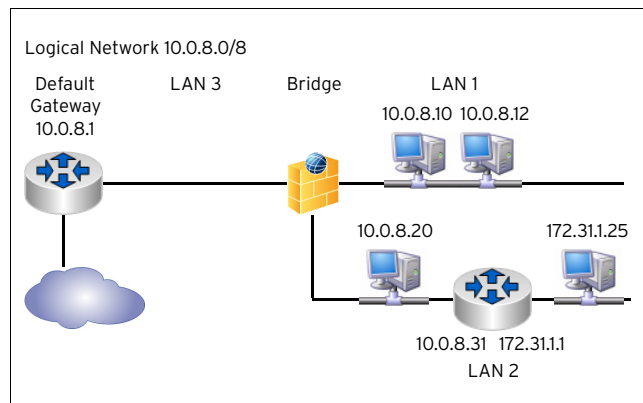
### 9.3 Bridging Methods

#### 9.3.1 Transparent Layer2 Bridging

Transparent Layer2 Bridging can be implemented best in a network with already existing and configured routers where only a few networks are to be separated. The following are the main characteristics of Transparent Layer2 Bridging:

- The bridging interface carries no IP address. It is thus not visible to other interfaces and as a result not vulnerable.
- All network traffic is delivered using Layer 2 lookups.
- Bridging is Layer 2 transparent, which means that the source MAC is propagated in connection requests.
- The bridged network nodes cannot locally communicate with the interface.
- A Transparent Layer2 Bridge requires a separate interface making it accessible for configuration.

Fig. 4-75 Network segmentation in a Transparent Layer2 bridged environment



The configuration example is described in detail at the end of this chapter (see 9.6.2.1 Using Transparent Layer2 Bridging, page 184).

#### 9.3.2 Routed Transparent Layer2 Bridging

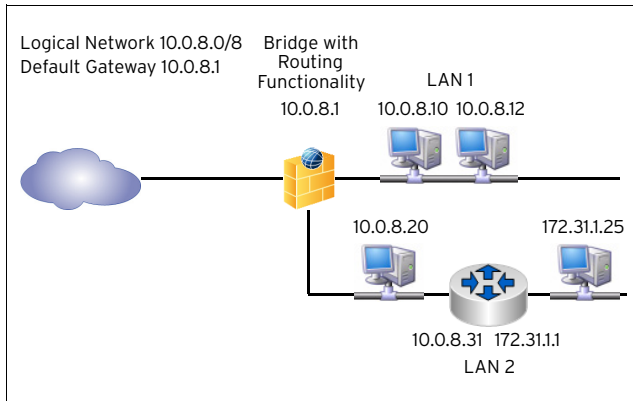
A Routed Transparent Layer2 Bridge is meant to be implemented in a network where the netfence, besides bridging functionality, may as well offer further functions. As the netfence by all means acts as a router, additional routers are no longer required. Beyond this, the bridging interfaces can be configured to use any other service installed on the netfence gateway.

The following are the main characteristics of Routed Transparent Layer2 Bridging:

- The bridging interface carries an IP address.
- Depending on source or destination, packets are delivered by either Layer 2 or Layer 3 lookup.

- Bridging is Layer 2 transparent, which means that the source MAP is propagated in connection requests.
- Unknown destinations are **actively** "ARPed".
- Traffic between routed and bridged destinations is forwarded.
- Bridged network nodes may (if allowed) locally communicate with the interface, which means that beside bridging other netfence services may be utilised simultaneously.

**Fig. 4-76** Network segmentation in a Routed Transparent Layer2 bridged environment



The configuration example is described in detail at the end of this chapter (see 9.6.2.3 Using Routed Transparent Layer2 Bridging - Example 2, page 185).

### 9.3.3 Layer3 Bridging

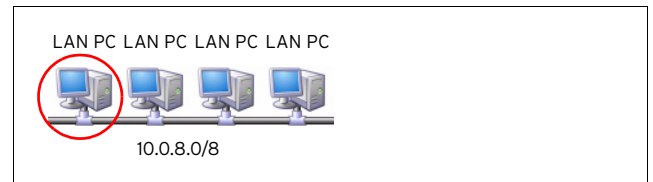
Layer3 Bridging works best with client/server groups, which seldom communicate with other machines than the ones belonging to their own group. It is easy and quick to configure, if only few clients are involved. The more clients the bridge has to serve the more time-consuming the configuration gets, as bridging and routing have to be configured for each client explicitly. Depending on residual demands it is better to configure a (Routed) Transparent Layer2 Bridge instead, if many clients are involved.

The following are the main characteristics of Layer3 Bridging:

- Layer3 Bridging is implemented with Proxy ARPs and host/network routes.
- All network traffic is delivered using Layer 3 lookups.
- All bridged network nodes must be entered into the configuration.
- Bridging is NOT Layer 2 transparent, which means that the source MAC is not propagated in connection requests.
- Traffic between routed and bridged destinations is forwarded.
- Bridged network nodes may (if allowed) locally communicate with the interface.

Figure 4-77 shows a common situation in which implementation of Non Transparent Translational Bridging would be appropriate.

**Fig. 4-77** Flat network structure

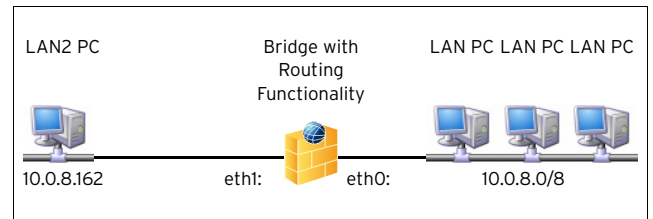


In the logical network 10.0.8.0/8 the encircled PC is to be detached from the other LAN PCs and protected by a firewall.

A possible approach to achieve this could be to define a new network (for example, 10.0.8.160/3) and place the PC inside this network. A firewall between the two networks could act as a router and as protective interface for the PC.

The disadvantage of such an approach is that network settings of all clients have to be modified. Through bridging implementation full security can be provided even in a flat network architecture, with only the need to change network settings on the client, which is to be separated.

**Fig. 4-78** Non Transparent Translational Bridging



As depicted in figure 4-78, after separation the firewall acts as bridge between the networks 10.0.8.160/3 and 10.0.8.0/8.

All ARP requests transmitted between the networks 10.0.8.160/3 and 10.0.8.0/8 are answered by the firewall.

The configuration example is described in detail at the end of this chapter (see 9.6.2.4 Using Layer3 Bridging, page 186).

### 9.3.4 Bridging Characteristics in Comparison

**Table 4-24** Bridging characteristics in comparison

	Transparent Layer2 Bridging	Routed Transparent Layer2 Bridging	Layer3 Bridging
<b>Mac Transparent</b>	✓	✓	
<b>Routing-Bridging-Forwarding</b>		✓	✓
<b>Local Firewall Traffic (Gateway)</b>		✓	✓
<b>Auto Learning of Network Nodes</b>	✓	✓	
<b>Active Learning of Network Nodes</b>		✓	
<b>Next Hop Bridging</b>	✓	✓	
<b>Broad-Multicast Propagation</b>	✓	✓	✓
<b>High Availability</b>	✓	✓	✓
<b>VLAN capable</b>	✓	✓	✓

## 9.4 Security

Bridging heavily depends on broadcasts to establish connectivity. This behaviour leads to a few weak points, which have to be considered carefully, in order to implement bridging in a secure manner.

Apart from the factor that broadcasts in huge environments consume a lot of bandwidth, regard must be paid to the aspect that bridging is inherently insecure and therefore requires a trusted environment.

netfence gateway offers methods, which allow averting the most common attacks.

### 9.4.1 IP or ARP Spoofing

Network nodes may for example use IP addresses of fake ARP responses in order to fake network traffic with arbitrary IP addresses. Since the firewall security enforcement is performed on layer 3 this would correspond to bypassing the security policy. These issues can be solved by taking the following measures:

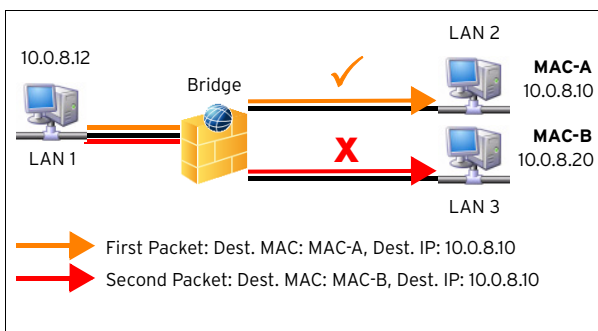
- **Segment Access Control Lists (Bridging Interface ACLs)**  
Specify allowed IP addresses on a segment explicitly.
- **Static Bridge ARP Entries**  
Specify IP, MAC, and segment statically to avoid learning via ARP.
- **MAC based Firewall Rules**  
Introduce source MAC conditions for network objects.
- **ARP Change reporting**  
Configure any changes of IP-MAC-Segment relationships to be reported in access cache and log.

### 9.4.2 Destination MAC Spoofing

Another security issue in bridged environments is the possible exploitation made available through security enforcement on layer 3 and traffic delivery on layer 2. This issue can be solved by taking the following measure:

- **Enforce layer 2 once a layer 3 session is granted**  
MAC addresses for a session are then fixated upon session creation and enforced until session end.

Fig. 4-79 Destination MAC spoofing prevention



In the situation depicted in figure 4-79, a client from LAN 1 tries to enforce a connection grant to a client in LAN 3. To do so, it sends a first packet to the client in LAN 2 using MAC-A as destination MAC and the IP address 10.0.8.10 as destination IP. After the session has been granted through the bridge and communication has been allowed, it sends a second packet to the client in LAN 3 using MAC-B as destination MAC and again IP address 10.0.8.10 as destination IP. It thus tries to spoof the destination MAC of its connection request. If MAC enforcement is configured, the communication to the client in LAN 3 will not be granted.

## 9.5 Implementation of Logical Entities

Table 4-25 Structural breakdown of bridging units

Bridging Groups	Bridging Interfaces	Bridging ARPs
Bridging Group <i>test</i>  phbr-test 10.0.8.1	eth1.123	00:02:34:56:77:88 eth1.123 10.0.8.20 10.0.7.50
	ACL 10.0.8.0/8 10.0.7.0/8	00:08:55:34:32:78 eth1.123 <b>STATIC</b> 10.0.8.22
	eth1.234	00:08:55:34:32:78 eth1.234
	eth3	00:12:55:66:21:71 eth3 10.0.8.30

### 9.5.1 Bridging Groups

A bridging group defines a set of network interfaces for which network traffic will be forwarded using bridging.

### 9.5.2 Bridging Interfaces

A bridging interface is a network interface that was assigned to a bridging group and is therefore subject to bridged traffic forwarding between bridging interfaces.

**Note:**

A bridging interface can only be member of one bridging group.

### 9.5.3 Bridging ARP Entries

A bridging ARP entry (BARP) stores the information on which bridge interface a certain MAC address resides. Additionally, associated IP addresses are stored along with the BARP entry.

**Note:**

The IP address is only used for visualisation purposes.

### 9.5.3.1 Dynamic BARPs

Dynamic BARPs are build up during run time by analysing network traffic. Whenever a packet is received on an interface, dynamic BARPs are generated or updated. This way the firewall "learns", which MAC address resides on which bridging interface. When analysing ARP packets the Layer 3 IP information is added to the BARP entry by adding the IP address.

Dynamic BARPs are characterised by the following activities:

- MAC-Interface relationship learned by any IP traffic
- MAC-Interface-IP relationship learned by ARP traffic

### 9.5.3.2 Static BARPs

Static BARPs are part of the configuration and define a MAC-Interface-IP relationship that is present at all time and will not be overwritten by "learning" from traffic.

## 9.5.4 Bridging Interface ACL

The Bridging Interface ACL (Access Control List) specifies which IP addresses are expected to be received on a bridging interface. These ACLs can be used to enforce a Layer 3 topology when operating on the firewall. The most restrictive implementation would be to maintain a list of single IP addresses that are to be expected on a certain bridge interface.

## 9.5.5 Virtual Bridge Interface

The virtual bridge interface is an interface that acts as parent interface for all interfaces of a bridging group. The name of a virtual interface is always the name of the bridging group with a phbr- prefix:  
(phbr- <group-name>).

## 9.5.6 Virtual Bridge Interface IP Address

Optionally, each virtual bridge interface may be configured with an IP address and a netmask. This way the firewall itself can actively probe (learn) on which segments which MAC address resides. It can also route traffic from a routed network to a bridged network or between bridging groups. Through the introduction of a virtual bridge interface one switches from *Transparent Layer2* to *Routed Transparent Layer2 Bridging*.

The main characteristics a virtual bridge interface brings along are the following:

- Active ARP queueing
- Forwarding between bridge groups
- Forwarding between routed and bridged networks
- Local firewall traffic (application gateways)
- Still MAC transparent (like Transparent Layer2 Bridging)

## 9.5.7 Broad- and Multicast

Broad- and multicast can be forwarded between segments and routed networks. In order to allow broad- or multicast propagation a specific rule action must be chosen. Once a rule is introduced that explicitly allows such a propagation a list of

- Network interfaces
- IP addresses
- Multicast addresses

can be specified in order to define how the broad- or multicast should be propagated. Note that Broad- to Uni- or Multicast translations are possible.

A rule specified as below:

- Rule from 10.0.8.0/8 to 10.0.0.255 (ALL-UDP) Action Broad- Multicast
- Propagate 10.0.1.45, eth1.123, eth2.234, eth4:10.0.4.244, phbr-test, eth3:224.1.2.3

will result in the following propagation mechanisms:

- Unicast to 10.0.1.45
- Broadcast 10.0.8.255 on interface eth1.123
- Broadcast 10.0.8.255 on interface eth1.234
- Broadcast 10.0.4.255 on interface eth4
- Broadcast 10.0.8.255 on all bridge interfaces on bridge group phbr-test
- Multicast 224.1.2.3 on interface eth3

## 9.5.8 High Availability







Bridging ARPs are synchronised to the partner box along with the session synchronisation. Synchronised BARPs are inactive as long as no bridging group exists that indicates bridged forwarding. Upon activation (HA takeover) the bridging groups are introduced and all related BARP entries activated. Along with the activation a dummy ARP request is sent on all bridging interfaces except for the one the BARP resides on. This causes the MAC address to be entered into the MAC-Port Table of the switch.

Action elements of High Availability bridging scenarios are:

- Firewall session synchronisation
- BARP HA synchronisation
- Dummy ARP for switch MAC-Port update

## 9.6 Bridging Configuration

Bridging is set up through the following configuration areas:

- On single boxes in  **Config** >  **Box** >  **Virtual Servers** >  **Assigned Services** >  **Firewall** >  **Firewall Forwarding Settings** > **Bridging** tab
- On MC administered boxes in the MCs respective repository.



## 9.6.1 Bridging Tab

To realise Transparent Layer2 or Routed Transparent Layer2 Bridging, the setup is done through the Bridging tab of the Forwarding Firewall. Here the following parameters are available for configuration:

List 4-47 Firewall Forwarding Settings - Bridging - section Layer2 Bridging

Parameter	Description								
<b>Bridging Group</b>	Click the <b>Insert</b> button and insert a <b>Name</b> for a new Bridging Group. Select an available Bridging Group and click the <b>Edit</b> button to change settings. Click the <b>Delete</b> button to delete all selected entries irreversibly. Creation of a new Bridging Group opens a further configuration area allowing specification of <b>Bridging Devices</b> and <b>Device IP</b> addresses. <b>Note:</b> In the Firewall Access Cache, bridging groups are labelled with the letters <b>phbr</b> prefixed to the group name as specified.								
<b>Bridging Device</b>	All interfaces created in this place are the ones responsible for bridge traffic forwarding. A bridging interface is defined by the following parameters: <table border="1" data-bbox="271 806 686 1176"> <tr> <td><b>Name</b></td> <td>In this place the exact labelling of the network interface has to be entered as it is listed in the network configuration. If explicit interfaces are in use, the <b>Name</b> has to match the <b>Interface Name</b> (page 69) as defined in the <b>Section Additional Local Networks</b>, if VLANs are in use the <b>Name</b> has to be constructed to match the <b>Hosting Interface</b> and the <b>VLAN ID</b> (page 65) separated by a dot (for example eth1.5) as defined in the <b>Network - Virtual LANs Configuration - section Virtual LAN Configuration List 3-30</b>.</td> </tr> <tr> <td><b>Allowed Networks</b></td> <td>The value of this parameter consists of all networks, which are allowed to communicate over this Bridging Device. The values specified can be complete networks, individual client/server IP addresses or network ranges.</td> </tr> <tr> <td><b>MAC Change Allowed</b></td> <td>This setting specifies, if network interfaces participating in a bridging group may change. A very restrictive policy will <b>Deny-MAC-Change</b> a less restrictive policy should <b>Allow-MAC-Change</b> (default).</td> </tr> <tr> <td><b>Comment</b></td> <td>Entering a comment is optional but useful for quicker orientation when many bridging interfaces are in use.</td> </tr> </table>	<b>Name</b>	In this place the exact labelling of the network interface has to be entered as it is listed in the network configuration. If explicit interfaces are in use, the <b>Name</b> has to match the <b>Interface Name</b> (page 69) as defined in the <b>Section Additional Local Networks</b> , if VLANs are in use the <b>Name</b> has to be constructed to match the <b>Hosting Interface</b> and the <b>VLAN ID</b> (page 65) separated by a dot (for example eth1.5) as defined in the <b>Network - Virtual LANs Configuration - section Virtual LAN Configuration List 3-30</b> .	<b>Allowed Networks</b>	The value of this parameter consists of all networks, which are allowed to communicate over this Bridging Device. The values specified can be complete networks, individual client/server IP addresses or network ranges.	<b>MAC Change Allowed</b>	This setting specifies, if network interfaces participating in a bridging group may change. A very restrictive policy will <b>Deny-MAC-Change</b> a less restrictive policy should <b>Allow-MAC-Change</b> (default).	<b>Comment</b>	Entering a comment is optional but useful for quicker orientation when many bridging interfaces are in use.
<b>Name</b>	In this place the exact labelling of the network interface has to be entered as it is listed in the network configuration. If explicit interfaces are in use, the <b>Name</b> has to match the <b>Interface Name</b> (page 69) as defined in the <b>Section Additional Local Networks</b> , if VLANs are in use the <b>Name</b> has to be constructed to match the <b>Hosting Interface</b> and the <b>VLAN ID</b> (page 65) separated by a dot (for example eth1.5) as defined in the <b>Network - Virtual LANs Configuration - section Virtual LAN Configuration List 3-30</b> .								
<b>Allowed Networks</b>	The value of this parameter consists of all networks, which are allowed to communicate over this Bridging Device. The values specified can be complete networks, individual client/server IP addresses or network ranges.								
<b>MAC Change Allowed</b>	This setting specifies, if network interfaces participating in a bridging group may change. A very restrictive policy will <b>Deny-MAC-Change</b> a less restrictive policy should <b>Allow-MAC-Change</b> (default).								
<b>Comment</b>	Entering a comment is optional but useful for quicker orientation when many bridging interfaces are in use.								
<b>Device IP Address</b>	<table border="1" data-bbox="271 1579 686 1713"> <tr> <td><b>Device IP Address</b></td> <td rowspan="2">This parameter takes one or multiple IP addresses that are to be assigned to a bridging group. Each entry is built up of the <b>Device IP Address</b> and its <b>IP Netmask</b>.</td> </tr> <tr> <td><b>IP Netmask</b></td> </tr> </table> <p><b>Note:</b> If the Device IP Address field is left empty, the Bridging Device is configured not to carry an IP address and thus <b>Transparent Layer2 Bridging</b> is configured. As soon as the Bridging Device IP is specified <b>Routed Transparent Layer2 Bridging</b> has been realised.</p>	<b>Device IP Address</b>	This parameter takes one or multiple IP addresses that are to be assigned to a bridging group. Each entry is built up of the <b>Device IP Address</b> and its <b>IP Netmask</b> .	<b>IP Netmask</b>					
<b>Device IP Address</b>	This parameter takes one or multiple IP addresses that are to be assigned to a bridging group. Each entry is built up of the <b>Device IP Address</b> and its <b>IP Netmask</b> .								
<b>IP Netmask</b>									
<b>Use IP BARP Entries</b>	This parameter controls generation of IP entries for all bridging ARP entries within a Bridging Group. When set to <b>yes</b> (default), the netfence gateway does not only learn the allocation of MAC addresses to ports from processed IP and ARP traffic, but also records IP addresses that are assigned to a specific MAC address in a separate table. Set to <b>no</b> , if a huge number of IP addresses within a specific network segment might cause an ARP table overrun.								

List 4-47 Firewall Forwarding Settings - Bridging - section Layer2 Bridging

Parameter	Description								
<b>Static Bridge MAC</b>	This configuration area may be used for statical MAC/IP address combination to minimise the risk of IP/ARP or Destination MAC Spoofing (see above). <table border="1" data-bbox="909 347 1444 638"> <tr> <td><b>Static Bridge MAC</b></td> <td>The expected MAC address of the external interface is set here.</td> </tr> <tr> <td><b>Device</b></td> <td>This is the name of the bridging interface through which the connection request is expected to be handled.</td> </tr> <tr> <td><b>IP Address</b></td> <td>This is the IP address of the external interface bound to the Static Bridge MAC specified before.</td> </tr> <tr> <td><b>Comment</b></td> <td>Entering a comment is optional but useful for quicker orientation when many statical entries are in use.</td> </tr> </table>	<b>Static Bridge MAC</b>	The expected MAC address of the external interface is set here.	<b>Device</b>	This is the name of the bridging interface through which the connection request is expected to be handled.	<b>IP Address</b>	This is the IP address of the external interface bound to the Static Bridge MAC specified before.	<b>Comment</b>	Entering a comment is optional but useful for quicker orientation when many statical entries are in use.
<b>Static Bridge MAC</b>	The expected MAC address of the external interface is set here.								
<b>Device</b>	This is the name of the bridging interface through which the connection request is expected to be handled.								
<b>IP Address</b>	This is the IP address of the external interface bound to the Static Bridge MAC specified before.								
<b>Comment</b>	Entering a comment is optional but useful for quicker orientation when many statical entries are in use.								
<b>Bridging TTL Policy</b>	This parameter controls the bridge's handling of the TTL field in the header of an IP packet. The following options are available: <ul style="list-style-type: none"> <li>➤ <b>Decrease-TTL</b> (default) The TTL value is decreased by 1 every time a packet arrives anew. When the TTL value reaches 0, the packet is dropped.</li> <li>➤ <b>Do-NOT-Decrease-TTL</b> The TTL value remains unchanged.</li> </ul>								

List 4-48 Firewall Forwarding Settings - Bridging - section Quarantine Bridging

Parameter	Description
<b>Quarantine Group</b>	To edit an already existing entry, select it and click <b>Edit...</b> To create a new entry, click <b>Insert</b> . To remove an existing entry, select it and click <b>Delete</b> . See list 4-49 for parameter description.

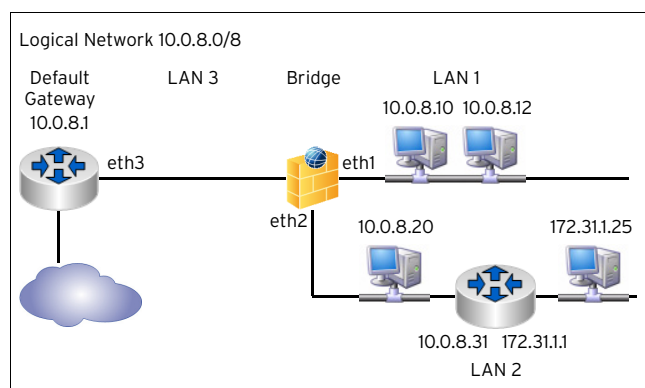
List 4-49 Firewall Forwarding Settings - Bridging - section Quarantine Bridging- Quarantine Group

Parameter	Description
<b>Disable Quarantine Group</b>	Disables this quarantine group. Use this to quickly deactivate a fully configured quarantine group.
<b>Quarantine Class 1 Interface</b>	Specifies one interface, where all quarantine class 1 clients will be located. This interface must not already be member of any other quarantine group.
<b>Quarantine Class 2 Interface</b>	Specifies one interface, where all quarantine class 2 clients will be located. This interface must not already be member of any other quarantine group.
<b>Quarantine Class 3 Interface</b>	Specifies one interface, where all quarantine class 3 clients will be located. This interface must not already be member of any other quarantine group.
<b>LAN Interfaces</b>	A list of interfaces where clients live. These clients may change their state to a quarantine class which is located on one of the above quarantine class interfaces.

## 9.6.2 Example Configurations

### 9.6.2.1 Using Transparent Layer2 Bridging

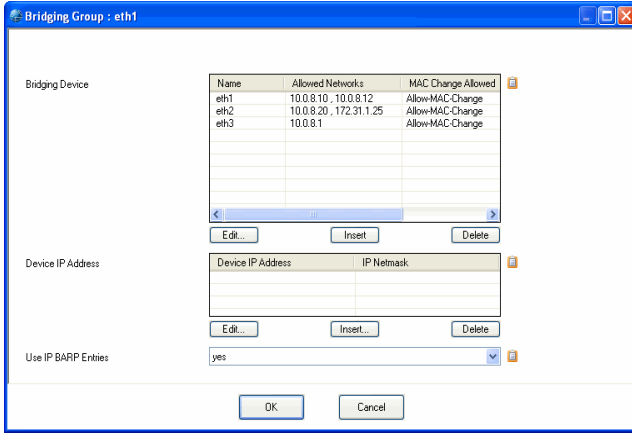
Fig. 4-80 Configuration of Transparent Layer2 Bridging



The realisation of Transparent Layer2 Bridging as depicted in the example above requires the following configuration settings:

In **Firewall Forwarding Settings > Bridging**.

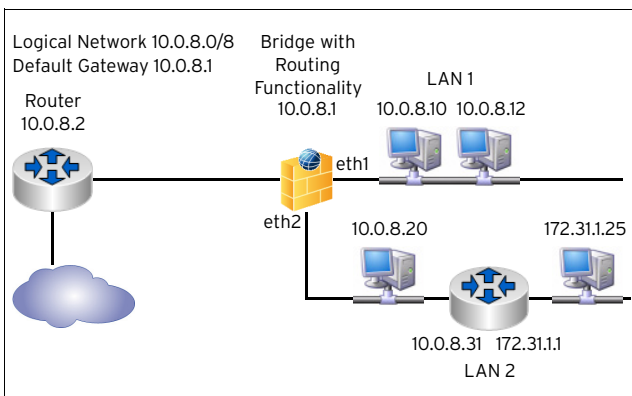
**Fig. 4-81** Bridging Group Setup for Transparent Layer2 Bridging



- Define a **Bridging Group**.
- Add the **Bridging Devices** eth1, eth2, and eth3 to the Bridging Group.
- Add network 10.0.8.0/8 or the two clients 10.0.8.10 and 10.0.8.12 individually to the **Allowed Networks** parameter of Bridging Device **eth1**.
- Add network 10.0.8.0/8 or the client 10.0.8.20 individually to the **Allowed Networks** parameter of Bridging Device **eth2**.
- Add the default gateway 10.0.8.1 to the **Allowed Networks** parameter of Bridging Device **eth3**.
- If you desire the client 173.31.1.25 to be reachable from clients in **LAN1**, add it to the **Allowed Networks** parameter of Bridging Device **eth2**. No further configuration is necessary to guarantee reachability between the clients 10.0.8.0.20 and 172.31.1.25.
- The **Device IP Address** of the Bridging Group does not have to be configured, as an external router (Default Gateway 10.0.8.1) already exists.

### 9.6.2.2 Using Routed Transparent Layer2 Bridging - Example 1

**Fig. 4-82** Configuration of Transparent Layer2 Bridging



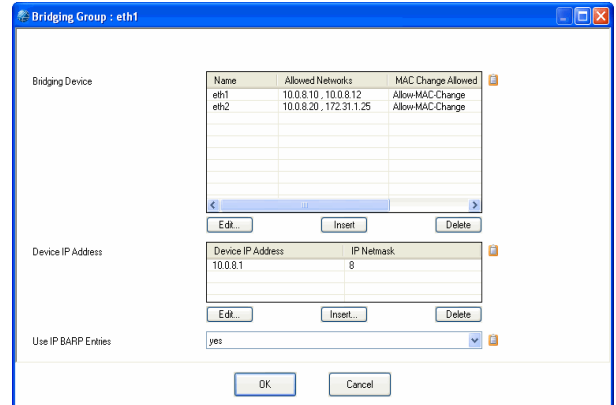
In figure 4-82 a similar network setup has been realised like in figure 4-80, page 184 with one main difference,

though - the bridge has been set up with routing functionality. Clients in LAN1 and LAN2 may now profit from being able to locally communicate with the bridging devices.

The realisation of Routed Transparent Layer2 Bridging as depicted in the example above requires the following configuration settings:

In **Firewall Forwarding Settings > Bridging**.

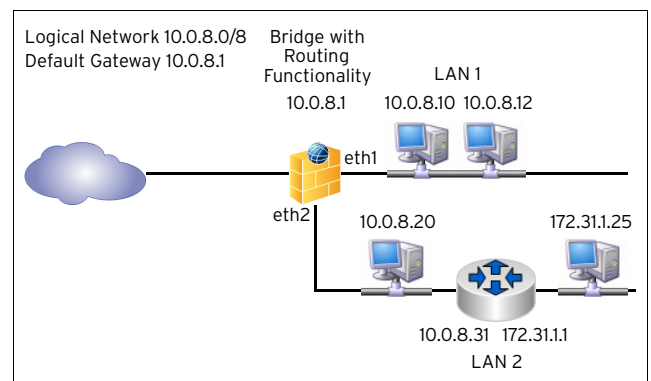
**Fig. 4-83** Bridging Group Setup for Routed Transparent Layer2 Bridging - Example 1



- Define a **Bridging Group**.
- Add the **Bridging Devices** eth1 and eth2 to the Bridging Group.
- Add network 10.0.8.0/8 or the two clients 10.0.8.10 and 10.0.8.12 individually to the **Allowed Networks** parameter of Bridging Device **eth1**.
- Add network 10.0.8.0/8 or the client 10.0.8.20 individually to the **Allowed Networks** parameter of Bridging Device **eth2**.
- If you desire the client 173.31.1.25 to be reachable from clients in **LAN1**, add it to the **Allowed Networks** parameter of Bridging Device **eth2**. No further configuration is necessary to guarantee reachability between the clients 10.0.8.0.20 and 172.31.1.25.
- Configure the Default Gateway address 10.0.8.1 as **Device IP Address** of the Bridging Group.

### 9.6.2.3 Using Routed Transparent Layer2 Bridging - Example 2

**Fig. 4-84** Configuration of Routed Transparent Layer2 Bridging

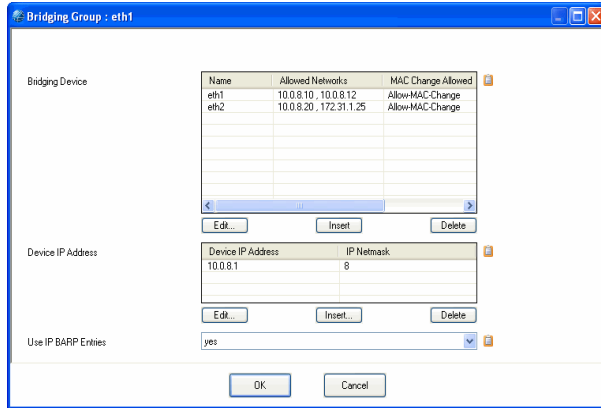


In the configuration example depicted in figure 4-84 introduction of a Device IP address is a must as not further

router exists. The realisation of the setup requires the following configuration settings:

In **Firewall Forwarding Settings > Bridging**.

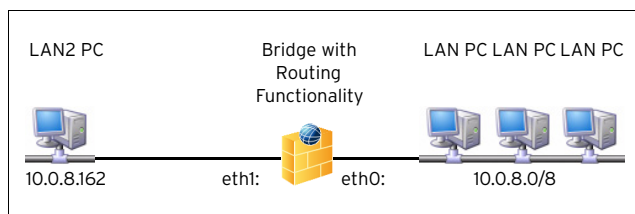
Fig. 4-85 Bridging Group Setup for Routed Transparent Layer2 Bridging



- Define a **Bridging Group**.
- Add the **Bridging Devices** eth1 and eth2 to the Bridging Group.
- Add network 10.0.8.0/8 or the two clients 10.0.8.10 and 10.0.8.12 individually to the **Allowed Networks** parameter of Bridging Device **eth1**.
- Add network 10.0.8.0/8 or the client 10.0.8.20 individually to the **Allowed Networks** parameter of Bridging Device **eth2**.
- If you desire the client 173.31.1.25 to be reachable from clients in **LAN1**, add it to the **Allowed Networks** parameter of Bridging Device **eth2**. No further configuration is necessary to guarantee reachability between the clients 10.0.8.0.20 and 172.31.1.25.
- Add the default gateway 10.0.8.2 to the **Allowed Networks** parameter of Bridging Device **eth3**
- Configure the Default Gateway address 10.0.8.1 as **Device IP Address** of the Bridging Group.

### 9.6.2.4 Using Layer3 Bridging

Fig. 4-86 Configuration of Non Transparent Translational Bridging

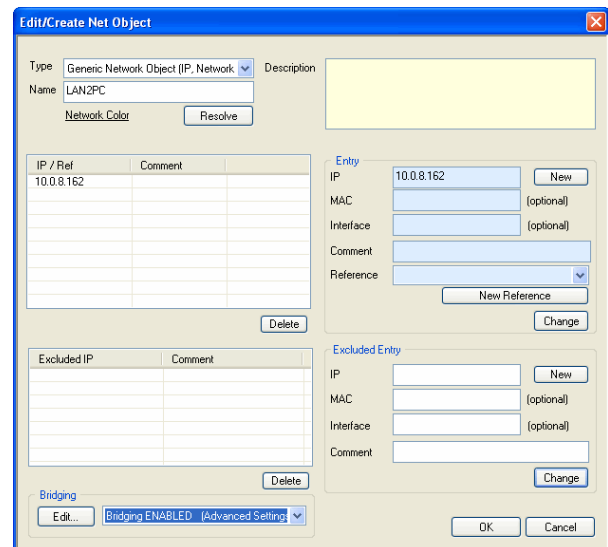


The realisation of non transparent translational bridging as depicted in the example above requires the following configuration settings:

In the **Networks** tab of the **Rules** configuration area of the **Forwarding Firewall**.

- Create a new **Net Object** for LAN2 PC. Enter LAN2 PCs IP address 10.0.8.162 into the **IP/Ref** field of this Net Object.

Fig. 4-87 Net Object creation for LAN2 PC



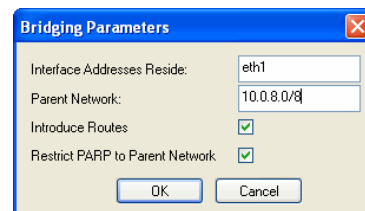
- Set parameter **Bridging** to **Bridging ENABLED (Advanced Settings)**.

#### Note:

See List 4-23 Net Object configuration parameters, section **Net Object configuration parameters - section Bridging**, page 141 for parameter configuration details.

- In the **Advanced Settings** window of the Bridging parameter enter the value **eth1** (the bridge's network interface pointing to LAN2 PC) into the **Device Addresses Reside** field.
- Enter network 10.0.8.0/8 into the **Parent Network** field.
- Activate checkboxes **Introduce Routes** and **Restrict PARP to Parent Network**.

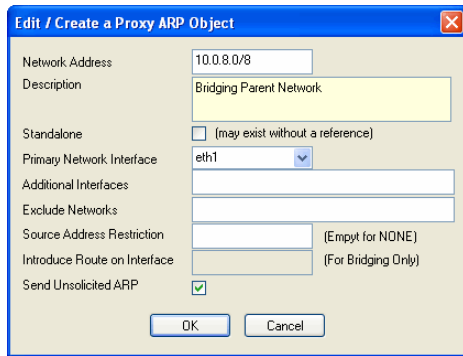
Fig. 4-88 Bridging Parameters configuration



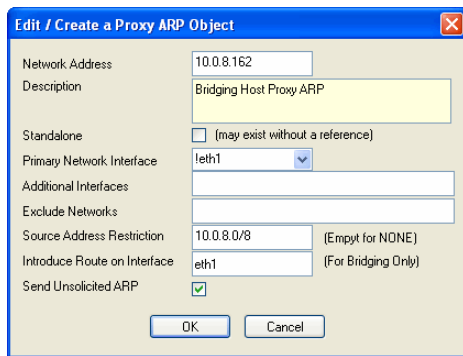
- Corresponding **ProxyARP Objects** ensuring that ARP requests are answered on the wanted interface are automatically generated when a Net Object with Bridging activated is created. Their references can be

viewed in the **Proxy ARPs** tab of the **Rules** configuration area:

**Fig. 4-89** Proxy ARP Object - Bridging Parent Network



**Fig. 4-90** Proxy ARP Object - Bridging Host Proxy ARP



For further information on Proxy ARP Objects see 2.2.9 Proxy ARPs, page 150.

### 9.6.3 Visualisation

**Fig. 4-91** Firewall > Dynamic > Bridging ARPs tab

MAC	Device	Group	IPs	Type	Timer
00:02:44:0e:c0:4d	eth1.18		10.0.3.65	dynamic	3d 17h 31m
00:02:44:48:fa:10	eth0.6		10.0.3.46	dynamic	1m 8s
00:02:55:fa:b0:98	eth0.6		10.0.3.102 10.0...	dynamic	6s
00:03:2d:05:59:5d	eth1.11		10.0.3.121	dynamic	1s
00:04:23:a7:f2:b0	eth1.11	dev	10.0.3.44	dynamic	3s
00:04:23:ae:d7:80	eth0.6		10.0.3.72 10.0.3...	dynamic	20m 31s
00:04:23:b0:78:f8	eth1.11		10.0.3.45(S)	static	0s
00:04:75:d0:3e:51	eth0.6	dev	10.0.3.99 10.0.3...	dynamic	0s
00:07:e9:08:00:00	eth0.6	dev		dynamic	7d 15h 35m
00:07:e9:08:fb:2a	eth0.6	dev	10.0.3.1	dynamic	0s
00:07:e9:09:04:30	eth0.6		192.168.99.4 19...	dynamic	20m 32s
00:0c:29:19:3f:ac	eth0.6		10.0.3.204 10.0...	dynamic	20h 12m 21s
00:0d:60:a1:65:7c	eth1.17		10.0.3.54	dynamic	0s
00:11:d8:c6:d9:14	eth1.18	dev	10.0.3.66	dynamic	12s

In the **Bridging ARPs** tab of the **Firewall** box menu entry (**Dynamic** tab > **Bridging ARPs** tab) all connections are recorded, which have been established over bridging devices.

Clicking the **Update List** button refreshes the list of entries.

Each row reports one connection establishment. The following columns are in use to detail it:

**Table 4-26** Overview of bridging operational information in the Bridging ARPs tab

Column	Description
<b>MAC</b>	This column displays the MAC address of the external interface which has established a connection to the bridging interface.

**Table 4-26** Overview of bridging operational information in the Bridging ARPs tab

Column	Description
<b>Interface</b>	This is the bridging interface through which the connection has been established.
<b>Group</b>	This is the name of the Bridging Group the interface belongs to.
<b>IPs</b>	The IPs recorded here belong to the MAC address displayed in the first column.
<b>Type</b>	The IPs bound to a MAC address are <b>dynamic</b> if they have been learned dynamically through proxy ARPing. The type is static, if the MAC/IP combination documented through the other columns has been configured statically through the parameter <b>Static Bridge MAC</b> (list 4-47, page 184).
<b>Timer</b>	This is the time interval, which has passed, since the connection establishment has been recorded.

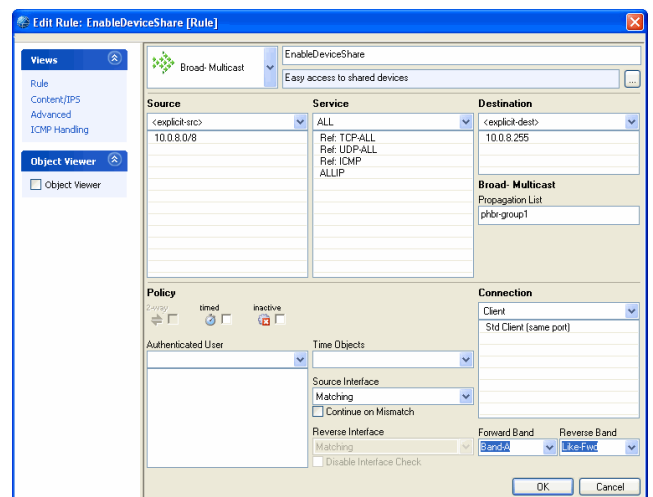
Clicking the label in the title row of each column sorts the entries ascending or descending by name.

Right-clicking a selected entry makes the following actions available in a context menu:

- **Remove Selected MACs**  
Deletes the selected MAC address(es) from the list.
- **Remove IPs from Selected MAC**  
Deletes IP addresses from a specific MAC, which have been saved during a bridged connection establishment, without removing the MAC address itself from the list.

### 9.6.4 Configuring Broadcast and Multicast Propagation over Bridging Interfaces

**Fig. 4-92** Utilising action type Broad-Multicast for Bridging Groups



Propagation of, for example, shared network interfaces is achieved through distribution of broadcast messages. If interface sharing is needed in bridged network setups, a rule allowing for this has to be introduced. Use the firewall action type **Broad-Multicast** to enable propagation of broadcast and multicast messages. Configure values in the following way:

**Table 4-27** Broad-Multicast action type rule configuration

	Description
<b>Source</b>	the network the shared interface resides in
<b>Destination</b>	the source network's broadcast address
<b>Propagation List</b>	the name of the bridging group responsible for bridge traffic forwarding ( <b>phbr</b> <group_name>)

# 10. Firewall Authentication

The Firewall Authentication component allows adding user information (in addition to IP addresses) to firewall rules, which results in a fourth condition (beside source, service, and destination). The firewall rule matches only as long as each condition is fulfilled. Since the firewall engine can only process IP addresses, a **user - IP address mapping** is being performed.

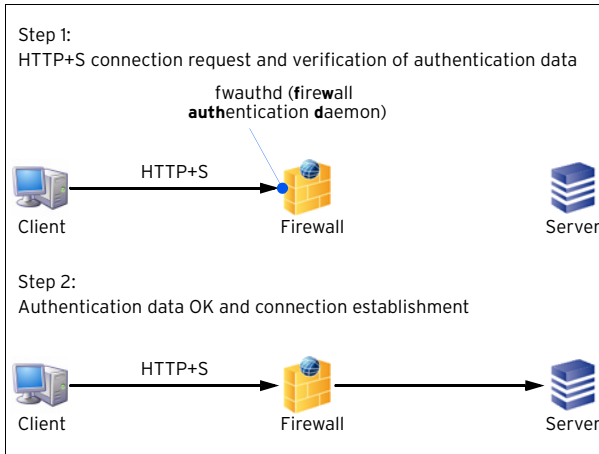
**Attention:**  
Due to the user - IP address mapping it is mandatory to have unique IP addresses for all users, which ought to be authenticated by the firewall.

phion offers two types of firewall authentication:

➤ **Inline Authentication**

works only in conjunction with HTTP and HTTPS; This way of authentication injects the authentication request into the data stream. The authentication is done via a pop-up window in the client's browser. The firewall redirects the HTTP/S request to an internal authentication server. This server generates the authentication request within the browser window by sending a HTTP 401 status code (Server Auth) to the client's browser.

Fig. 4-93 Connection buildup using inline authentication

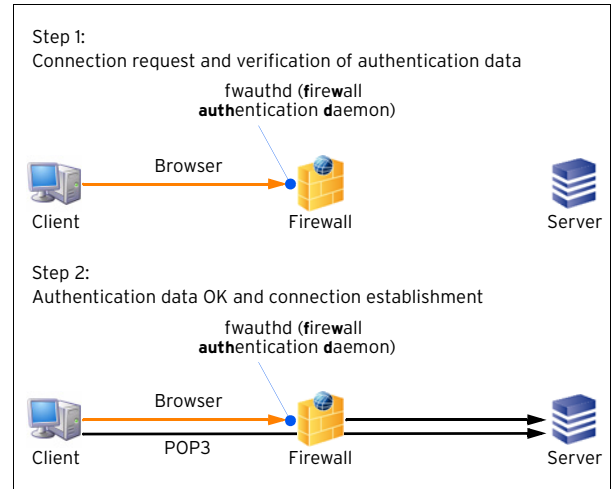


➤ **Offline Authentication**

works in conjunction with all protocols (for example, POP3); When using this authentication method a browser is required to enter the authentication info (then checked by fwauth daemon) in order to get access granted.1







**Note:**  
This browser window has to stay open as long as the connection is required. Otherwise the connection will be terminated due to a (configurable) refresh timeout.

Fig. 4-94 Connection buildup using offline authentication



## 10.1 Configuring Firewall Authentication

### 10.1.1 Configuring the fwauth Daemon

The fwauth daemon (required for **Offline Authentication**, see above) is configured via the following parts of the **Firewall Forwarding Settings** (  **Config** >  **Box** >  **Virtual Servers** >  <servername> >  **Assigned Services** >  <servicename>).

#### 10.1.1.1 Authentication

List 4-50 Firewall configuration - Authentication parameters - section FW Authentication Server

Parameter	Description
<b>Settings</b>	By clicking <b>Show ...</b> , a configuration dialogue is opened where settings concerning firewall authentication are to be specified (see 10. Firewall Authentication, page 188).
Parameter	Description
<b>Force re-authentication</b> [default: Yes]	Activating this parameter (by setting to <b>Yes</b> ) causes that the user has to re-authenticate as soon as the login times out.
<b>WWW root</b> [/var/phion/fwauthd]	This directory specifies the root directory of the mini web server provided by phion.
<b>HTTP/1.1-Keep-Alive</b> [Yes]	
<b>HTTP/1.1-Keep-Alive timeout</b> [10]	Defines after which time (in minutes) a keep-alive session is terminated.
<b>Authentication success page</b> [success.html]	The HTML page specified here is shown after a successful firewall authentication. Take into consideration that it is relative to WWW root (see above).
<b>Authentication error page</b> [error.html]	The HTML page specified here is shown after a failed firewall authentication. Take into consideration that it is relative to WWW root (see above).



**List 4-50** Firewall configuration - Authentication parameters - section FW Authentication Server

Parameter	Description
<b>Authentication logout page</b> [logout.html]	The HTML page specified here is shown after a successful firewall authentication logout. Take into consideration that is relative to WWW root (see above).
<b>Authentication index page</b> [index.html]	The HTML page specified here is used as login page. Take into consideration that is relative to WWW root (see above).
<b>Max size of a file to cache (kb)</b> [2048]	Files that exceed this value will not be cached but loaded from disk.
<b>Max files to cache</b> [20]	Here the maximum number of files is specified that are cached simultaneously.
<b>Refresh auth every ... min</b> [5]	This parameter defines after how long (in minutes) authentication is refreshed. If the authentication information cannot be retrieved (for example because of a closed authentication browser window) the connection is terminated.
<b>Refresh auth tolerance ... min</b> [1]	The authentication is automatically refreshed (without prompting) if peer reconnects after <code>&lt;Refresh auth every ... min + Refresh auth tolerance ... min&gt;</code> .
<b>Root certificates</b>	Here the root certificate for verification of browser peer certificates is handled.
<b>Default HTTPS Private Key / Default HTTPS Certificate</b>	The default key generated/imported here will be used for offline authentication via SSL connections (see 10. Firewall Authentication, page 188). Take into consideration that default certificate AND default key have to match for successful connection establishment.
<b>Destination-specific SSL-Settings</b>	Via this field you may define certain certificates and keys that used for SSL connections to explicit IP addresses.

### 10.1.1.2 Phibs

The following parameters are available for specifying Phibs behaviour:

**List 4-51** Firewall configuration - PHIBS settings - section Phibs Authentication Settings

Parameter	Description
<b>PHIBS Authentication Scheme</b>	A pull-down menu gives five different schemes to choose from: <b>MSNT, RADIUS, LDAP, MSAD, RSAACE</b> <b>Note:</b> The authentication schemes are activated and configured in the box configuration ( <b>Configuration Service</b> - 5.2.1 Authentication Service, page 111).
<b>PHIBS Listen IP</b>	Defines the IP address of the box where the PHIBS-authentication daemon is running on.
<b>PHIBS Timeout</b>	Specifies the response timeout (in minutes) for the authentication server.
<b>User List Policy</b>	The option <b>deny-explicit</b> means that all domain-users who are listed in the user list are not allowed to use the proxy service. The option <b>allow-explicit</b> means that only domain users that are listed in the user list are allowed to use the proxy service. This does not mean that they do not require authentication.
<b>User List</b>	List of usernames that are used for the <b>User List Policy</b> .

### 10.1.1.3 WWW tab

This tab acts as a kind of simple upload tool for the integrated phion web server that is used during Offline Authentication, for either HTML code or binaries.

A possible task would be to place the `proxy.pac` in the configured root directory (parameter **WWW root**, see 10.1.1.1 Authentication, page 188) of the integrated phion web server.

**Note:**

Do not customize default html files (see list 4-50, page 188).

Consequences of customization:

- Dirty Release status (see **Control Centre** - 2.5.1 Section Version Status, page 37).
- The customized files will potentially be overwritten when installing patches or updates.

## 10.1.2 Introducing User-specific Rules

For this purpose the Create Rule dialogue provides the **Authenticated User Section**, where you can select an existing user object (see 10.1.2.1 Firewall - User Window) or set a user explicitly. The available parameters for user configuration are the same for both ways of configuring.

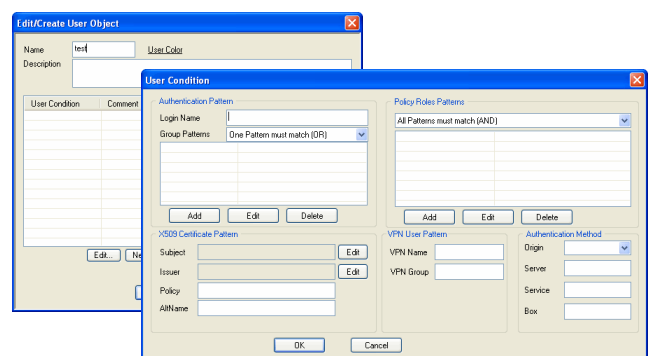
### 10.1.2.1 Firewall - User Window

This window is used for defining user specific rules. Such rules are required when using the Firewall Authentication feature. In order to open the configuration dialogue for a new user/user group click **New ...** in the **Edit User** navigation bar of the **Firewall - User Groups** window of the Rules tab. Now enter a name for this user/user group data set and, optionally, a describing text. By clicking **New ...**, the next configuration dialogue for defining the user conditions is opened. This dialogue provides the following parameters:

**Note:**

Take into consideration that combining fields is also possible. For example, for enforcing a VPN connection (by entering required **VPN User Patterns**) AND a matching X.509 certificate installed in the browser application (by entering required **X509 Certificate Patterns**).

**Fig. 4-95** Configuration dialogues - User Object & User Condition



**List 4-52** Firewall configuration - Rules - User Groups - section Authentication Pattern

Parameter	Description
<b>Login Name</b>	This parameter serves for defining the required login name. Take into consideration that using wildcards (? and *) is also possible (?* requires at least one character as login name).
<b>Group Patterns</b>	This field allows specifying the required group assignment(s) according to the affected external authentication scheme (MSAD, LDAP or RADIUS). The following buttons are available: <b>Add</b> - adding a new entry <b>Edit</b> - modifying an existing entry <b>Delete</b> - removing a marked entry <b>Note:</b> Take into consideration that combining fields is also possible, for example, for enforcing a VPN connection (by entering required <b>VPN User Patterns</b> ) AND a matching X.509 certificate installed in the browser application (by entering required <b>X509 Certificate Patterns</b> ). For information concerning how to gather such group patterns, have a look at <b>Appendix - 1.1</b> How to gather Group Information, page 524.

**List 4-53** Firewall configuration - Rules - User Groups - section Policy Roles Patterns

Parameter	Description
Selector	This field allows specifying the required group assignment(s) according to the affected external authentication scheme (MSAD, LDAP or RADIUS). The following buttons are available: <b>Add</b> - adding a new entry <b>Edit</b> - modifying an existing entry <b>Delete</b> - removing a marked entry

**List 4-54** Firewall configuration - Rules - User Groups - section X509 Certificate Pattern

Parameter	Description
<b>Subject</b>	Here the subject of the affected X.509 certificate is to be entered. By clicking <b>Edit</b> the dialogue Certificate Condition is opened, where the required subject has to be configured. If multiple subject parts (key value pairs) are required separate them with / (for example, OU=test1 and OU=test2 are required, select <b>OU</b> and enter test1/test2). <b>Note:</b> Take into consideration that combining fields is also possible, for example, for enforcing a VPN connection (by entering required <b>VPN User Patterns</b> ) AND a matching X.509 certificate installed in the browser application (by entering required <b>X509 Certificate Patterns</b> ). Using wildcards (?, *) is possible. <b>Attention:</b> Take into consideration that order is mandatory.
<b>Issuer</b>	Here the issuer of the affected X.509 certificate is to be entered. By clicking <b>Edit</b> the dialogue Certificate Condition is opened, where the required issuing instance has to be configured. If multiple subject parts (key value pairs) are required separate them with / (for example, OU=test1 and OU=test2 are required, select <b>OU</b> and enter test1/test2). <b>Note:</b> Take into consideration that combining fields is also possible. For example for enforcing a VPN connection (by entering required <b>VPN User Patterns</b> ) AND a matching X.509 certificate installed in the browser application (by entering required <b>X509 Certificate Patterns</b> ). Using wildcards (?, *) is possible. <b>Attention:</b> Take into consideration that order is mandatory.
<b>Policy</b>	Here the ISO number according to the used X.509 certificate may be entered.
<b>AltName</b>	Here the SubjectAltName according to the used X.509 certificate may be entered.

**List 4-55** Firewall configuration - Rules - User Groups - section VPN User Pattern

Parameter	Description
<b>VPN Name / VPN Group</b>	Parameter <b>VPN Name</b> holds the required VPN login name. Parameter <b>VPN Group</b> holds the required VPN group policy the user has to be assigned to. <b>Note:</b> When using Offline Authentication ensure that user-specific rules are sequenced after the fwauthd rule (see 10.1.4 Activate Offline Firewall Authentication).

**List 4-56** Firewall configuration - Rules - User Groups - section Authentication Method

Parameter	Description
<b>Origin</b>	This parameter is used for defining the type of originator. The following originators are available: <b>VPNP</b> (PersonalVPN) <b>VPNG</b> (GroupVPN) <b>VPNT</b> (Tunnel) <b>HTTP</b> (Browser login) <b>Proxy</b> (Login via proxy)
<b>Server / Service / Box</b>	These parameters allow enforcing authentication on a certain server/service/box.

## 10.1.3 Activate Inline Firewall Authentication

In order to activate Inline Firewall Authentication, simply enter the **Advanced Rule Parameters** dialogue of the affected rule and set the parameter **Authentication** to the required authentication mode. The following modes are available:

- **No Inline Authentication** (default)
- **Login+Password Authentication**
- **X509 Certificate Authentication**
- **X509 Certificate & Login+Password Authentication**

## 10.1.4 Activate Offline Firewall Authentication

### 10.1.4.1 Introducing Redirect Rule for fwauthd

fwauthd listens on the following ports of the local loopback (127.0.0.1) adapter:

- **443** - listening for HTTPS connections (authentication via user & pw)
- **444** - listening for connections using X.509 certificates for authentication
- **445** - listening for connections using X.509 certificates and user/pw for authentication
- **80** - listening for HTTP connections (authentication via user & pw)

To introduce a redirect rule for fwauthd, it is necessary to redirect the IP address, where the users connect to for authentication matters.

#### Attention:

Correlation between used authentication method and used port is mandatory for authentication success.

**Step 1** Create a fwauth rule

**Step 2** Action: Select *Local Redirect*

**Step 3** Destination: Enter the IP address that users have to access to authenticate themselves

**Step 4** Redirection: Enter the loopback IP address (127.0.0.1) and the correct port

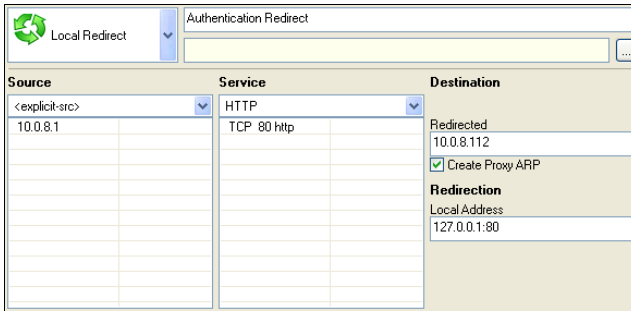
**Step 5** Service: Enter the correct port for your authentication method

**Note:**

After introducing ensure that the just created fwauth rule is on top of the user specific rules.

In the example below a rule has been introduced redirecting a client with the IP address 10.0.8.1 attempting access to the firewall authentication interface running on http://10.0.8.112 to the fwauth daemon on 127.0.0.1:80.

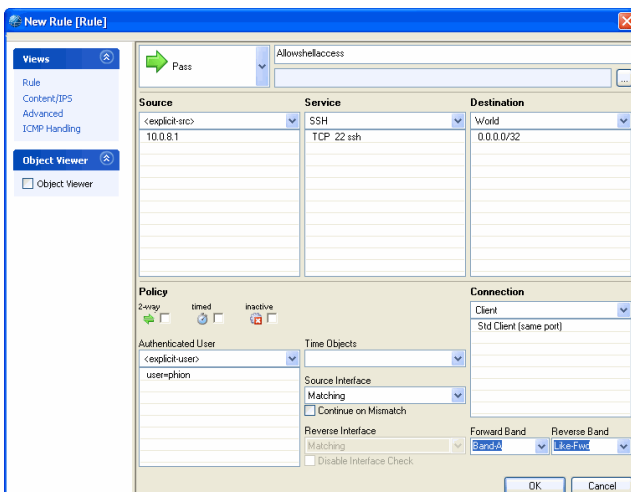
Fig. 4-96 fwauthd redirection rule



**10.1.4.2** Introducing a User Authentication Rule for fwauthd

After the firewall authentication redirection rule has been introduced, actions can be defined for authenticated users. In the example below, shell access to any server in the Internet is explicitly allowed for user "phion", in case this user has established a connection using the IP address 10.0.8.1.

Fig. 4-97 fwauthd user authentication rule



**10.1.4.3** Authentication Procedure

When firewall authentication has been configured, the user authenticates himself using a browser. In the example below the firewall authentication login screen is opened on http://10.0.8.112 using Microsoft Internet Explorer.

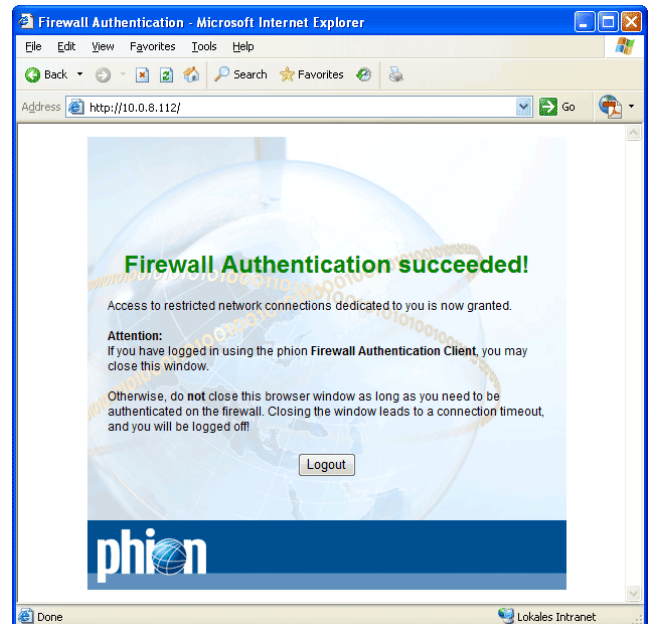
Fig. 4-98 Firewall Authentication login screen



**Note:**

Having logged in, do not close the browser window, until firewall authentication is no longer needed. Closing the browser window terminates the active firewall authentication session.

Fig. 4-99 Firewall Authentication succeeded login screen



**Note:**

The phion Firewall Authentication Client is available to automate and facilitate firewall authentication procedure (10.2 phion Firewall Authentication Client, page 192).

## 10.2 phion Firewall Authentication Client

The phion Firewall Authentication Client (available on your Application CD-ROM) is appointed to automate handling of Offline Firewall Authentication. The client is an optional tool, which can be installed if it is desirable to avoid circumstantial browser window operation.

Only one parameter has to be provided explicitly during installation:

### ➤ Home Page

This is the URL of the firewall authentication login interface. With regard to the example described in 10.1.4 Activate Offline Firewall Authentication, the homepage would have to be entered as `http://10.0.8.112`.

#### Note:

The homepage URL can always be changed with hindsight in the configuration options of the tool itself.

#### Note:

During installation the authentication client adopts the connection settings provided in the Internet Explorer settings. If proxy settings have to be adjusted for authentication client usage, settings always have to be changed directly in Internet Explorer and not in the tool itself.

The phion Firewall Authentication Client is automatically started with Microsoft Windows (Registry entry `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\phionauth.exe`).

You may manually start the client from the Start menu by browsing to `Start > phion > phion Firewall Authentication > phion Firewall Authentication Client`.


A browser-like window opens asking for the specific login data. Enter the user information you have been applied with and login to the firewall.

You may now close the window again. The client withdraws to an icon in the status bar. It may be opened from the status bar, either to log out from the firewall or to be closed.

#### Note:

Exiting from the client leads to a timeout on the firewall and thus terminates an active firewall authentication connection.





## 10.3 Monitoring

Monitoring takes place in the **AuthUser** tab of the  **Firewall** box menu entry.

The button **Update List** on top of this tab allows starting the updating sequence manually.

The following columns are used for displaying all necessary information:

**Table 4-28** Monitoring parameters overview

Column	Description
Peer	This column contains the IP address used to establish the connection and an icon for each auth-connection type: <ul style="list-style-type: none"> <li> VPNT - VPN Tunnel</li> <li> VPNP - Personal VPN</li> <li> VPNG - Group VPN</li> <li> HTTP - via browser</li> </ul>
Timeout	Displays time until authentication expires
Origin	Displays the type of connection for authentication. The following entries are possible: <ul style="list-style-type: none"> <li>VPNT - VPN Tunnel</li> <li>VPNP - Personal VPN</li> <li>VPNG - Group VPN</li> <li>HTTP - via browser</li> </ul>
Server	Displays the phion server/service/box that was used for authentication purpose
Service	
Box	
User	Shows the login name.
Groups	Displays the authentication group the user is assigned to
VPN Name	Shows the name of the VPN tunnel
VPN Group	Displays the group policy the user is assigned to
X509 Subject	These columns show information obtained from the X.509 certificate that was used for authentication.
X509 Issuer	
X509 Policy	
X509 AltName	

# 11. RPC

## 11.1 General

phion provides three ways of dealing with RPC: passive, active, and active & passive.

**Table 4-29** RPC - comparison passive / active

	Advantage	Disadvantage
<b>Passive</b>	The firewall immediately notices RPC port changes (traffic analyses client - server)	The firewall notices the RPC port which is used only on client requests. If a firewall reboot occurs, the firewall will not know the port until the next client request gets scanned.
<b>Active</b>	The firewall actively looks for all RPC informations independent of client requests.	All RPC servers have to be configured manually. Port changes within a polling interval will not be recognised by the firewall.

- **PASSIVE;** which means "sniffing" RPC information passively.  
Using this type causes that the firewall engine reads the RPC information from RPC requests (using UDP/TCP on port 135 (DCERPC) or port 111 (OCNRPC)) automatically using the plugin **DCERPC** or **OCNRPC**. This way you are benefiting from the fact that the firewall is always up-to-date on the currently valid ports (with slight performance loss, though). The main problem of passive is that in case of a reboot of the firewall there would not be any information concerning the required ports as the information is not written to disk. This would lead to a blocked connection attempt.
- **ACTIVE;** which means requesting RPC information actively.  
This method uses a defined RPC server where the firewall obtains the RPC information periodically. A benefit of this type is that the firewall knows the type of services available on the RPC server. However, problems may occur if the RPC server is not available for some time. In this case the RPC server may have new portmapping information as soon as it is online again but the firewall still uses the "old" information as valid ones which leads to blocked connection attempts.
- **ACTIVE & PASSIVE** at the same time; that is combining the benefits of both (recommended)

## 11.2 ONCRPC

The **ONCRPC** (**O**pen **N**etwork **C**omputing **R**emote **P**rocedure **C**all; formerly known as **SUNRPC**), allows services to register on a server, which then makes them available on dynamic TCP/UDP ports. By means of this mechanism, ports required for specific purposes (for example NFS), can be dynamically enabled without weakening a strict security policy.

The heart of ONCRPC is the so-called **portmapper**, an interface responsible for allocation of ports and protocols to services. If an application demands a certain service, a request is sent to the portmapper. The portmapper's answer contains the required port and protocol, which are then used for connection establishment. How does the firewall handle such actions?

### 11.2.1 Configuring ONCRPC

**Note:**  
Please consider the following configuration option regarding the parameter **Dyn. Service** when reading the guidance below as it applies to all available methods:

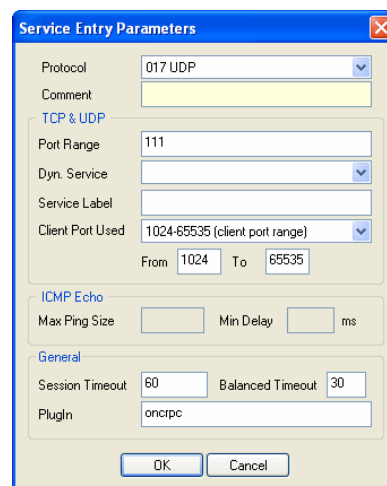
- The parameter **Dyn. Service** can be configured to utilize all available services by just entering **ONCRPC** into the **Dyn. Service** field.

#### 11.2.1.1 Configuring Passive ONCRPC

##### Step 1 Enabling access to the portmapper

Create a pass rule for portmapper access using a corresponding service object. When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port **111**. Last but not least, you need to enter the **Plugin** **ONCRPC** in the **General** section of the **Service Entry Parameters** dialogue (see figure).

**Fig. 4-100** General *Service Object* needed for creating a pass rule to enable passive ONCRPC

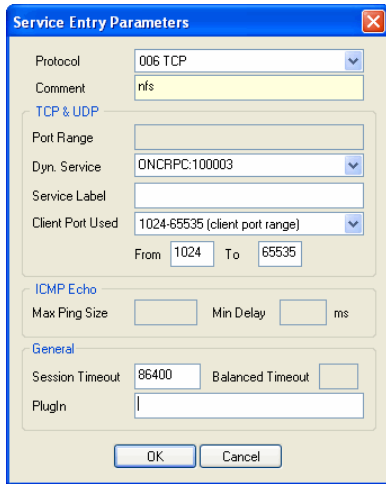




**Step 2 Creating a rule for the required service** (for example NFS)

Again, as mentioned in Step 1, the settings for the service object are of interest. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (which means servicename:serviceID; in our example this would be ONCRPC:100003, see figure 4-101).

Fig. 4-101 Service Object needed for enabling nfs usage via a portmapper



**Step 3 Checking rule set hierarchy**

For successful usage of dynamic services it is mandatory to have the general rule (created during Step 1, page 193) situated above the service rules (created during Step 2, page 194).

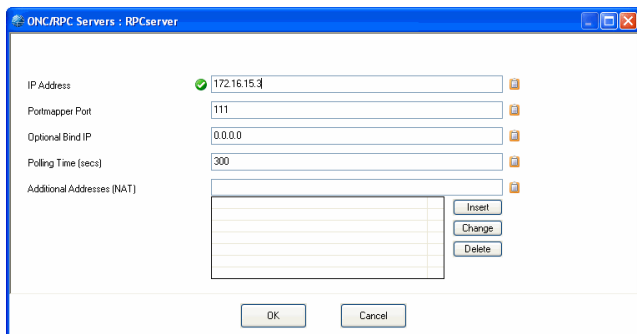
## 11.2.2 Configuring Active ONCRPC

**Step 1 Configuring the RPC server information**

The RPC server information is configured via the RPC tab of the **Firewall Forwarding Settings** ( **Config** > **Box** > **Virtual Servers** > <servername> > **Assigned Services** > <servicename>).

Via button **Edit ...** you may modify an already existing server entry. Via button **Insert ...** you may create a new server entry (however, both configuration dialogues are the same). Selecting an existing entry and clicking **Delete** removes this entry.

Fig. 4-102 RPC Server information configuration dialogue



The following parameters are available for configuration:

List 4-57 Firewall configuration - Forwarding Firewall - RPC tab - section RPC Settings

Parameter	Description
<b>Default Poll Time (secs)</b> [default: 300]	Here the interval for requesting RPC information from the RPC server is defined.

List 4-58 Firewall configuration - Forwarding Firewall - RPC tab - section ONCRPC Servers / DCERPC Servers

Parameter	Description
<b>Name</b>	This is the describing name of the <b>ONCRPC Server</b> specified at creation time.
<b>IP Address</b>	Here the IP address of the considered RPC server is to be entered.
<b>Portmapper Port</b> [111]	This parameter defines the port where portmapper is listening on. <b>Attention:</b> Take into consideration that the service object for the portmapper rule (created in Step 2, page 194) has to match this port.
<b>Optional Bind IP</b> [0.0.0.0]	This parameter allows you to define an explicit IP address that is used when connecting to the RPC server. This comes handy as soon you are using policy routing. The default value of <b>0.0.0.0</b> deactivates this parameter and the correct Bind IP address will be specified via the routing table.
<b>Polling Time (secs)</b> [300]	Here the interval for requesting RPC information from the RPC server is defined.
<b>Additional Addresses (NAT)</b>	If you want to use NAT, enter the corresponding addresses in this section.

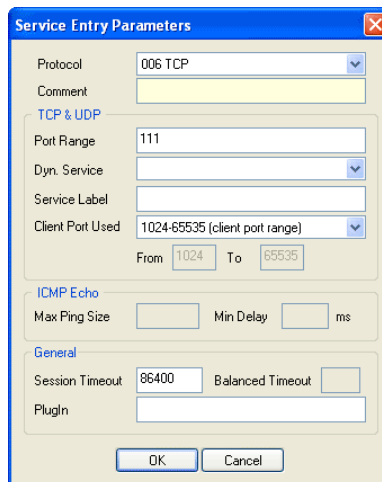
**Step 2 Enabling access to the portmapper**

Create a pass rule for portmapper access using a corresponding service object. When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port **111** (see figure 4-103).

**Note:**  
If you have specified an alternative port in the server configuration, do not forget to define this alternative port instead of the default port here.

**Note:**  
Do not fill in the PlugIn field when configuring Active ONCRPC.

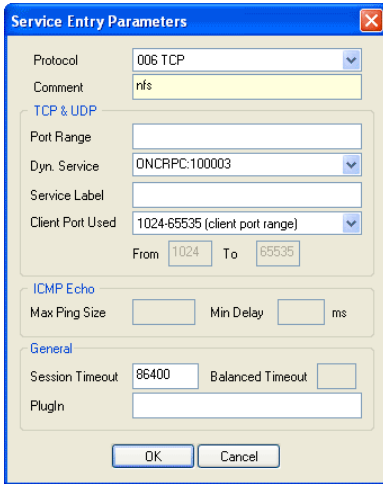
Fig. 4-103 General *Service Object* needed for creating a pass rule to enable active ONCRPC



**Step 3 Creating a rule for the required service** (for example NFS)

Again, as mentioned in Step 1, the settings for the service object are of interest. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (`servicename:serviceID`; in our example this would be `nfs:100003`, see figure 4-104).

**Fig. 4-104** Service Object needed for enabling nfs usage via a portmapper



**Step 4 Checking rule set hierarchy**

For successful usage of dynamic services it is mandatory to have the general rule (created during Step 2, page 194) situated above the service rules (created during Step 3, page 195).

**11.2.2.1 Configuring Active&Passive ONCRPC (recommended)**

**Step 1 Configuring the RPC server information**

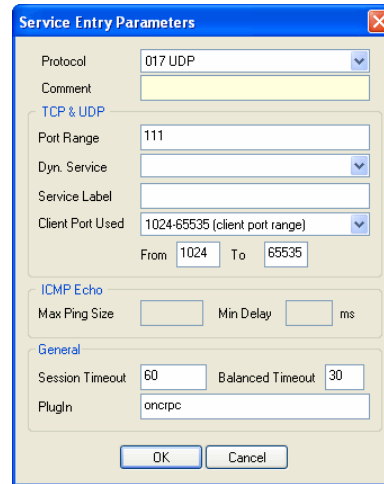
Configure the RPC Server information as described above in Step 1 Configuring the RPC server information, page 194.

**Step 2 Enabling access to the portmapper**

Create a pass rule for portmapper access using a corresponding service object. When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port **111**. Last but not least, you need to enter the **Plugin** ONCRPC in the **General**

section of the **Service Entry Parameters** dialogue (see figure 4-105).

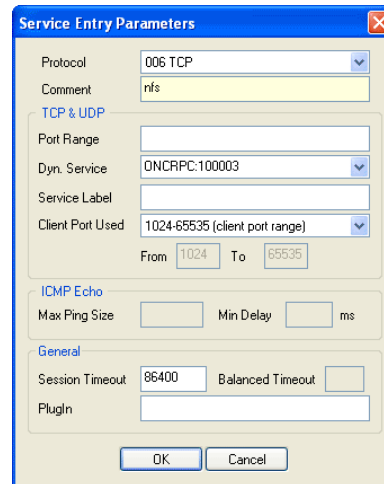
**Fig. 4-105** General Service Object needed for creating a pass rule to enable active&passive ONCRPC



**Step 3 Creating a rule for the required service** (for example, NFS)

Again, as mentioned in Step 1, the settings for the service object are of interest. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (`servicename:serviceID`; in our example this would be `nfs:100003`).

**Fig. 4-106** Service Object needed for enabling nfs usage via a portmapper



**Step 4 Checking rule set hierarchy**

For successful usage of dynamic services it is mandatory to have the general rule (created during Step 2, page 195) situated above the service rules (created during Step 3, page 195).

**Note:**  
The parameter **Dyn. Service** can be configured to utilize all available services by just entering **DCERPC** into the **Dyn. Service** field.

**Note:**

In addition to explicit creation of new Service Objects you may as well make use of the already existing predefined Service Objects (for example, Service Objects bound to Microsoft Exchange usage). Please consider, though, that you might possibly have to adapt the preconfigured objects due to potential requirement changes of the software.

## 11.3 DCERPC

The OSF Distributed Computing Environment (DCE) is a protocol standardised by the Open Group ([www.opengroup.org/dce](http://www.opengroup.org/dce)). Analogous to the ONCRPC protocol (see 11.2 ONCRPC, page 193), DCERPC allows services to register on a server which then provides these services on dynamic TCP/UDP ports.

The most widespread application depending on DCERPC is possibly Microsoft Exchange. Besides other Microsoft products, DCERPC for example is as well used by HP Open View.

Since the so-called **end point mapper** knows which service requires which port and protocol, the client application first sends a request to the end point mapper to determine the dynamically assigned ports.

The endpoint mapper listens on TCP/UDP port **135**.

What's the difference to ONCRPC?

- Portmapper is called **Endpoint Mapper** and uses **TCP/UDP port 135** instead of UDP/TCP 111
- Service identification via UUID instead of program numbers
- Multiple services per port possible  
Having multiple services on one TCP port a "pre-validation" by the firewall is required. This pre-validation checks whether at least one service offered by this port is granted by the rule set:  
**NO** - block  
**YES** - session is granted using service name `DCERPC:ANY` and is subsequently analysed further. As soon as the service is selected, the rule set is checked again whether exactly this service is permitted or not. If granted, the service name changes to the now-known name and session is active (first matching rule is used). If the service is not permitted the session is terminated.
- One service can be offered on multiple ports
- Using UDP DCERPC offers an additional function in order to avoid arbitrary spoofed request to the RPC server
- Service can change within a session

### 11.3.1 Configuring DCERPC

**Note:**

Please consider the following configuration options regarding the parameter **Dyn. Service** when reading the guidance below as it applies to all available methods:

- The parameter **Dyn. Service** can be configured to utilize all available services by just entering **DCERPC** into the **Dyn. Service** field.
- In addition to explicit creation of new **Service Objects** you may as well make use of the already existing predefined Service Objects (for example, Service Objects bound to Microsoft Exchange usage). Please consider, though, that you might possibly have to adapt the preconfigured objects due to potential requirement changes of the software.

#### 11.3.1.1 Configuring Passive DCERPC

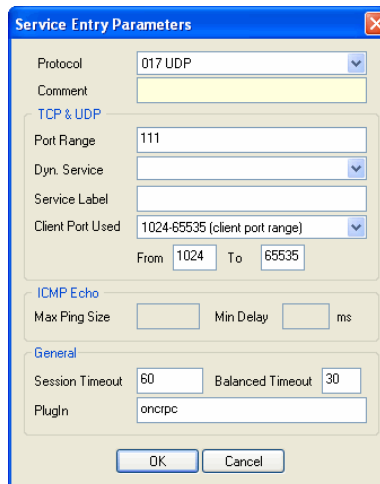
**Note:**

For the advantages and disadvantages of passive and active configuration see 11.1 General, page 193.

##### Step 1 Enabling access to the end point mapper

Creating a pass rule for end point mapper access using a corresponding service object (phion default service object: DCERPC135). When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port **135**. Last but not least, you need to enter the **Plugin** `DCERPC` in the **General** section of the **Service Entry Parameters** dialog (see figure 4-107).

**Fig. 4-107** General Service Object needed for creating a pass rule to enable passive DCERPC



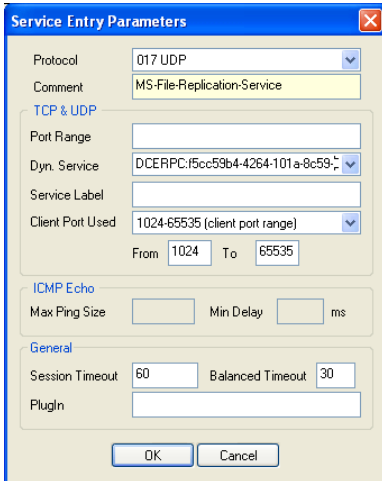
The screenshot shows the 'Service Entry Parameters' dialog box with the following settings:

- Protocol: 017 UDP
- Comment: (empty)
- TCP & UDP:
  - Port Range: 111
  - Dyn. Service: (dropdown menu)
  - Service Label: (empty)
  - Client Port Used: 1024-65535 (client port range)
  - From: 1024 To: 65535
- ICMP Echo:
  - Max Ping Size: (empty)
  - Min Delay: (empty) ms
- General:
  - Session Timeout: 60
  - Balanced Timeout: 30
  - Plugin: oncrpc

**Step 2 Creating a rule for the required service** (for example MS Exchange)

Again, as mentioned in Step 1, the settings for the service object are of interest. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (`servicename:UUID`; see figure 4-108).

**Fig. 4-108** Service Object needed for enabling MS-File Replication Service usage via an end point mapper



**Step 3 Checking rule set hierarchy**

For successful usage of dynamic services it is mandatory to have the general rule (created during Step 1, page 193) is situated above the service rules (created during Step 2, page 194).

**11.3.1.2 Configuring Active DCERPC**

**Note:**

For the advantages and disadvantages of passive and active configuration see 11.1 General, page 193.

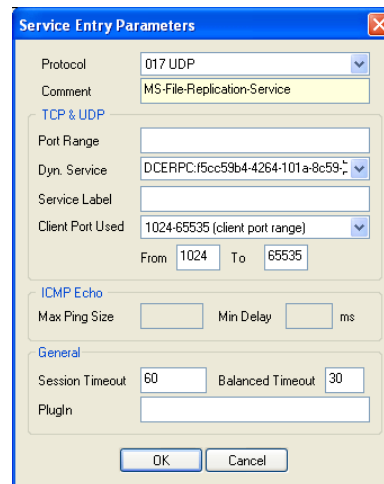
**Step 1 Configuring the RPC server information**

The RPC server information is configured via the RPC tab of the **Firewall Forwarding Settings** (Config > Box > Virtual Servers > <servername> > Assigned Services > <servicename>). The configuration is analogue to the one mentioned under 11.2.2 Configuring Active ONCRPC, Step 1, page 194, except that the port **135** has to be entered (instead of port 111).

**Step 2 Enabling access to the portmapper**

Create a pass rule for portmapper access using a corresponding service object. When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port **135** (see figure 4-109).

**Fig. 4-109** General Service Object needed for creating a pass rule to enable active DCERPC



**Note:**

If you have specified an alternative port in the server configuration, do not forget to define this alternative port instead of the default port here.

**Note:**

Do not fill in the PlugIn field when configuring Active DCERPC.

**Step 3 Creating a rule for the required service** (for example MS Exchange)

Again, as mentioned in Step 1, the settings for the service object are of interest. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (`servicename:UUID`).




**Step 4 Checking rule set hierarchy**

For successful usage of dynamic services it is mandatory to have the general rule (created during Step 2, page 194) is situated above the service rules (created during Step 3).

### 11.3.1.3 Configuring Active&Passive DCERPC (recommended)

#### Step 1 Configuring the RPC server information

The RPC server information is configured via the RPC tab

of the  **Firewall Forwarding Settings** ( **Config** >  **Box** >  **Virtual Servers** >  <servername> >  **Assigned Services** >  <servicename>).

The configuration is analogue to the one mentioned under 11.2.2 Configuring Active ONCRPC, Step 1, page 194, except that port **135** has to be entered (instead of port 111).

#### Step 2 Enabling access to the portmapper

Create a pass rule for portmapper access using a corresponding service object. When configuring the service entry, select either **UDP** or **TCP** as protocol and set the parameter **Port Range** to port **135**. Last but not least, you need to enter the **Plugin** `DCERPC` in the **General** section of the **Service Entry Parameters** dialogue.


#### Step 3 Creating a rule for the required service (for example NFS)

Again, as mentioned in Step 1, the settings for the service object are of interest. Select the required protocol (either **UDP** or **TCP**) and use parameter **Dyn. Service** for defining the service information (`servicename:UUID`).

#### Step 4 Checking rule set hierarchy

For successful usage of dynamic services it is mandatory to have the general rule (created during Step 2) is situated above the service rules (created during Step 3).

## 11.4 Monitoring

Monitoring takes place in the **Dynamic Services** tab of the  **Firewall** box menu entry (tab **Dynamic**).

Via the button **Update List** you can refresh the displayed information.

The following columns are in use:

**Table 4-30** Monitoring parameters overview

Column	Description
Used Address	IP address used by the dynamic service
Proto	Protocol used by the dynamic service
Port	Port used by the dynamic service
Service Name	Name and Number of the dynamic service
Service Desc	Description for the dynamic service
Target Address	IP address where the dynamic service connects to
Expires	Displays when the dynamic service connection expires
Used	Expired time since last usage
Updated	Expired time since last information update
Source Address	IP address for which the dynamic service entry is valid for (entry <b>0.0.0.0</b> indicates all IP addresses)
Source Mask	Netmask for which the dynamic service entry is valid for



# VPN

<b>1.</b>	<b>Overview</b>	
1.1	Client Remote Access .....	200
1.2	Site to Site VPN .....	201
1.3	Certificate Authority .....	201
1.4	Authentication, GroupVPN, Encryption and Transport .....	201
<b>2.</b>	<b>Configuring Personal Remote Access</b>	
2.1	VPN Configuration Block Diagram .....	205
2.2	Introduce and Configure Box, Server, Firewall and VPN Service .....	205
2.3	Install Licenses and Configure Personal Networks .....	206
2.4	Configuring VPN GTI Settings .....	209
2.5	Configuring L2TP/PPTP Settings .....	210
2.6	Configuring Personal VPN .....	212
2.7	Configuring VPN Tunnel Settings .....	220
<b>3.</b>	<b>SSL-VPN</b>	
3.1	Introduction .....	229
3.2	Parameters .....	229
3.3	Setup Examples .....	232
3.4	Hints .....	234
<b>4.</b>	<b>Monitoring</b>	
4.1	Active Tab .....	237
4.2	Status Tab .....	237
4.3	Access Tab .....	238
<b>5.</b>	<b>Examples for VPN Tunnels</b>	
5.1	Fully Transparent Tunnel .....	239
5.2	Stealth Tunnel .....	239
5.3	Star-shaped Topologies .....	240
5.4	Redundant VPN Tunnels .....	240
<b>6.</b>	<b>Configuring the Personal Firewall</b>	
6.1	General .....	242
<b>7.</b>	<b>entegra VPN client</b>	
7.1	Installation & Configuration .....	242
7.2	Troubleshooting .....	242

# 1. Overview

Virtual Private Networks are an efficient and cost-saving way to use the internet as a transport alternative to dedicated lines or dial-up RAS overcoming the security risks of internet communications.

There are two well-established technologies for data encryption: IPSec and SSL (Secure Socket Layer)

Most VPN implementations rely solely on IPSec, which has several disadvantages (for example problems with NAT, NAPT, filtering interfaces,...) in modern network topologies. phion netfence VPN has incorporated both technology standards and hence improves the VPN connectivity substantially.

## 1.1 Client Remote Access

Mobile workers often need secure access to corporate information resources. This can be realised by dial-up Remote Access Servers (RAS) or by VPN technologies. RAS implementations suffer several limitations, such as bandwidth, scalability, and manageability. Due to the spreading availability of broadband access via cable and xDSL VPN provides a superior solution for the remote access challenge.

The Client - Server communication can be established in three archetypical ways:

- Direct Connection (1.1.1 Direct Connection, page 200)
- Connection through a firewall with or w/o NAT (1.1.2 Connection through a Firewall, page 200)
- Connections via proxy or SOCKS server (1.1.3 Connections via Proxy/SOCKS Server, page 201)

The several different ways of internal/external address assignment and routing can be distinguished into four archetypal conditions.

The two criteria are:

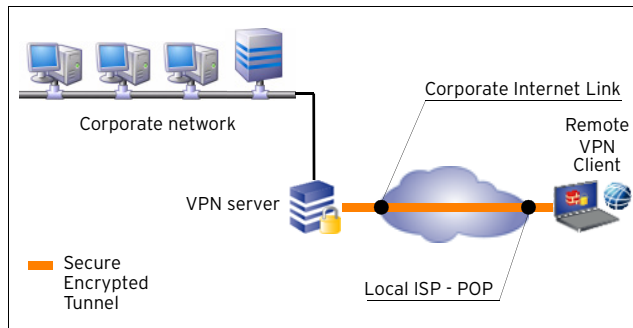
- Is the client IP routed through the Internet?
- Is the VPN server IP routed through the private net the client is in?

**Table 5-1** Client - Server communication options

Conditions		Solutions		
Client IP routed through Internet	Server IP routed through client network	Transparent transport without Source NAT	Transparent transport with Source NAT	HTTPS proxy/SOCKS 4-5
yes	yes	yes	yes	yes
no	yes	no	yes	yes
yes	no	no	no	yes
no	no	no	no	yes

### 1.1.1 Direct Connection

**Fig. 5-1** General scheme of remote access VPN



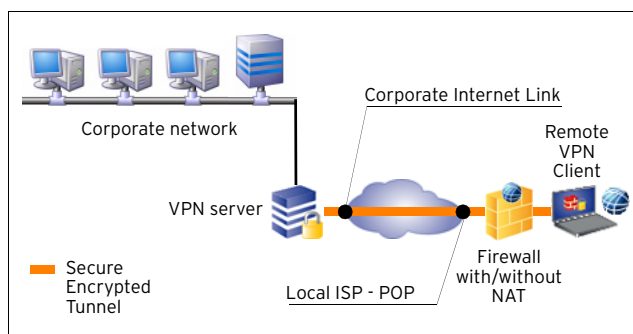
A necessary condition for direct conditions to work is that the client IP as well as the Server IP is routed throughout the whole connection. Because of security and flexibility reasons, most corporate networks use private addresses (often called RFC1918 addresses). These addresses are not routed in the Internet itself. Moreover, some corporate networks do not route other IP addresses than their own. This leads to severe problems in VPN client deployment. Raw IPSec protocol based VPNs cannot provide a proper solution for such situations.

The client simply connects itself to the VPN server on port 691.

Optionally the client can use port 443 as well.

### 1.1.2 Connection through a Firewall

**Fig. 5-2** Remote Access with the client placed behind a firewall



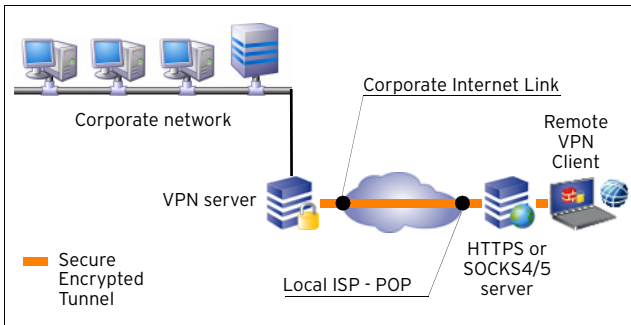
As the client does not use IPSec-ESP or another non-TCP protocol as transport facility the firewall administrator has to provide access to the connection:

- client:(client-port) -> VPN Server: port 691 or
- client:(client-port) -> VPN Server: port 443

Whether the firewall performs NAT (destination or source) does not have any implications to the functionality of the VPN connection.

### 1.1.3 Connections via Proxy/SOCKS Server

**Fig. 5-3** Remote Access with the client using a proxy or SOCKS server for routing assistance



If either the client is not allowed to connect to the VPN server directly or if there is no route to the VPN server, it is necessary to use either a HTTPS proxy or a socks server.

To connect via a HTTPS Proxy it is often necessary to connect to port 443 at the VPN server side, because most proxies restrict the connect method to port 443.

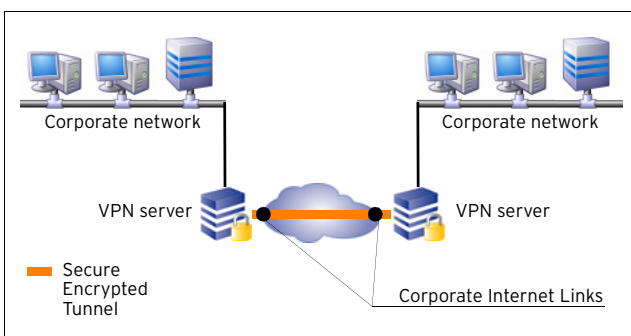
## 1.2 Site to Site VPN

Connecting two corporate locations using VPN can be even more dramatic cost saving than remote access. Saving the costs of bandwidth limited dedicated lines you can easily connect as many locations as necessary into one large corporate network without even losing performance, manageability, and control of costs.

The netfence firewall establishes strongly encrypted (DES, 3DES, AES-128, AES-256, ...) VPN tunnels between two phion firewalls. It supports active and passive tunnel initiation and provides maximum flexibility.

Furthermore it is capable of establishing VPN connections to IPSec based systems.

**Fig. 5-4** Two corporate networks linked together via VPN tunnel



## 1.3 Certificate Authority

For authentication, the netfence VPN server includes a full-featured **Certificate Authority (CA)** that allows the administrator to create, delete, and renew X.509 certificates for strong authentication of remote access users.

**Note:**

To achieve full flexibility and security it is mandatory to combine a firewall with the VPN server. At the end of the VPN tunnel the traffic is directed into the firewall engine, which applies its rule set to the traffic that comes out of the tunnel and goes into the tunnel.

The VPN tunnel terminates before the traffic is directed into the firewall engine. This means that even if the VPN RAS client appears to the firewall with an address of the local LAN the administrator has still full control over access policies of the clients connected to the LAN.

## 1.4 Authentication, GroupVPN, Encryption and Transport

### 1.4.1 General

The phion VPN implementation supports a range of authentication, encryption, and transport methods. The default settings fit for most practical purposes, but there is a number of special situations in modern network reality which need special solutions.

### 1.4.2 Authentication

#### 1.4.2.1 phion Client to Site VPN

There are several different ways of authentication for phion VPN connections:

- **phion x.509 certificate**  
A phion x.509 certificate and the private/public key pair is provided in a password protected file.
- **User and Password**  
For this authentication method the user has to enter his username and password.  
This type is capable of VPN groups. For more information see 1.4.3 VPN Groups, page 202.
- **External x.509 certificate**  
This method requires only an external (not-phion), root-signed x.509 certificate from a CA (PKI).  
This type is capable of VPN groups. For more information see 1.4.3 VPN Groups, page 202.
- **External x.509 certificate with user and password request**  
This type of authentication consists of an external (not-phion), root-signed x.509 certificate from a CA (PKI) and requires manual username and password entry.  
This type is capable of VPN groups. For more information see 1.4.3 VPN Groups, page 202.
- **External x.509 certificate with password request**

This type of authentication consists of an external (not-phion), root-signed x.509 certificate from a CA (PKI) and requires manual user and password entry. The username has to match with the one the x.509 certificate contains.

This type is capable of VPN groups. For more information see 1.4.3 VPN Groups, page 202.

**Note:**  
For authentication methods that require a x.509 certificate, the certificate and the private/public key pair may be provided on a smart card. This offers increased security since the private key is not extractable.

### 1.4.2.2 Client to Site IPSec

The authentication method for IPSec tunnels consists of an external, root-signed x.509 certificate from a Certificate Authority (CA). This method is capable of VPN groups (see 1.4.3 VPN Groups, page 202).

### 1.4.2.3 phion VPN Site to Site

There are several different ways of authentication for phion VPN Site to Site tunnels:

- Pre-shared RSA public key
- External root-signed x.509 certificate (1.3 Certificate Authority, page 201)  
This method is capable of many restrictive configurations (match on one root certificate, match on all root certificates, additional pattern check for subject/subject alternative name, policy match, generic v3 OID match).
- Explicit x.509 certificate (for example self-signed)  
This method is used if no CA/PKI (Public Key Infrastructure) is available.

### 1.4.2.4 Site to Site IPSec

There are several different ways of authentication for phion VPN Site to Site tunnels:

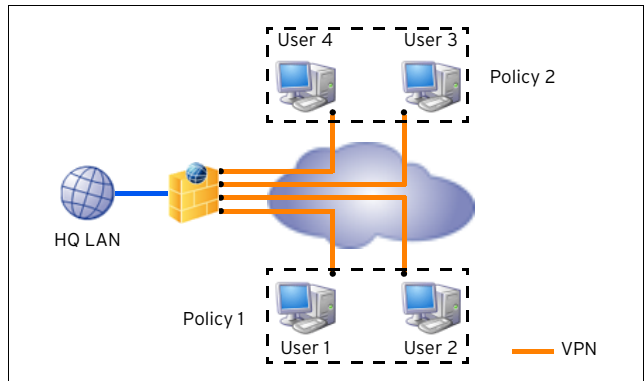
- Pre-shared pass phrase
- External root-signed x.509 certificate (1.3 Certificate Authority, page 201)  
This method is capable of many restrictive configurations (match on one root certificate, match on all root certificates, additional pattern check for subject/subject alternative name, policy match, generic v3 OID match).
- Explicit x.509 certificate (for example self-signed)  
This method is used if no CA/PKI (Public Key Infrastructure) is available.

## 1.4.3 VPN Groups

When having lots of VPN clients, it can be very annoying to configure every single client one by one. To make configuration work more comfortable and faster, some authentication methods provide the possibility of working with so-called VPN groups.

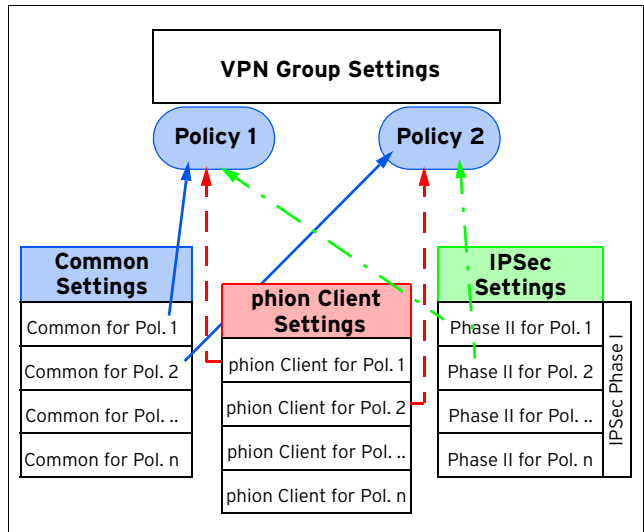
These groups are not necessarily identical with the one for LDAP authentication for example. This fact implies "1-to-n" mapping.

Fig. 5-5 Example for a VPN constellation



The configuration of VPN groups is made via a global **VPN Group Settings** part that affects all VPN groups and **VPN Group Policies**, which contain **Common Settings**, **IPSec Settings** (Phase II), and **Phion Client Settings**. These setting categories are referenced into the **Policies** (profiles) (figure 5-6).

Fig. 5-6 Data scheme for VPN groups



## 1.4.4 Encryption

The following encryption algorithms are available for VPN connections:

- DES  
Digital Encryption Standard
- 3DES  
Triple DES
- AES-128  
Advanced Encryption Standard with up to 128 bit encryption
- AES-256  
Advanced Encryption Standard with up to 256 bit encryption
- Blowfish  
by Bruce Schneier
- CAST  
by Carlisle Adams and Stafford Tavares
- Null  
Not encrypted

### Attention:

It is highly recommended not to use **DES** or **Null** encryption for VPN connections, since these algorithms are unsafe.

## 1.4.5 Transport

There are four different transport modes available for phion VPN connections:

- **UDP**  
Tunnel uses UDP port 691 to communicate. This connection type is best suited for response optimised tunnels.
- **TCP**  
Tunnel uses TCP connections on port 691 or 443 (if http proxies are used). This mode is necessary for connections over SOCKS 4 or http proxies.
- **UDP&TCP**  
Tunnel uses TCP AND UDP connections. The tunnel engine uses the TCP connection for UDP requests and the UDP connection for TCP and ICMP based applications.
- **ESP**  
Tunnel uses ESP (IP protocol 50) to communicate. This connection type is best suited for performance optimised tunnels.

### Note:

**DO NOT** use ESP if there are filtering or NAT interfaces in between.

Table 5-2 Comparison of different tunnel transport modes

Transport mode	Proxy/ SOCKS compatibility	NAT compatibility	Response time	Transport reliability
UDP	no	yes	fast	normal
TCP	yes	yes	normal	complete
UDP&TCP	no	yes	fast	complete
ESP	no	no	fast	normal

### 1.4.5.1 Personal Access Clients

The phion VPN Server uses the built-in certificate authority and/or external root-certificates to guarantee the authenticity of both communication partners. After exchanging the certificates, the communication uses RSA 1024 bit encryption to build up a secure connection to exchange session keys. Afterwards the connection is strongly encrypted with a key renewing after every 30 minutes.

### 1.4.5.2 Tunnel Connections

The phion VPN Servers have to exchange their respective public keys to build up the trusted relationship. After exchanging the public RSA keys, the communication uses RSA 1024 bit encryption to build up a secure connection. Afterwards the connection is strongly encrypted with a session key renewing after every 10 minutes. The time between the key renewing is configurable and can also be dependent on the amount of traffic being encrypted with the same key.

For details see "Kryptografie" by Klaus Schmech, ISBN 3-932588-90-8 (german)

## 1.4.6 Excursion: Description of VPN NoHash Security Issues

### Standard ESP

The ESP protocol provides packet authentication and packet encryption. Packet authentication is performed using a hashing algorithm (MD5, SHA, etc.) which is used to hash the packet spanning the ESP header, the encrypted ESP payload (the tunnelled IP packet) and the payload padding (see figure 5-7, page 204). Packet encryption only spans the encrypted ESP payload and the payload padding and **not** the ESP header.

An ESP packet is only valid if the following checks are passed (the order is important):

- the authentication using the hashing algorithm is correct
- the sequence number is larger than all sequence numbers of all received **valid** esp packets (replay protection)
- the encryption of the ESP payload is successful (the is performed by a padding check)

This method was used already 10 years ago when hashing algorithms were much faster than encryption algorithms. The intention was to authenticate the packet before decryption in order to avoid an expensive decryption for unauthentic packets. With AES this assumption is no longer true. In fact AES is even faster than SHA.

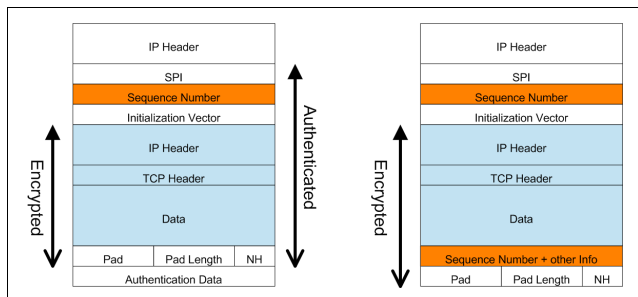
### The NoHash method is based on the following consideration:

Encryption can be used as authentication since only the VPN partner holding the same encryption session key may construct an ESP packet which will be correctly decrypted. The only problem by simply turning off the authentication would be that packets can be replayed using old (captured) ESP packet and replay it exchanging the sequence number



with a larger one. The receiver would trust the packet since the sequence number is not part of the encryption (see figure 5-7, page 204). This way a denial of service could be achieved.

**Fig. 5-7** ESP and NoHash



**The solution to this problem is quite simple:**

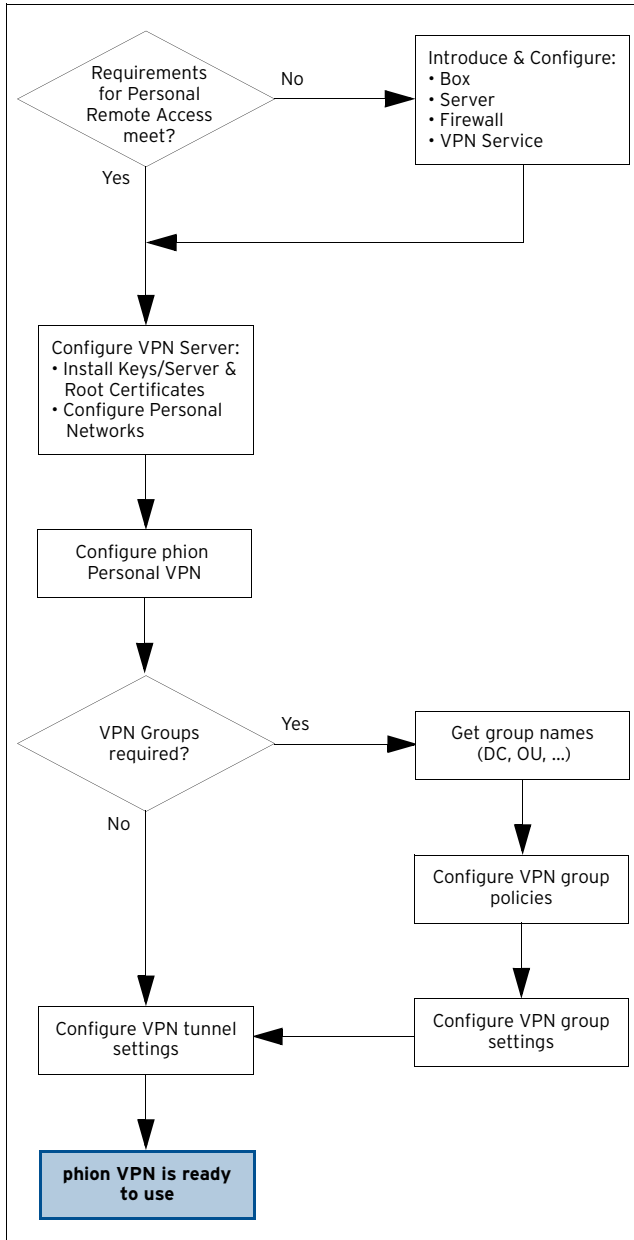
By including the sequence number redundantly in the encryption data of the ESP packet, tampering of the sequence number as described above is not possible. After decryption the two sequence numbers are simply compared and the packet discarded on mismatch.

As a consequence, ESP packets can be exchanged authenticated and encrypted with replay protection using only a single encryption step as long as the sequence number is part of the encrypted data. This leads to a significant performance improvement because the hashing operation can be skipped.

## 2. Configuring Personal Remote Access

### 2.1 VPN Configuration Block Diagram

Fig. 5-8 VPN configuration block diagram



The VPN Configuration can be opened in two ways:

- via config tree (🔧 **Config** > 📦 **Box** > 🏠 **Virtual Servers** > 🌐 <servername> > 📁 **Assigned Services** > 📁 <servicename> (**vpnserver**))
- via box menu (📦 **VPN**)

### 2.2 Introduce and Configure Box, Server, Firewall and VPN Service

Fig. 5-9 VPN configuration - Introduce and Configure block diagram

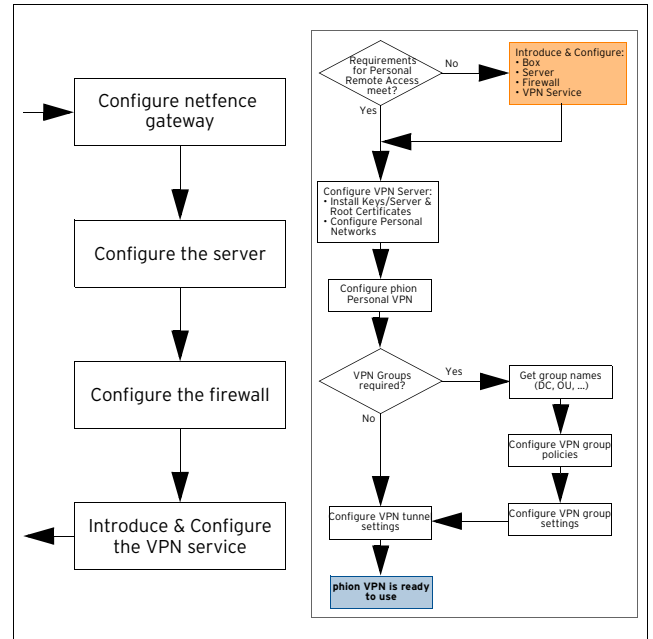


Table 5-3 VPN configuration - Introduce and Configure

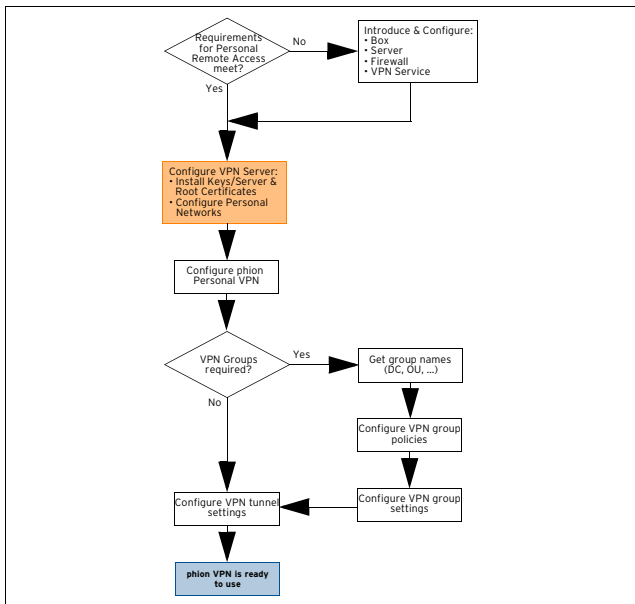
Issue	Description
Configure netfence gateway	<b>Configuration Service</b> - 2. Configuring a New System, page 48
Configure the server	<b>Configuration Service</b> - 3. Configuring a New Server, page 94
Configure the firewall	<b>Firewall</b> , page 123
Introduce & configure the VPN service	<b>Configuration Service</b> - 4. Introducing a New Service, page 97

**Note:**

If you are using **Additional Server IPs** entries in your server configuration, these IP addresses have to be configured as **Explicit Bind IPs** within the VPN Service Configuration.

## 2.3 Install Licenses and Configure Personal Networks

Fig. 5-10 VPN configuration block diagram - Configure VPN server



Normally, the phion firewall is delivered with one personal and unlimited firewall-to-firewall VPN license. All other licenses must be ordered from phion separately. For more detailed information about license activation see **Licensing**, page 497.

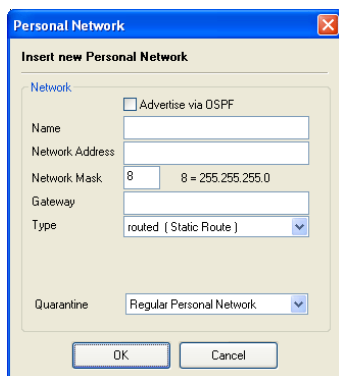
Additional personal licenses must be available as a file (\*.lic files) on floppy, hard disc, or as e-mail.

Configuring the server settings is done by clicking **VPN Settings** (accessible through **Config > Box > Virtual Servers > <servername> > Assigned Services > <servicename> (vpnserver)**) in the VPN configuration tree.

### 2.3.1 Personal Networks Tab

To create a VPN Personal network, lock the configuration dialogue, open the context menu and select **New VPN Network ...**. This opens the following configuration dialogue.

Fig. 5-11 Personal Network configuration dialogue



**Note:**

Maximum number of personal networks: 256.

**Note:**

The corresponding gateway routes for the configured personal network (both local and routed) are assigned to the VPN client automatically when connecting.

List 5-1 VPN configuration - Personal Network - section Network

Parameter	Description
<b>Advertise via OSPF</b>	By ticking this checkbox, the personal network is advertised via OSPF.
<b>Name</b>	This is the network name.
<b>Network Address</b>	This the network address.
<b>Network Mask</b>	Use phion notation ( <b>Getting Started - 5. phion Notation</b> , page 25).
<b>Gateway</b>	This is the client's gateway address.
<b>Type</b>	Type of VPN network used. Available types are: <ul style="list-style-type: none"> <li>➤ <b>routed (Static Route)</b> (virtual network/DMZ) (for illustrated example see figure 5-12) A separate net is offered. A static route leads to the local network via the VPN server. VPN client addresses can be distributed through DHCP as fixed or dynamic one.</li> <li>➤ <b>local (Proxy ARP)</b> (for illustrated example see figure 5-13, page 206) A part of the local network is offered via VPN. The defined addresses are entered as Proxy ARP on the VPN Server (see figure 5-12). VPN client addresses can be distributed through DHCP as fixed or dynamic ones. The following two values have to be defined additionally:                             <ul style="list-style-type: none"> <li><b>IP Range Base</b> - defines the starting point of the offered addresses from the local network</li> <li><b>IP Range Mask</b> - defines the scope of the offered addresses</li> </ul> </li> </ul>
<b>Quarantine</b>	Quarantine networks may be defined in order to assort clients accessing a VPN tunnel into separate network classes. This configuration parameter has been introduced in preparation for VPN client release R8. It will not work with the current VPN client release R7 or older versions. The recommended setting for all netfence versions is to leave the setting at the default value <b>Regular Personal Network</b> when creating a new Personal Network. Quarantine Network Classes momentarily will not be effective.

Fig. 5-12 VPN configuration with Routed Network (Static Route; virtual network/DMZ)

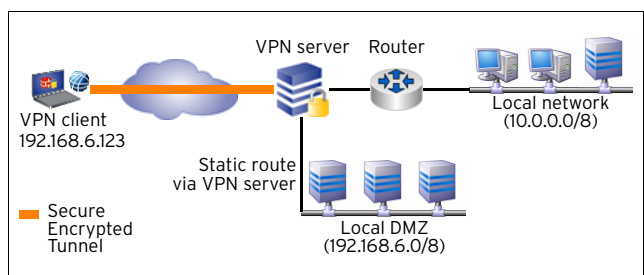
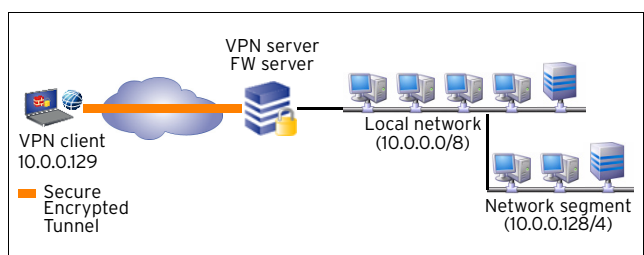


Fig. 5-13 VPN configuration with Local (Proxy ARP)



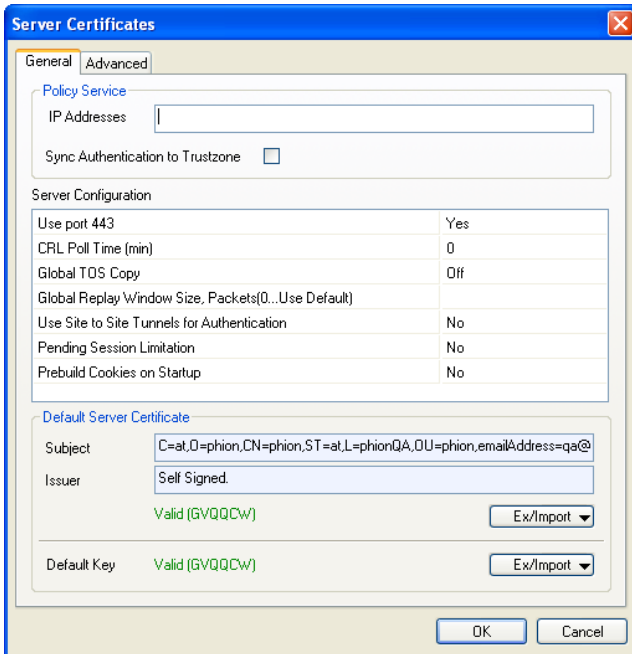
## 2.3.2 Server Key/Settings Tab

Manage server keys and certificates through this configuration dialogue.

### 2.3.2.1 Server Certificates

To open the *Server Certificates* window, click the **Click here for Server Settings** link on top of the *Server Key/Settings* tab:

Fig. 5-14 Server Certificates configuration



#### Tab *General*.

List 5-2 VPN configuration - Server Certificates - General - section Policy Service

Parameter	Description
<b>IP Addresses</b>	Define here the IP address of the policy service to use.
<b>Sync Authentication to Trustzone</b>	Set to <b>yes</b> if authentication information should be propagated to the other boxes in the same trustzone. Set to <b>no</b> to disable authentication synchronisation.

List 5-3 VPN configuration - Server Certificates - General - section Server Configuration

Parameter	Description
<b>Use port 443</b> [default Yes]	Defines, whether incoming VPN connections on port 443 should be accepted or not. In some cases you might want to disable using port 443 for incoming VPN connections, for example connections arriving at port 443 should be redirected by the firewall service to another machine.
<b>CRL Poll Time</b>	Defines the time interval (in minutes) for fetching the Certificate Revocation List. <b>Note:</b> Setting this parameter to value 0 results in a poll time of 15 minutes.
<b>Global TOS Copy</b> [Off]	This setting globally defines the ToS (Type of Service) flag for <b>Site to Site</b> tunnels. Global employment of the ToS flag is disabled by default (setting: <b>Off</b> ). Effects of ToS settings are described in detail in <b>VPN Envelope Policy</b> (applying to TINA Tunnels, page 226) and list 5-55, page 228 (applying to IPsec Tunnels, page 228). Individual tunnel ToS policies override the global policy settings.

List 5-3 VPN configuration - Server Certificates - General - section Server Configuration

Parameter	Description
<b>Global Replay Window Size</b> [0]	The <b>Replay Window Size</b> is designed for sequence integrity assurance and avoidance of IP packet "replaying", when due to ToS policies assigned to VPN tunnels and/or transports packets are not forwarded instantly according to their sequence number. The window size specifies a maximum number of IP packets that may be on hold, until it is assumed that packets have been sent repeatedly and sequence integrity has been violated. Individual window size settings (see <b>Replay Window Size</b> , page 226) are configurable per tunnel and transport, overriding the global policy settings. Setting to <b>0</b> (default) defines that these tunnel/transport specific settings should be used. ToS details are described in <b>VPN Envelope Policy</b> , page 226. The effective <b>Replay Window Size</b> is visualised in the Transport Details window (Attribute: transport_replayWindow), which can be accessed by double-clicking the tunnel in the <b>VPN Monitoring GUI &gt; Active</b> tab (see 3. Monitoring, page 229).
<b>Use Site to Site Tunnels for Authentication</b> [Yes]	Normally a tunnel registers itself at the firewall causing an auth.db entry with the tunnel network and the tunnel credentials. This can be used to build firewall rule having the tunnel name or credentials as condition. This feature is rarely used (maybe not at all).
<b>Pending Session Limitation</b> [Yes]	Session buildup is limited that once a buildup of 5 sessions is detected any further session request will be dropped until one of the already initiated sessions is completed.
<b>Prebuild Cookies on Startup</b> [No]	Normally cookie are built on demand. For many tunnel building up simultaneously it is better to have the cookie already precalculated. This causes a slower VPN service startup but a faster tunnel buildup afterwards.

List 5-4 VPN configuration - Server Certificates - General - section Default Server Certificate

Parameter	Description
<b>Subject/Issuer</b>	These two fields display certificate subject and issuer. <b>Note:</b> L2TP/IPSEC require server certificates with <b>SubAltNames</b> .
<b>Default Key</b>	If the VPN server demands a key but the key is not stated explicitly, it may be generated by clicking the <b>Ex/Import</b> button and selecting a suitable option.

#### Tab *Advanced*.

List 5-5 VPN configuration - Server Certificates - Advanced - section Device Configuration

Parameter	Description
<b>Device Index</b>	Click the <b>Add ...</b> button to open the <b>VPN Device Properties</b> window and to add virtual interfaces equipped with unique index numbers. Indexed virtual interfaces may for example be needed for direct OSPFv2/RIP multicast propagation of VPN networks. After assigning the interface with a local IP address it may be directly used within the OSPF router configuration. The interfaces become active and visible in the <b>Control &gt; Network</b> tab of the corresponding box as soon as a tunnel endpoint using the indexed interface has been created. Indexed VPN interfaces are labelled in the following way: <b>vpn[INDEX]</b> (for example, <b>vpn1, vpn2, ...</b> ).
<b>MTU</b>	Specify the MTU (Maximum Transmission Unit) size in this field ( <b>1398 / 1500</b> ).
<b>IP Addresses</b>	Insert the IP addresses that should be started on the vpnX interface into this field. Separate multiple entries with spaces.
<b>Multicast Addresses</b>	Insert the multicast addresses that should be propagated into this field. For example, to transport OSPF multicast via VPN tunnel, insert "224.0.0.5 224.0.0.6". Separate multiple entries with spaces.

List 5-6 VPN configuration - Server Certificates - Advanced - section IKE Parameters

Parameter	Description
<b>IKE Parameters</b>	The IKE (Internet Key Exchange) Parameters section is globally applicable to all configured IPSEC tunnels.

List 5-6 VPN configuration - Server Certificates - Advanced - section IKE Parameters

Parameter	Description
<b>Exchange Timeout (s)</b>	This value defines the maximum period to wait until the request for IPsec tunnel connection establishment has to be approved by the remote peer (default: <b>30</b> seconds).
<b>Tunnel Check Interval (s)</b>	This value defines the interval in which to query if a valid exchange is assignable to an IPsec tunnel (default: <b>5</b> seconds). In case a tunnel configured with direction assignment <b>Active</b> has been terminated, it will be re-established automatically as soon as the check interval has expired. In case a tunnel configured with direction assignment <b>Passive</b> has been terminated, a corresponding status message will be triggered causing a GUI update in the VPN monitoring view (3. Monitoring, page 229).
<b>Dead Peer Detection Interval (s)</b>	This value defines the interval in which to execute keep alive checks on the remote peer (default: <b>5</b> seconds).
<b>Use IPsec dynamic IP</b>	Set to <b>Yes</b> if the the service is connected to the internet via dynamic link (dynamic IP address). In this case the server IP address is not yet known at configuration time and IKE then listens to all local IP addresses.
<b>IPsec Log Level</b>	Defines the debug log level of IKE. <b>Note:</b> Debug log may be very "noisy". Avoid a log level greater than 0 if not required for solving an issue.

List 5-7 VPN configuration - Server Certificates - Advanced - section Custom Ciphers

Parameter	Description
	For internal use only

## 2.3.3 Root Certificates Tab

This tab allows importing and viewing of root certificates that have been issued to the VPN server by a **Certificate Authority (CA)**. Root certificates that may be imported have to be available as either **.cer** or phion proprietary **.pem** files.

### 2.3.3.1 Certificate Details Tab

To import a new root certificate, lock the **Root Certificates** tab, then right-click into the configuration window, then select a suitable **Import** option, depending on the format the certificate is available in.

The following configuration options are available:

List 5-8 VPN configuration- Root Certificates - Certificate details tab - section Certificate

Parameter	Description
	This section shows the certificate's <b>Subject</b> and <b>Issuer</b> . Into the <b>Name</b> field, insert a certificate name for easier recognition.

List 5-9 VPN configuration- Root Certificates - Certificate details tab - section Usage

Parameter	Description
	This section contains options that define which tunnel types a certificate should be valid for. The following tunnel types are available for selection: <b>Phion Personal</b> , <b>Phion Site-to-Site</b> , <b>IPsec Personal</b> , <b>IPsec Site-to-Site</b> .
<b>Comment</b>	Into this field, optionally insert a certificate description.

List 5-10 VPN configuration- Root Certificates - Certificate details tab - section CRL error handling

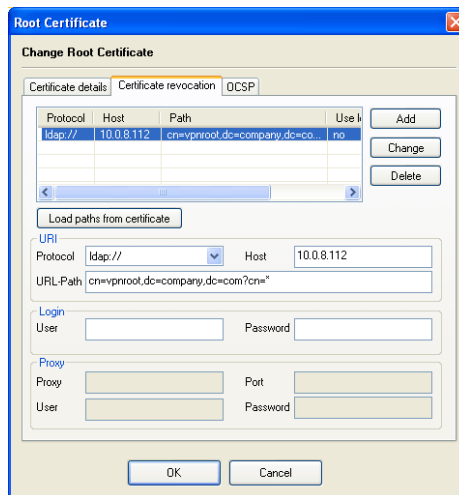
Parameter	Description
	This section defines actions that should be taken in case the <b>Certificate Revocation List (CRL)</b> a certificate refers to is unavailable.

List 5-10 VPN configuration- Root Certificates - Certificate details tab - section CRL error handling

Parameter	Description
<b>Timeout (min.)</b>	If all URIs of the root certificate fail then the fetching process is started again after this time period. In case of the CRL is still not available, the fetching process is stopped and parameter Action (see below) is activated.
<b>Action</b>	The following actions are available if CRL fetching is not possible: <ul style="list-style-type: none"> <li>➤ <b>Terminate all sessions</b> Every VPN session relating to this root certificate is terminated.</li> <li>➤ <b>Do not allow new sessions</b> New VPN session relating to this root certificate are not allowed.</li> <li>➤ <b>Ignore</b> This option creates a log entry, but does not have any affect to VPN connections relating to this root certificate.</li> </ul>

### 2.3.3.2 Certificate Revocation Tab

Fig. 5-15 Certificate Revocation tab



This tab allows specifying paths to CRLs.

If a CRL is already included in the certificate, import the CRL URI by clicking the **Load paths from certificate** button.

To add a CRL URI manually, insert the CRL details into the fields available in the **URI**, **Login** and **Proxy** sections and then click the **Add** button.

List 5-11 VPN configuration - Root Certificates - Certificate revocation tab - section URI

Parameter	Description															
<b>Protocol</b>	From this list, select the needed connection protocol. The following protocols are available: <table border="1" style="width: 100%; margin-top: 5px;"> <thead> <tr> <th>Protocol</th> <th>Default port</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>LDAP</td> <td>389</td> <td>DNS resolvable</td> </tr> <tr> <td>LDAPS</td> <td>636</td> <td></td> </tr> <tr> <td>HTTP</td> <td>80</td> <td></td> </tr> <tr> <td>HTTPS</td> <td>443</td> <td></td> </tr> </tbody> </table> <b>Note:</b> In LDAP directories, valid CRL file types are restricted to <b>.pem</b> and <b>.crt</b> files.	Protocol	Default port	Comment	LDAP	389	DNS resolvable	LDAPS	636		HTTP	80		HTTPS	443	
Protocol	Default port	Comment														
LDAP	389	DNS resolvable														
LDAPS	636															
HTTP	80															
HTTPS	443															
<b>Host</b>	Into this field insert the DNS resolvable host name or IP address of the server that makes the CRL available.															



**List 5-11** VPN configuration - Root Certificates - Certificate revocation tab - section URI

Parameter	Description
<b>URL-Path</b>	<p>Into this field insert the path to the Certificate Revocation List (CRL) (for example <code>cn=vpnroot,ou=country,ou=company,dc=com?cn=*</code>).</p> <p><b>Note:</b> When the CRL is made available through SSL encrypted LDAP (LDAPS) take the following into consideration: To enable connection establishment, the CRL has to be referred to by using the fully qualified domain name (that is the resolvable host name) in the CN subject. For example, if a server's host name is <code>server.domain.com</code> it has to be stated in the URL-path as follows: <code>cn=vpnroot,ou=country,ou=company,dc=com,cn=server.domain.com</code>.</p> <p><b>Note:</b> The A-Trust LDAP server requires that a CRL distribution point referring to it <b>MUST</b> terminate with a CN subject. Therefore, as from netfence 3.6.3 when loading the CRL from a certificate, the search string "<code>?cn=*</code>" will automatically be appended, if the CRL is referring to an LDAP server and if a search string (CN subject) is not available in the search path by default. Note that existing configurations will remain unchanged and that the wildcard CN subject does not conflict with other LDAP servers.</p>

**List 5-12** VPN configuration - Root Certificates - Certificate revocation tab - section Login

Parameter	Description
<b>User / Password</b>	Into these fields, insert user name and corresponding password if the LDAP/HTTP server requires authentication.

**List 5-13** VPN configuration - Root Certificates - Certificate revocation tab - section Proxy

Parameter	Description
<b>Proxy</b>	Into this field insert the DNS resolvable host name or IP address of the proxy server.
<b>Port</b>	Into this field insert the port of the proxy server that is used for connection requests.
<b>User / Password</b>	Into these fields, insert user name and corresponding password if the proxy server requires authentication.

### 2.3.3.3 OCSP Tab

**List 5-14** VPN configuration- Root Certificates - OCSP tab - section OCSP Server

Parameter	Description
<b>Host</b>	Here the corresponding DNS-resolvable hostname or the host IP address has to be entered.
<b>Port</b>	This parameter holds the port the OCSP server is listening on.
<b>Use SSL</b> checkbox	Ticking this checkbox enforces a SSL connection to the OCSP server.
<b>Phibs Scheme</b>	Allows selection of an OCSP scheme (default: <i>ocsp</i> ).

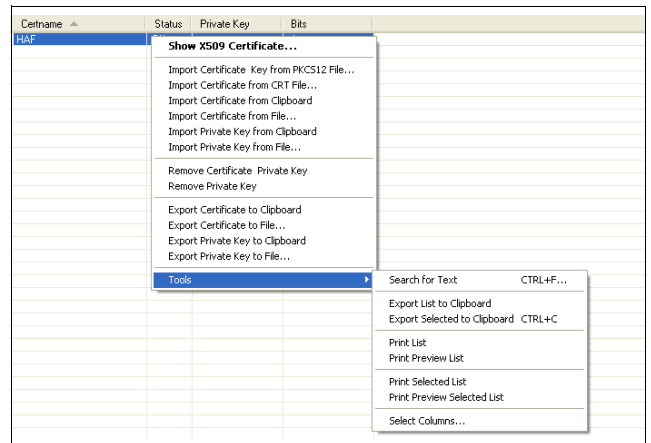
**List 5-15** VPN configuration- Root Certificates - OCSP tab - section OCSP Server Identification

Parameter	Description
<b>CA Root</b>	<p>This parameter specifies how the OCSP server is verified. The following options are available: <b>This root certificate</b> - The OCSP server certificate signing the OCSP answer was issued by this root certificate. <b>Other root certificate</b> - The OCSP server certificate signing the OCSP answer was issued by another root certificate. This other root certificate has to be imported via parameter Other root (see below).</p> <p><b>Note:</b> Take into consideration that the extended certificate usage is set to <b>OCSP signing</b> in the OCSP-server certificate when using <b>This root certificate</b> or <b>Other root certificate</b>. <b>Explicit Server certificate</b> - The OCSP server certificate signing the OCSP answer may be self-signed or another certificate. This X.509 certificate has to be imported via parameter Explicit X.509 (see below).</p>
<b>Other root</b>	If <b>CA Root</b> parameter is set to <b>Other root certificate</b> this certificate has to be imported via the <b>Ex/Import</b> button (either in PEM or PKCS12 format).
<b>Explicit X509</b>	If <b>CA Root</b> parameter is set to <b>Explicit Server certificate</b> this certificate has to be imported via the <b>Ex/Import</b> button (either in PEM or PKCS12 format).

## 2.3.4 Server Certificates Tab

This tab displays the available server certificates.

**Fig. 5-16** Server certificates with open context menu



As shown in figure 5-16 the context menu of this configuration tab provides multiple ways for import, removal, and export of certificates.

## 2.4 Configuring VPN GTI Settings

VPN GTI Settings configuration is only of interest for MC-administered boxes. It determines default settings applying to tunnels when they are created by use of the VPN GTI Editor. The functionality of the VPN Graphical

Tunnel Interface (GTI) is described in **phion management centre** - 15. VPN GTI, page 464.

**Note:**

Merging of local **VPN GTI Settings** (as configured through the parameters below on each box) and global **VPN Settings** (applying for a specific VPN group, see 15.2.2 Defining Global Settings for a VPN Group, page 466) determines the initial default settings of VPN servers and tunnels when they are introduced in the graphical tunnel interface on the management centre.

The following parameters specify a VPN server's default settings:

List 5-16 VPN configuration- VPN GTI Settings

Parameter	Description
<b>My IP Type</b>	<p>Defines which IP address(es) to use when a VPN connection is established:</p> <ul style="list-style-type: none"> <li>➤ <b>&lt;default&gt;</b>- Utilises all Bind IPs configured in the VPN server's service configuration section. The VPN connection then binds to the first available IP chosen from the pool.</li> <li>➤ <b>First-IP</b>- Utilises the VPN server's First IP.</li> <li>➤ <b>Second-IP</b>- Utilises the VPN server's Second IP.</li> <li>➤ <b>Dynamic (via routing)</b>- Utilises a dynamically assigned IP address according to the routing table.</li> <li>➤ <b>Explicit</b>- Allows assignment of an explicit IP address or interface name in the <b>My IP Explicit</b> field below.</li> </ul> <p><b>Note:</b> Remember that explicitly assigned IP addresses have to be included in the service configuration as well.</p>
<b>My IP Explicit</b>	<p>This field expects specification of an explicit IP address, if <b>My IP Type</b> has been set to <b>Explicit</b>.</p> <p><b>Note:</b> Insertion of <b>interface names</b> into the <b>My IP Explicit</b> parameter is additionally possible in the configuration area of the VPN GTI Editor.</p>
<b>My Peer Type</b>	<p>Defines the IP address(es) on which to accept VPN connection establishment:</p> <ul style="list-style-type: none"> <li>➤ <b>&lt;default-from-My-IP&gt;</b>- Accepts connections on all Bind IPs configured in the VPN server's service configuration section. The VPN connection then binds to the first available IP chosen from the pool.</li> <li>➤ <b>First+Second-IP</b>- Accepts connections on the VPN server's First and Second IP.</li> <li>➤ <b>First-IP</b>- Accepts connections on the VPN server's First IP.</li> <li>➤ <b>Second-IP</b>- Accepts connections on the VPN server's Second IP.</li> <li>➤ <b>Explicit</b>- Specifies connection acceptance for explicitly assigned IP addresses, interface names or host names as defined in the <b>My Peer IP Explicit</b> field below.</li> </ul> <p><b>Note:</b> This data will be used for both partners (active/passive) of the VPN tunnel. Due to this, only <b>explicit</b> IP addresses can be configured.</p>
<b>My Peer IP Explicit</b>	<p>This field expects specification of an explicit IP address, if <b>My Peer Type</b> has been set to <b>Explicit</b>.</p> <p><b>Note:</b> Insertion of <b>interface names</b> or <b>host names</b> (if DNS resolution is available) into the <b>My Peer IP Explicit</b> parameter is additionally possible in the configuration area of the VPN GTI Editor.</p>
<b>Use ospf</b>	<p>Setting to <b>yes</b> (default: <b>no</b>) causes that the configured VPN information is advertised via OSPF.</p>

List 5-17 VPN configuration- VPN GTI Settings - section Proxy

Parameter	Description
<b>Proxy Type</b>	<p>Defines the type of proxy that is to be used; The following settings are available: <b>Direct (no-Proxy)</b>, <b>HTTP-Proxy</b>, <b>Socks-4-Proxy</b>, <b>Socks-5-Proxy</b>.</p>
<b>Proxy Address</b>	<p>Defines the proxy server's IP address or DNS-resolvable host name.</p>
<b>Proxy User / Password</b>	<p>Defines user and password for authentication on the proxy.</p>

List 5-17 VPN configuration- VPN GTI Settings - section Proxy

Parameter	Description
<b>Accept Identification Type</b>	<p>Defines the identification type required for VPN access. The following authentication methods may be used:</p> <ul style="list-style-type: none"> <li>➤ <b>Public Key</b></li> <li>➤ <b>X509 Certificate (CA signed)</b></li> <li>➤ <b>X509 Certificate (explicit)</b></li> <li>➤ <b>Box SCEP Certificate (CA signed)</b>.</li> </ul>

## 2.5 Configuring L2TP/PPTP Settings

To access the configuration file for L2TP and PPTP select **Config** > **Box** > **Virtual Servers** > **Assigned Services** > **<servicename> (vpn)** > **L2TP/PPTP Settings**.

The file itself consists of the following sections:

- **General**
- **L2TP/IPSEC**
- **PPTP**
- **User List** (page 211)

### 2.5.1 General

List 5-18 VPN configuration- L2TP/PPTP Settings - General - section Common Settings

Parameter	Description
<b>Maximum Transmission Unit</b>	<p>This parameter defines the maximum packet size that will be sent without fragmentation (default: <b>1400</b>).</p>
<b>Maximum Receive Unit</b>	<p>This parameter defines the maximum packet size that will be accepted (default: <b>1400</b>).</p>
<b>First / Second DNS</b>	<p>Enter the IP address of the primary/secondary DNS server here.</p>
<b>First / Second WINS</b>	<p>Enter the IP address of the primary/secondary WINS server here.</p>
<b>Static IP</b>	<p>Set this parameter to <b>yes</b>, if static IP assignments are required (default: <b>no</b>).</p>

### 2.5.2 L2TP/IPSEC

**Note:**

L2TP is not enabled by default. Set **Enable L2TP** to **yes** to activate the configuration section below.

**Note:**

Connecting to the phion VPN service using the L2TP client of Windows Vista or Windows Vista SP1 may lead to unexpected connection termination. The outcome of an in-depth analysis is that the Microsoft Vista L2TP client suddenly terminates an already established connection without even notifying the VPN service. Usually the L2TP client terminates the connection after a period of 60 seconds. It may be possible that the issue is not related to the netfence VPN/L2TP service but a wrong behaviour of the L2TP client system.

**Note:**

Please consult 2.3.2 Server Key/Settings Tab, page 207, for information concerning certificate requirements.

**Fig. 5-17** Configuration Dialogue for L2TP

**List 5-19** VPN configuration- L2TP/PPTP Settings - L2TP/IPSEC - section L2TP Settings

Parameter	Description
<b>L2TP Bind IP</b>	Here enter the IP address of the VPN server that listens for VPN connection requests.
<b>IPSec PSK</b>	This parameter holds the <b>Pre-Shared Key</b> for IPsec/IKE authentication. <b>Attention:</b> The character # is not allowed.
<b>Local Tunnel IP</b>	This parameter holds the server-side IP address of the tunnel.
<b>Pool IP-Begin</b>	This parameter defines the starting IP address for the IP-address pool available to clients.
<b>Pool Size</b>	This parameter defines the number of available pool IP addresses (for example <b>Pool IP-Begin</b> 10.0.8.10 and <b>Pool Size</b> 2 results in IP addresses 10.0.8.10 and 10.0.8.11).
<b>LCP Echo Failure / LCP Echo Interval</b>	This parameters indicate the maximum number of lost echoes and the time period a echo reply may last (default for both parameters: <b>0</b> ).
<b>Idle Timeout</b>	If this value (in seconds; default: <b>300</b> ) is exceeded without having traffic over the VPN tunnel, the connection is terminated.
<b>User Authentication</b>	Choose a user authentication: <b>Local-use-database</b> or <b>Remote MS-CHAP-v2</b> .
<b>Phase 1 Lifetime (s)</b>	The default IPsec phase 1 lifetime for all L2TP clients.
<b>Max. phase 1 Lifetime (s)</b>	The maximum IPsec phase 1 lifetime for all L2TP clients.
<b>Min. phase 1 Lifetime (s)</b>	The minimum IPsec phase 1 lifetime for all L2TP clients.

### 2.5.3 PPTP

**Note:**

PPTP is not enabled by default. Set **PPTP Enable** to **yes** to activate the configuration section below.

**List 5-20** VPN configuration- L2TP/PPTP Settings - PPTP - section PPTP Settings

Parameter	Description
<b>PPTP Bind IP</b>	In this field enter the IP address of the VPN server that listens for VPN connection requests.
<b>Initiation Timeout [s]</b>	The timeout parameter defines the maximum time for establishing the GRE tunnel (default: <b>10</b> ). As a rule of thumb it can be said that the faster the connection the shorter this timeout can be set.
<b>Local Tunnel IP</b>	Enter the server-side IP address of the tunnel here.
<b>Pool IP-Begin</b>	This parameter defines the starting IP address for the IP-address pool available to clients.
<b>Pool Size</b>	This parameter defines the number of available pool IP addresses (for example, Pool IP-Begin 10.0.8.10 and Pool Size 2 results in IP addresses 10.0.8.10 and 10.0.8.11).
<b>MPPE Encryption Strength</b>	This parameter defines the required encryption strength ( <b>40bit</b> , <b>128bit</b> (default) or <b>election</b> ). The option <b>election</b> causes that the strongest available encryption will be used.
<b>LCP Echo Failure / LCP Echo Interval</b>	These parameters indicate the maximum number of lost echoes and the time period a echo reply may last (default for both parameters: <b>0</b> ).
<b>Idle Timeout</b>	If this value (in seconds; default: <b>300</b> ) is exceeded without having traffic over the VPN tunnel, the connection is terminated.
<b>User Authentication</b>	Choose a user authentication: <b>Local-use-database</b> or <b>Remote MS-CHAP-v2</b> .

### 2.5.4 User List

This section handles the client user names and passwords (**Challenge Handshake Authentication Protocol**).

To add a new entry click button **Insert ...** To modify an existing entry select the entry and click button **Edit ...** To remove an entry from the list select the entry and click button **Delete**.

Creating a new entry and modifying an existing entry works via the same Configuration Dialogue (figure 5-18).

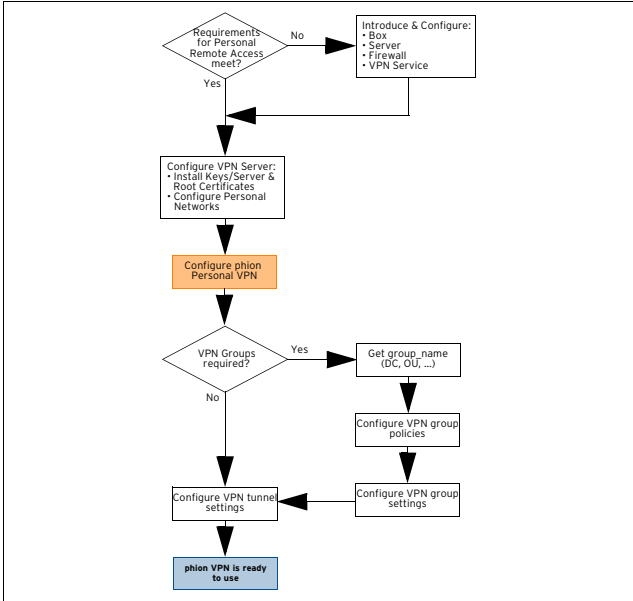
**Fig. 5-18** Configuration Dialogue for Chap Secrets






**List 5-21** VPN configuration- L2TP/PPTP Settings - User List

Parameter	Description
<b>Username</b>	Defines the user's name.
<b>Password / Confirm / Current</b>	Enter the (new) password and confirm it by re-entering into the confirm field (existing entries <b>require</b> the current password to unlock the fields <b>Password</b> and <b>Confirm</b> ).
<b>IP Address</b>	This IP address is used for static assignment (list 5-18, <b>Static IP</b> , page 210).

## 2.6 Configuring Personal VPN

Fig. 5-19 VPN configuration block diagram - Configure phion Personal VPN



The  **Client to Site** item (accessible through  **Config** >  **Virtual Servers** >  **Assigned Services** >  <servicename> (**vpnserver**) is used for configuring remote VPN connections between a netfence gateway and the entegra VPN client with usage of phion certificates and private-public key pairs (no groups) (see 1.4.2.1 phion Client to Site VPN, phion x.509 certificate, page 201).

### 2.6.1 Phion VPN CA Tab

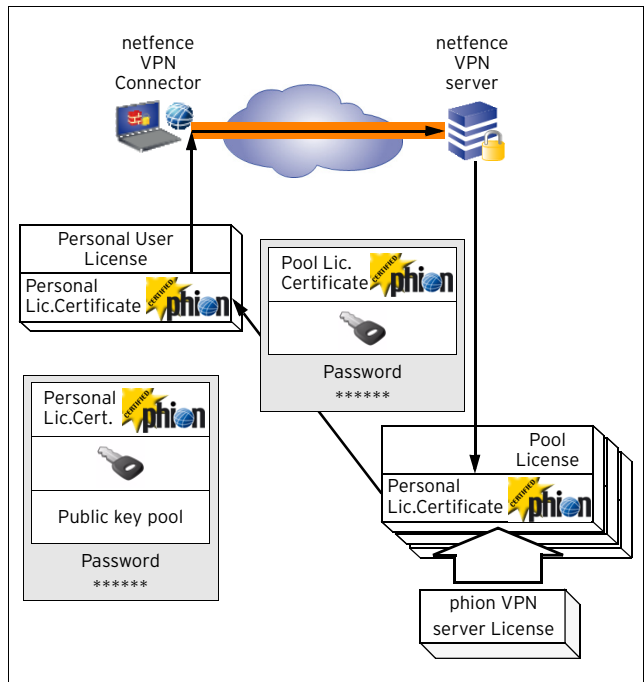
This tab is used for management (which means import and removal) of pool licenses as well as for management (creation, cloning, and removal) of personal licenses. In addition, the options provided allow customising graphics and messages displayed to the client user and security routines (for example registry checks on the client's workstation, management of the personal firewall, ...).

#### 2.6.1.1 Pool Licenses Tab

When buying a phion netfence product, a VPN server license is distributed with one Personal License. All

additional VPN Pool Licenses must be purchased from phion.

Fig. 5-20 Heredity of phion certificates



**Note:**

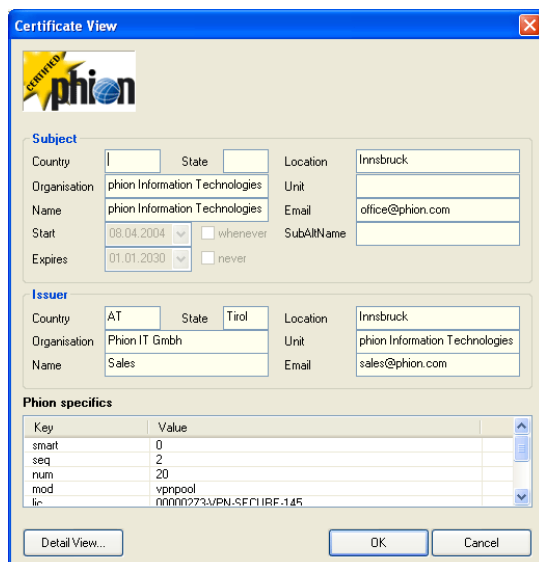
VPN Pool Licenses have to be imported into the **Personal VPN** section of the VPN server. Do not treat VPN Pool Licenses like box licenses and do not import them into the Pool License section of the global MC Identity settings.

To install a VPN Pool License, right-click into the main window of the **Pool Licenses** tab and select whether to import from file or from clipboard.

If the Pool License has been delivered to you in a .lic file, import it by selecting **Insert License from File ...** from the context menu.

The Pool License Certificate appears after submission and confirmation of the password defined at purchase.

Fig. 5-21 Pool License Certificate









**List 5-24** VPN configuration - Client to Site - Phion VPN CA tab - Personal License creation - section Password and Peer Restriction

Parameter	Description
<b>VPN-Type</b>	Select the appropriate option: ↗ <b>Personal + SSL</b> ↗ <b>Personal Only</b> or ↗ <b>SSL Only</b>  <b>Note:</b> This parameter takes effect when - connecting via SSL-VPN - Authentication Scheme <b>Local</b> is selected.
<b>Change Server Password ...</b> button	Change the password needed for connection to the VPN server.
<b>ACL list</b>	Access Control List for VPN connections. The client is only allowed to connect to the VPN server from one of these IP addresses or address ranges.

**List 5-25** VPN configuration - Client to Site - Phion VPN CA tab - Personal License creation - section Active Certificate / Obsolete Certificate

Parameter	Description
	<b>Note:</b> The Usage listing to the right defines whether only the active key is permitted or both active AND obsolete key.
<b>License Type</b> pull-down menu	Type of license;  <b>File</b> or  <b>Certificate Store</b> based.
<b>Server Key</b> pull-down menu	Choose a pre-defined server private key.
<b>Edit Certificate ...</b> button	Edit the information of the VPN certificate.
<b>Create New Key</b> button	Create a new user private key.
<b>Import Key ...</b> button	Import a user private key either from clipboard or from file.
<b>Copy to Obsolete</b> button	Copy the current certificate to obsolete. This way it is possible to create a new certificate without losing the information of the old one.
<b>Usage</b> pull-down menu	Selects whether the user can only log in with the active certificate or also with a certificate that is set to obsolete status.
<b>Export to Clipboard ...</b> button	Export the certificate to the clipboard. Clicking the button opens a dialogue where you can additionally protect the certificate with a password.
<b>Export to File ...</b> button	Export the certificate to a file. You have to choose whether you want to protect the certificate with a password or not.
<b>Export Issuer Cert ...</b> button	Exports the issuer certificate to a .cer-file.
<b>Certificate Mgmt ...</b> button	Clicking this button opens the <b>Phion Crypto Provider Frame</b> .

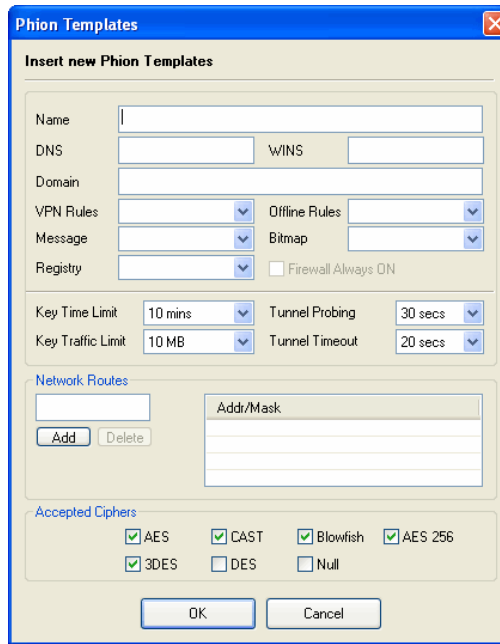
### 2.6.1.2 Templates Tab

This tab lists all templates that have been introduced on this VPN server.

Templates contain sets of parameters (DNS server IP, WINS server IP, ...) needed for personal VPN access. Define templates with pre filled-in frequently used data content, to facilitate VPN client profile administration.

To create a new template lock the dialogue, and click **New Template** in the context menu.

**Fig. 5-24** Template configuration



**List 5-26** VPN configuration - Client to Site - Phion VPN CA tab - phion Template creation

Parameter	Description
<b>Name</b>	Name of the template (for example, the name of the user the template will be assigned to).
<b>DNS</b>	IP address of the DNS server that is assigned to the client.
<b>WINS</b>	IP address of the WINS server that is assigned to the client.
<b>Domain</b>	DNS domain that is assigned to the client.
<b>VPN Rules</b>	From this list, a rule set may be selected and therewith assigned to a VPN client's personal firewall during an active VPN connection (6. Configuring the Personal Firewall, page 241).
<b>Offline Rules</b>	From this list, a rule set may be selected and therewith assigned to a VPN client's personal firewall. The offline rule set is applicable while the client is not connected to a VPN server. Note that the <b>Offline Rule Set</b> overwrites a possibly existing user customised rule local set defined in the personal firewall on the client itself (6. Configuring the Personal Firewall, page 241).
<b>Message</b>	From this list a predefined welcome message (see 2.6.3 Messages Tab, page 219) may be selected and therewith assigned to a VPN client.
<b>Bitmap</b>	From this list a predefined bitmap (see 2.6.4 Pictures Tab, page 219) may be selected and therewith assigned to a VPN client.
<b>Key Time Limit</b>	This parameter defines the period of time after which the re-keying process is started. Possible settings are <b>5</b> , <b>10</b> (default), <b>30</b> and <b>60</b> minutes.
<b>Key Traffic Limit</b>	This parameter defines the amount of traffic after which the re-keying process is started. Possible settings are: <b>No Limit</b> <b>50 MB</b> <b>10 MB</b> (default) <b>5 MB</b> <b>1 MB</b>
<b>Tunnel Probing</b>	The probing parameter defines the interval of sent probes. If such a probe is not answered correctly, the parameter <b>Tunnel Timeout</b> (see below) is in charge. The available time settings (in seconds) for the probing parameter are: - <b>silent</b> (no probes are sent; disables the parameter) - <b>10 secs</b> - <b>20 secs</b> - <b>30 secs</b> (default) - <b>60 secs</b>



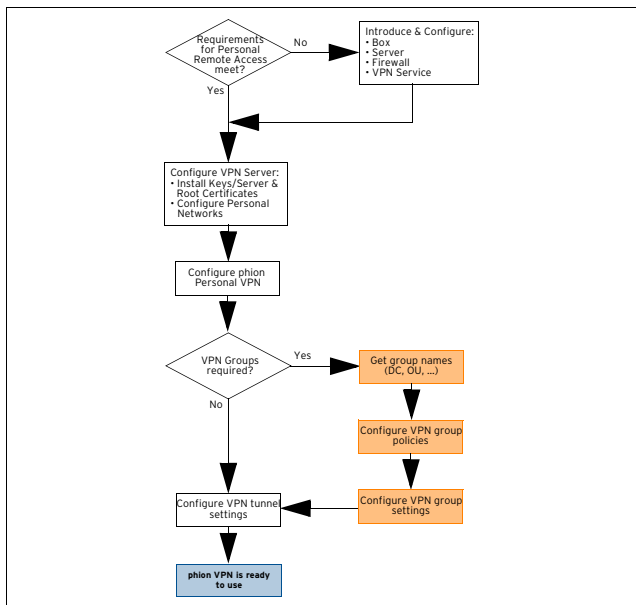
**List 5-26** VPN configuration - Client to Site - Phion VPN CA tab - phion Template creation

Parameter	Description
<b>Tunnel Timeout</b>	<p>If for some reason the enveloping connection breaks down the tunnel has to be re-initialised. This is extremely important for setups with redundant possibilities to build the enveloping connection. The timeout parameter defines the period of time after which the tunnel is terminated. The available settings (in seconds) for the timeout parameter are:</p> <ul style="list-style-type: none"> <li>- <b>10 secs</b></li> <li>- <b>20 secs</b> (default)</li> <li>- <b>30 secs</b></li> <li>- <b>60 secs</b></li> </ul> <p><b>Note:</b> The choice of the ideal timeout parameter strongly depends on the availability and stability of the connection. phion recommends setting the timeout to <b>30 seconds for internet connections</b> and to <b>10 seconds for intranet connections</b> or connections over a dedicated line.</p>
<b>Network Routes</b>	<p>Routes assigned to the client when connecting to the VPN server.</p> <p><b>Note:</b> You may define up to 63 network routes.</p>
<b>Accepted Ciphers</b>	<p>Specifies the encryption method allowed for users of this template when connecting to the VPN server.</p>

## 2.6.2 External CA Tab

### 2.6.2.1 Configuring Group VPN

**Fig. 5-25** VPN configuration block diagram - Configure Group VPN



Group VPN allows specification of global settings for VPN personal tunnels using an external x.509 certificate. Furthermore group configurations concerning the used authentication scheme or certificate can be defined.

### 2.6.2.2 Gathering Group Names

In order to have a working group VPN, you will have to know the proper group names. The corresponding group names can be obtained from your assigned administrator.

**Note:**

If you are using MSAD or LDAP the distinguished names are used for group\_name; please have a look at **Appendix - 1.1 How to gather Group Information**, page 524.

### 2.6.2.3 Configure VPN Group Policies

To create VPN policies enter the **External CA** tab, lock the configuration dialogue and enter the required information into the tabs described in the following.

**Note:**

As the configurations of **Rules** and **Policies** are interdependent on settings configured in the other tabs **Common**, **Phion** and **IPSec**, the following configuration sections are described from right to left beginning with a description of tab **IPSec**.

### 2.6.2.4 IPSec Tab

This tab is used for defining (multiple) templates concerning Phase 2 of an IPsec connection. To create IPsec Phase 2 datasets, activate the tab, lock the configuration dialogue and select **New phase II ...** from the context menu.

**List 5-27** VPN configuration - Client to Site - External CA tab > IPSec tab - section Phase 1 (default) / Phase 2

Parameter	Description
<b>Encryption</b>	<p>Defines the kind of encryption used. Available algorithms for both phases <b>Phase 1</b> and <b>Phase 2</b> are: <b>AES</b>, <b>AES256</b>, <b>3DES</b> (default), <b>Blowfish</b>, <b>CAST</b>, and <b>DES</b>.</p>
<b>Hash Meth.</b>	<p>Defines the hash algorithm used. Available algorithms are <b>MD5</b> (default) and <b>SHA</b>.</p>
<b>DH-Group</b>	<p>The Diffie-Hellman Group defines the way of key exchange. The available options for this parameter are <b>Group1</b> (default; 768-bit modulus), <b>Group2</b> (1024-bit modulus), <b>Group5</b> (1536-bit modulus) and <b>none</b>.</p>

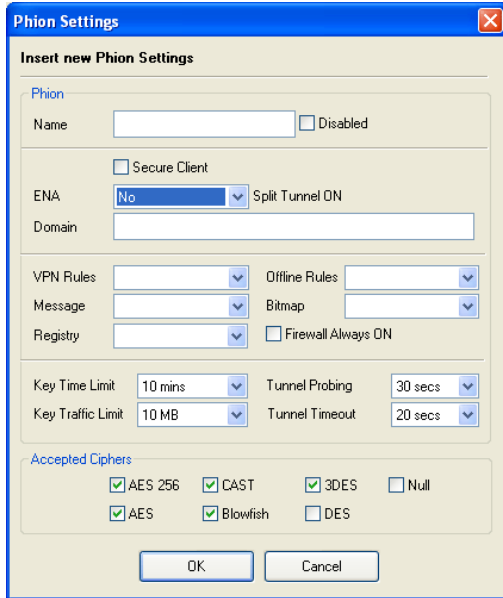
**List 5-28** VPN configuration - Client to Site - External CA tab > IPSec tab - section Lifetime

Parameter	Description
<b>Time</b>	<p>Rekeying time in seconds the server offers to the partner.</p>
<b>Minimum</b>	<p>Minimum rekeying time in seconds the server accepts from its partner.</p>
<b>Maximum</b>	<p>Maximum rekeying time in seconds the server accepts from its partner.</p>

### 2.6.2.5 phion Tab

To create phion connection datasets, activate the tab, lock the configuration dialogue and select **New phion ...** from the context menu.

Fig. 5-26 New phion client policy



List 5-29 VPN configuration - Client to Site - External CA tab > Phion tab - section Phion

Parameter	Description
<b>Name</b> field	Defines the name of the dataset. By ticking the checkbox <b>Disabled</b> , the settings are disabled.
<b>Secure Client</b> checkbox	Ticking this checkbox causes that only Secure Clients are access.
<b>ENA</b> (Exclusive Network Access)	Setting this parameter to <b>yes</b> causes that any other network access except for the tunnel is blocked for the client. If the client does not have ENA set within its configuration a connection is not granted.
<b>Domain</b> field	Name of the partner's domain.
<b>Message</b> pull-down menu	This menu contains the available welcome messages that are shown to the client as soon as the VPN tunnel is established (see 2.6.3 Messages Tab, page 219).
<b>VPN Rules</b> pull-down menu	This menu contains the available rule sets for the client's phion Personal Firewall. As long as the VPN tunnel is established, this rule set is active (see 2.6.6 VPN FW / Offline FW Tab, page 219).
<b>Offline Rules</b> pull-down menu	This menu contains the available offline rule sets for the clients phion Personal Firewall. As long as the VPN tunnel is not established, this rule set is active (see 2.6.6 VPN FW / Offline FW Tab, page 219).
<b>Bitmap</b> pull-down menu	This menu contains the available bitmaps that are shown to the client as soon as the VPN tunnel is established (see 2.6.4 Pictures Tab, page 219).
<b>Registry</b> pull-down menu	This menu provides the available registry checks for selection (see 2.6.1 Phion VPN CA Tab, Registry Tab, page 219). The checks are carried out when connecting.
<b>Firewall Always ON</b> checkbox	Ticking this checkbox disables the deactivation of the clients Personal Firewall.
<b>Key Time Limit</b>	This parameter defines the period of time after which the re-keying process is started. Possible settings are 5, 10 (default), 30 and 60 minutes.
<b>Key Traffic Limit</b>	This parameter defines the amount of traffic after which the re-keying process is started. Possible settings are: ⚡ <b>No Limit</b> ⚡ <b>50 MB</b> ⚡ <b>10 MB</b> (default) ⚡ <b>5 MB</b> ⚡ <b>1 MB</b>

List 5-29 VPN configuration - Client to Site - External CA tab > Phion tab - section Phion

Parameter	Description
<b>Tunnel Probing</b>	The probing parameter defines the interval of sent probes. If such a probe is not answered correctly, the parameter <b>Tunnel Timeout</b> (see below) is in charge. The available time settings (in seconds) for the probing parameter are: ⚡ <b>silent</b> (no probes are sent; disables the parameter) ⚡ <b>10 secs</b> ⚡ <b>20 secs</b> ⚡ <b>30 secs</b> (default) ⚡ <b>60 secs</b>
<b>Tunnel Timeout</b>	If for some reason the enveloping connection breaks down the tunnel has to be re-initialised. This is extremely important for setups with redundant possibilities to build the enveloping connection. The timeout parameter defines the period of time after which the tunnel is terminated. The available settings (in seconds) for the timeout parameter are: ⚡ <b>10 secs</b> ⚡ <b>20 secs</b> (default) ⚡ <b>30 secs</b> ⚡ <b>60 secs</b> <b>Note:</b> The choice of the ideal timeout parameter strongly depends on the availability and stability of the connection. phion recommends setting the timeout to <b>30 seconds for internet connections</b> and to <b>10 seconds for intranet connections</b> or connections over a dedicated line.

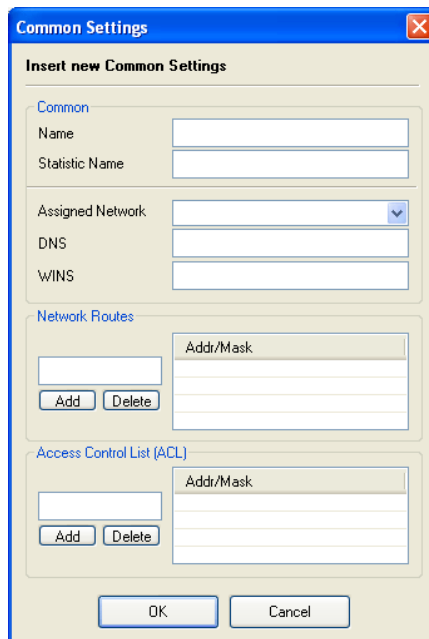
List 5-30 VPN configuration - Client to Site - External CA tab > Phion tab - section Accepted Ciphers

Parameter	Description
<b>Accepted Ciphers</b>	This section specifies the encryption algorithm(s) which are accepted from the client at connection time. If the client tries to establish a tunnel with a cipher not specified here, it will not be able to connect.

### 2.6.2.6 Common Tab

To create common datasets activate the tab, lock it and select **New common ...** from the context menu.

Fig. 5-27 New common - Common Settings



**List 5-31** VPN configuration - Client to Site - External CA tab > Common tab - section Common

Parameter	Description
<b>Name</b> field	Defines the name of the data set.
<b>Statistic Name</b> field	This field specifies the name that is displayed in statistics.
<b>Assigned Network</b> pull-down menu	Every already defined network (see 2.3.1 Personal Networks Tab, page 206) is available for selection.
<b>DNS</b> field	Enter the IP address of an optional DNS server into this field.
<b>WINS</b> field	Enter the IP address of an optional WINS server into this field.

**List 5-32** VPN configuration - Client to Site - External CA tab > Common tab - section Network Routes

Parameter	Description
	This section is used to define network routes. Enter an IP address and click <b>Add</b> to add the entry to the listing on the right side. <b>Note:</b> You may define up to 63 network routes.

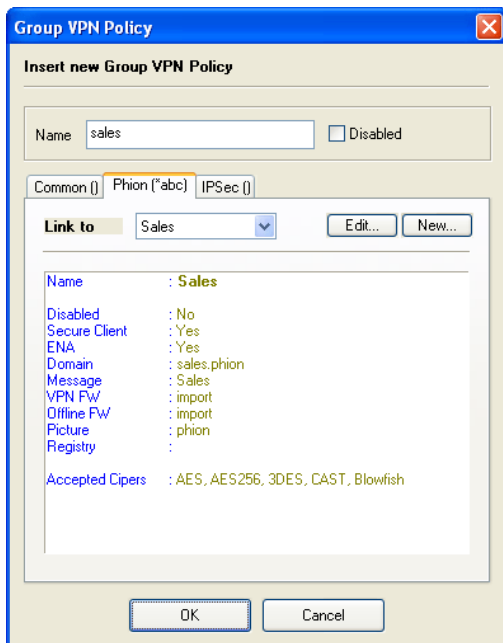
**List 5-33** VPN configuration - Client to Site - External CA tab > Common tab - section ACL

Parameter	Description
	This section is used to define the ACL (Access Control List). Enter an IP address and click <b>Add</b> to add the entry to the listing on the right side.

### 2.6.2.7 Policy Tab

To create VPN group policies activate this tab, lock it and select **New Policy ...** from the context menu.

**Fig. 5-28** Configuration dialogue - New policy



If settings at the tabs **Common**, **Phion**, and **IPSec** have not yet been configured and thus cannot be selected in the corresponding tabs described here, you may generate a new data set now with use of the button **New ...** Furthermore an existing data set may be changed by selecting it and clicking **Edit ...**

### 2.6.2.8 Configure VPN Group Rules

The VPN group rules specify the global settings for VPN personal tunnels using an external x.509 certificate and group configurations, such as what kind of certificate is to be used or the authentication scheme.

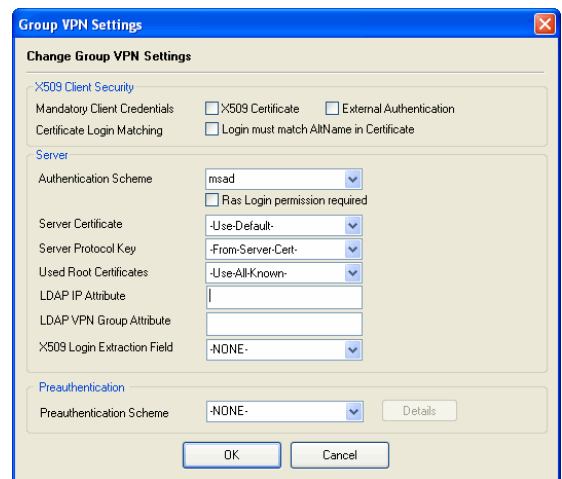
The configuration consists of two separate instances:

- general settings available via the link on top of the tab (or context menu entry **Group Match Settings ...**)
- group policy conditions via the context menu entry **New Rule ...**

**Note:**  
Take into consideration that up and down movement of available group policies is necessary due the sequential processing order. This movement is done by selecting an entry and using the context menu entries **Up** or **Down**.

### 2.6.2.9 Change Group VPN Settings

**Fig. 5-29** Change Group Match Settings



**List 5-34** VPN configuration - Client to Site - External CA tab > Rules tab > ... Group Match Settings ... - section X.509 Client Security

Parameter	Description
<b>Mandatory Client Credentials</b>	Specifies the used certificate: <b>X.509 Certificate</b> - enforces authentication via certificate <b>External Authentication</b> - enforces authentication via username and password Concurrent activation of both options forces both, certificate AND username and password authentication.
<b>Certificate Login Matching</b>	This parameter specifies whether the alternative name in the certificate has to match the user login for successful authentication. Therefore, the subjectAltName has to contain a value of type email and the user part of the e-mail has to match the login name (see 1.4.2 Authentication, External x.509 certificate with password request, page 201, and/or, if not selected, External x.509 certificate with user and password request, page 201).

**List 5-35** VPN configuration - Client to Site - External CA tab > Rules tab > ... Group Match Settings ... - section Server

Parameter	Description
<b>Authentication Scheme</b>	Here the corresponding authentication scheme has to be selected. The following values are available: ➤ <b>ldap</b> ➤ <b>msnt</b> ➤ <b>msad</b> ➤ <b>radius</b> ➤ <b>rsaace</b>

**List 5-35** VPN configuration - Client to Site - External CA tab > Rules tab > ... Group Match Settings ... - section Server

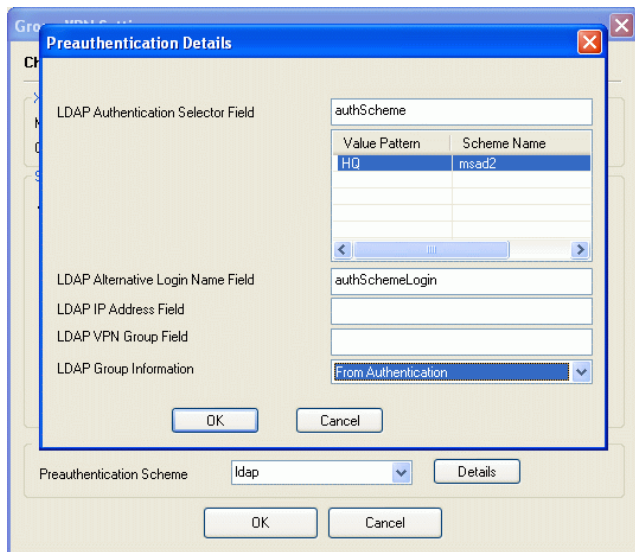
Parameter	Description
<b>Server Certificate</b>	This list contains all available server certificates (see 2.3.4 Server Certificates Tab, page 209). When selecting <b>-Use-Default-</b> the default server certificate is used (see 2.3.3 Root Certificates Tab, page 208).
<b>Server Protocol Key</b>	This menu defines the to be used key. The entry <b>-From-Server-Cert-</b> causes that the server certificate key is used. Alternatively, as long as configured, any key that was created in the <b>VPN Server Settings</b> (see 2.3.2 Server Key/Settings Tab, page 207) can be activated.
<b>Used Root Certificates</b>	The selected entry of this listing defines the root certificate that is used to verify this VPN partner. The entry <b>-Use-All-Known-</b> allows that all available root certificates can be used for verification of the partner. Alternatively, you can select an explicit root certificate.
<b>LDAP IP Attribute</b>	Here you define the name of the attribute that contains the IP address that is assigned to a VPN user. Only IP addresses from a personal network configured in the "VPN settings" are allowed.
<b>LDAP VPN Group Attribute</b>	Here you define the name of the attribute that contains the name of the group policy that is assigned to a VPN user. The assigned policy overrules other existing group policy rules. There will be no connection if this attribute contains a non existing value (policy name).
<b>X509 Login Extraction Field</b>	The VPN server requires a username of the VPN user for successful pre-authentication. If authentication takes place only through x.509 certificates, the VPN server has to extract the username out of the x.509 certificate. This field defines which attribute of the certificate contains the username. <ul style="list-style-type: none"> <li>➤ <b>CN (Common Name)</b></li> <li>➤ <b>altName (Alternative Name)</b></li> <li>➤ <b>emailAddress (EmailAddress)</b></li> </ul>

**List 5-36** VPN configuration - Client to Site - External CA tab > Rules tab > ... Group Match Settings ... - section Preauthentication

Parameter	Description
<b>Pre-authentication Scheme</b>	Here the pre-authentication scheme can be selected. The following values are available: <ul style="list-style-type: none"> <li>➤ <b>ldap</b></li> <li>➤ <b>msad</b></li> </ul>

**Preauthentication Details:**

**Fig. 5-30** Preauthentication Details



**List 5-37** VPN configuration - Client to Site - External CA tab > Rules tab > ... Group VPN Settings > Preauthentication Details

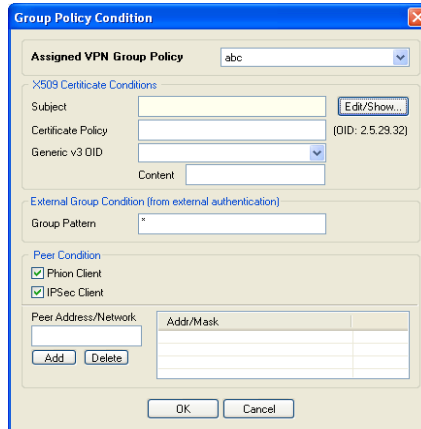
Parameter	Description
<b>LDAP Authentication Selector Field</b>	Name of the attribute in the LDAP compatible directory service/MSAD in which the name of the authentication scheme is enclosed. Therewith it is possible to assign to every user a different authentication scheme. The identifiers are the same as in "Authentication Service", for example MSAD. If there is an additional MSAD authentication scheme configured, the identifier are user-specific, for example MSAD-HQ, RADIUS ... With a right-click in the field beneath the values of the attribute can be transformed. For example for attribute "authScheme", enter the value pattern "HQ" and the scheme name "msad2". For the final authentication the authentication service "msad2" will then be used. <b>Note:</b> Using this field, the authentication scheme in the Group VPN Settings will be deactivated.
<b>LDAP Alternative Login Name Field</b>	If a user has to use a different login name for authentication at the authentication server it can be defined on the pre-authentication server. This field defines the attribute, that contains the alternative login name.
<b>LDAP Group Information</b>	Defines, whether the group information of the pre-authentication server or the one of the authentication server will be assigned to a VPN user.

**Group Policy Condition:**

This section displays all configured VPN group policies.

Right-click into the tab's main window and select **New Rule** from the context menu to create a new group policy or mark an existing policy and select **Show/Edit** to view or edit the settings.

**Fig. 5-31** Configuration dialogue - Group Policy Condition



**2.6.2.10 Security**

**List 5-38** VPN configuration - Client to Site - External CA tab > Rules tab > Group Policy Condition

Parameter	Description
<b>Assigned VPN Group Policy</b>	This list contains the available VPN group policies (see 2.6.2.3 Configure VPN Group Policies, page 215).

**List 5-39** VPN configuration - Client to Site - External CA tab > Rules tab > Group Policy Condition - section X509 Certificate Conditions

Parameter	Description
<b>Subject</b>	This field defines what kind of group information is taken into consideration (pattern matching). By clicking <b>Edit/Show</b> the dialogue <b>Certificate Condition</b> is opened (figure 5-32). If multiple, for example, OUs are required they have to be separated using / (for example, entering FOO*/COMPANY results in that all subjects with OU=FOO* and OU=COMPANY match). <b>Note:</b> For information concerning group information from MSAD or LDAP authentication scheme, have a look at <b>Appendix - 1.1</b> How to gather Group Information, page 524.
<b>Certificate Policy</b>	This field defines the required value of the <b>certificate policy</b> field (for example OID: 2.5.29.31).
<b>Generic OID</b>	This field defines a v3-extension field per OID number.
<b>Content</b>	Required content/value of the <b>Generic OID</b> field.

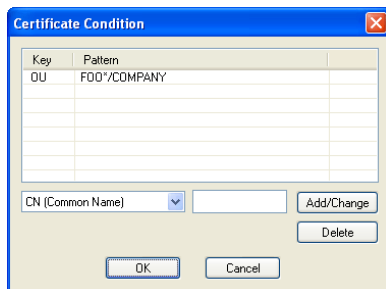
**List 5-40** VPN configuration - Client to Site - External CA tab > Rules tab > Group Policy Condition - section External Group Condition

Parameter	Description
<b>Group Pattern</b>	Defines the matching pattern (case in-sensitive) for groups from external authentication (for example OU=Department1*).

**List 5-41** VPN configuration - Client to Site - External CA tab > Rules tab > Group Policy Condition - section Peer Condition

Parameter	Description
<b>Phion Client / IPSec Client</b>	These two check boxes define the way, the VPN partners are allowed to establish the VPN tunnel.
<b>Peer Address / Network</b>	This field is used to specify the allowed peer IP by defining an ACL with networks (address/mask). By clicking <b>Add</b> the value is entered into the list to the left of the field. Selecting an entry in the list and clicking <b>Delete</b> this entry can be removed.

**Fig. 5-32** Certificate Conditions configuration



## 2.6.3 Messages Tab

In the **Messages** tab, customised welcome messages may be defined for later assignment to specific licenses. Assigned messages are displayed in the VPN client requesting connection to a VPN server after successful connection establishment.

## 2.6.4 Pictures Tab

In the **Pictures** tab, customised pictures (for example the company logo) may be defined for later assignment to specific licenses. Assigned pictures are displayed in the

VPN client requesting connection to a VPN server after successful connection establishment.

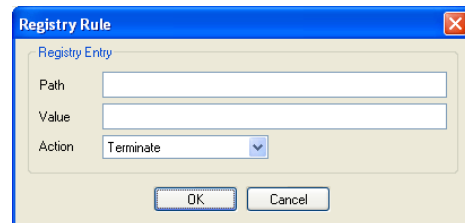
Note that only **Bitmap** files (.bmp) with a maximum of 256 colours and a maximum size of 150x80 pixels may be imported.

## 2.6.5 Registry Tab

Use this configuration dialogue to define registry checks to be performed on the client's system on connection. Specify the next to take action depending on the situation encountered. For example, the connection attempt can be terminated or a warning can be generated if the automatic virus scanner update on the client is deactivated.

Simply choose **New Registry Rule set ...** from the context menu and enter a name for the rule set. Right-click into the just opened configuration window and choose **New ...** from the context menu to open the configuration dialogue as displayed in figure 5-33.

**Fig. 5-33** Configuration dialogue for registry rules



### 2.6.5.1 Security

**List 5-42** VPN configuration - Client to Site - Registry tab > New Registry Rule Set ... - section Registry Entry

Parameter	Description
<b>Path</b>	Enter the path to the registry entry that is to be checked.
<b>Value</b>	Enter the value for the required readout.
<b>Action</b>	Specify the next to take action on value mismatch. Possible actions are termination of the connection (default) or generation of a warning message.

## 2.6.6 VPN FW / Offline FW Tab

These tabs allow specification of two kinds of rule sets for the entegra VPN client's Personal Firewall:

### ➤ Personal VPN Firewall

This rule set is used when being connected via VPN. During connection establishment, the server-held VPN Firewall rule set is sent to the client.

### ➤ Personal Offline Firewall

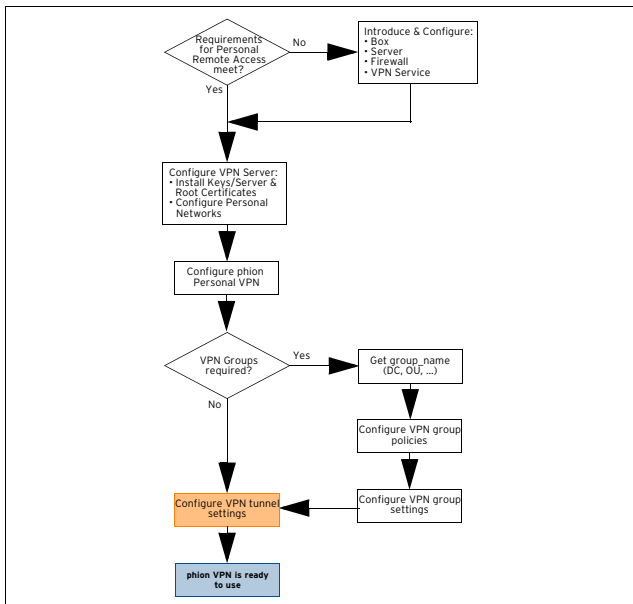
This rule is used when there is no connection via VPN. The offline rule set replaces the customised rule set of the client's Personal firewall and thus assures that the company policy for Internet access is guaranteed.

Due to the complexity of this configuration tree entry, have a look at Configuring the Personal Firewall, page 241.



## 2.7 Configuring VPN Tunnel Settings

Fig. 5-34 VPN configuration block diagram - Configure VPN tunnel



Besides the routing relevant information each tunnel has some general settings. These include the way the tunnel is built up and is kept active.

### Note:

You may define up to 2048 VPN tunnels (sum of Client-to-Site and Site-to-Site tunnels).

To access the configuration dialogues, double-click **Site to Site** (accessible through **Config > Virtual Servers > Assigned Services > <servicename> (vpnserver)**).

The main task in building a **Virtual Private Network** is the creation of IP tunnelling. The basics of IP tunnelling are rather simple.

### Note:

However, the details can be difficult to set up because of overlapping IP address ranges and redundancy needs.

The goal is to get a transparent connection from a host within a local network to another host within a partner network.

Table 5-4 Involved objects within a phion VPN framework

Object	Description
Local Network	The source IP addresses that should use the tunnel to reach the partner network.

Table 5-4 Involved objects within a phion VPN framework

Object	Description
IP Address used for tunnel	IP address that is used by the system to build up the tunnel enveloping connection to the VPN server 2.
Peer IP	IP address of VPN server 2 used to build up the tunnel enveloping connection.
Partner Network	The destination addresses that should be reached via the tunnel by the local networks.

### Note:

phion provides a tool called `vpnadminclt (/opt/phion/bin/)` for direct access on the VPN server for user "root".

Usage of this tool:

```
/opt/phion/bin/vpnadminclt <server>_<service> <protocol command>
```

### Available commands:

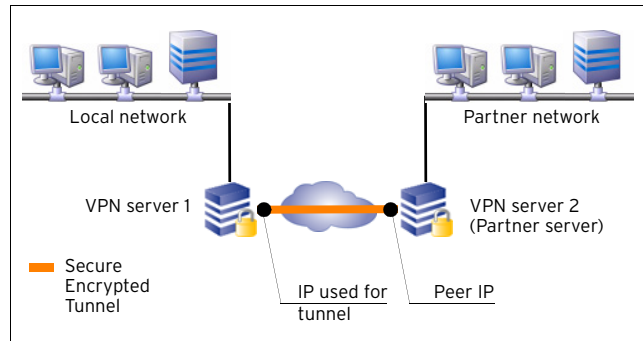
`kill <name>` (example: `kill FW2FW-2hq1`) - terminates a phion Site-To-Site tunnel

`ipsechardkill <name>` - terminates IPsec site-to-site tunnels

`init <name>` (example: `init FW2FW-2hq1`) - establishes a tunnel

`disable <num> <name>` (example: `disable 0 FW2FW-hq1`) - disables (num=0), enables a tunnel permanently (num=-1) or enables a tunnel with x-seconds time limit (num > 0)

Fig. 5-35 Scheme with the basic notations of VPN tunnelling



### 2.7.1 Configuring TINA Tunnels (Firewall-to-Firewall Tunnels)

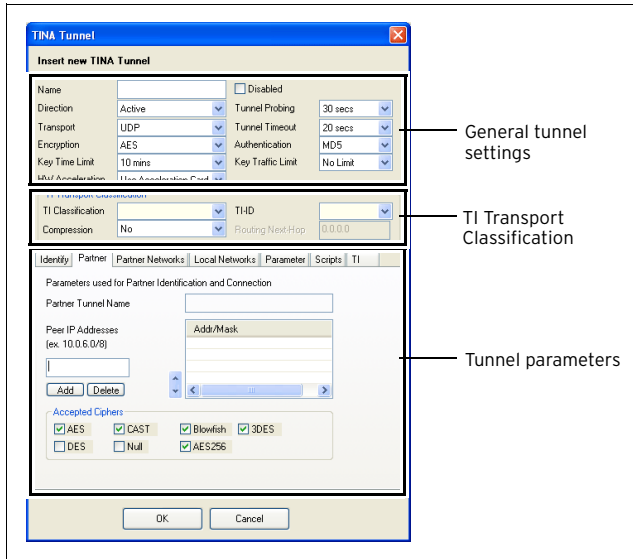
**Step 1** Enter config tree entry **Site to Site > TINA Tunnels** tab and lock the configuration dialogue

**Step 2** Create a new tunnel object

Access the tunnel configuration dialogue via the context menu entry **New TINA tunnel ...**

### Step 3 Set the general tunnel settings

Fig. 5-36 Tunnel configuration



#### 2.7.1.1 Security

List 5-43 VPN configuration - Site to Site - TINA Tunnels tab &gt; New TINA tunnel ... - section General tunnel settings

Parameter	Description
<b>Name</b>	This is the tunnel name needed for informational and partner identification purpose. <b>Note:</b> The maximum length of this parameter is 64 characters.
<b>Disabled checkbox</b>	Select this checkbox to disable the tunnel manually.
<b>Direction</b>	Operational mode of the tunnel. Each tunnel can be operated in the following modes: <ul style="list-style-type: none"> <li>➤ <b>Active</b> An active VPN server accepts tunnel requests as well as tries to initiate the tunnel connection. When the tunnel is down for a defined time (see Tunnel Timeout, page 222) it will clean its state to accept retries from its partner as well as try to initiate the connection.</li> <li>➤ <b>Passive</b> A passive VPN server does not build up the tunnel, it merely accepts requests from its partner. If the tunnel is down for a defined time (see Tunnel Timeout, page 222) it will clean its state to accept retries from its partner. <b>Note:</b> Do not try to establish a tunnel between two passive VPN servers as both would wait for the other to initiate the tunnel.</li> <li>➤ <b>OnDemand</b> This direction type is only of interest in combination with Traffic Intelligence configuration (see 2.7.1.2 Traffic Intelligence (TI), page 223). A VPN Server set to direction mode <b>OnDemand</b> actively builds up a connection and terminates it again, when a connection times out. The connection timeout is configured through parameter <b>On Demand Transport Timeout</b> (page 226). <b>Note:</b> It is possible to set both VPN servers to <b>OnDemand</b> in the GTI editor (<b>phion management centre</b> - 15.2.2.4 Defining Tunnel Properties, page 469).</li> </ul>

List 5-43 VPN configuration - Site to Site - TINA Tunnels tab &gt; New TINA tunnel ... - section General tunnel settings

Parameter	Description
<b>Transport</b>	Transport mode of the tunnel; only accessible if <b>Direction</b> is set to <b>active</b> . Four options are available: <ul style="list-style-type: none"> <li>➤ <b>UDP</b> Tunnel uses UDP port 691 to communicate. This connection type is suited best for response optimised tunnels.</li> <li>➤ <b>TCP</b> Tunnel uses TCP connection on port 691 or 443 (for HTTP proxies). This mode is required for connection over SOCKS4 or HTTP proxies.</li> <li>➤ <b>UDP&amp;TCP</b> Tunnel uses TCP AND UDP connections. The tunnel engine uses the TCP connection for UDP requests and the UDP connection for TCP requests and ICMP-based applications.</li> <li>➤ <b>ESP</b> Tunnel uses ESP (IP protocol 50) to communicate. This connection type is best suited for performance optimised tunnels.</li> </ul> <b>Note:</b> Do NOT use ESP if there are filtering or NAT interfaces in between. <ul style="list-style-type: none"> <li>➤ <b>Routing</b> <b>Attention:</b> Unencrypted data.  This transport type is only of interest in combination with Traffic Intelligence configuration (see 2.7.1.2 Traffic Intelligence (TI), page 223). Specifying routing as transport disables data payload encryption within the tunnel. This transport should only be used for uncritical bulk traffic. Transport type Routing activates parameter <b>Routing Next-Hop</b> in the VPN configuration - Site to Site - TINA Tunnels tab &gt; New TINA Tunnel ... - section TI Transport Classification List 5-44 (page 224), where the next-hop address for routed data packets has to be specified.</li> </ul>
<b>Encryption</b>	Encryption mode the tunnel wants to establish as the active part. phion tunnels work with various encryption algorithms. The initialising partner tries to establish the encrypted connection by offering ONE of the following methods. <ul style="list-style-type: none"> <li>➤ <b>AES</b> Advanced Encryption Standard; default; capable of 128/256 bit key length</li> <li>➤ <b>3DES</b> Further developed DES encryption; three keys with each 56 bit length are used one after the other resulting in a key length of 168 bit.</li> <li>➤ <b>CAST</b> by Carlisle Adams and Stafford Tavares; algorithm similar to DES with a key length of 128 bit.</li> <li>➤ <b>Blowfish</b> works with a variable key length (up to 128 bit)</li> <li>➤ <b>DES</b> Digital Encryption Standard; since DES is only capable of a 56 bit key length, it cannot be considered as safe any longer. <b>Attention:</b> Do NOT use DES with high risk data.</li> </ul>
<b>Key Time Limit</b>	This parameter defines the period of time after which the re-keying process is started. Possible settings are <b>5</b> , <b>10</b> (default), <b>30</b> and <b>60</b> minutes.
<b>HW Acceleration</b>	The <b>HW Acceleration</b> parameter allows selection of the preferred encryption engine - that is the CPU or a hardware accelerator - if present. This allows for load balancing between CPU and an optional crypto card with more than one tunnel in use. <ul style="list-style-type: none"> <li>➤ <b>Use Acceleration Card (if present)</b> (default) Select this option, if you have installed and intend to use a crypto accelerator hardware board. Note that for this to function the corresponding module supporting the card has to be loaded in the local firewall settings (see <b>VPN HW Modules</b>, page 128).</li> <li>➤ <b>Use CPU</b> Select this option to use CPU acceleration.</li> </ul>

**List 5-43** VPN configuration - Site to Site - TINA Tunnels tab > New TINA tunnel ... - section General tunnel settings

Parameter	Description
<b>Tunnel Probing</b>	The probing parameter defines the interval of sent probes. If such a probe is not answered correctly, the parameter <b>Tunnel Timeout</b> (see below) is in charge. The available time settings (in seconds) for the probing parameter are: <ul style="list-style-type: none"> <li>- <b>silent</b> (no probes are sent; disables the parameter)</li> <li>- <b>10 secs</b></li> <li>- <b>20 secs</b></li> <li>- <b>30 secs</b> (default)</li> <li>- <b>60 secs</b></li> </ul>
<b>Tunnel Timeout</b>	If for some reason the enveloping connection breaks down the tunnel has to be re-initialised. This is extremely important for setups with redundant possibilities to build the enveloping connection. The timeout parameter defines the period of time after which the tunnel is terminated. The available settings (in seconds) for the timeout parameter are: <ul style="list-style-type: none"> <li>- <b>10 secs</b></li> <li>- <b>20 secs</b> (default)</li> <li>- <b>30 secs</b></li> <li>- <b>60 secs</b></li> </ul> <p><b>Note:</b> The choice of the ideal timeout parameter strongly depends on the availability and stability of the connection. phion recommends setting the timeout to <b>30 seconds for internet connections</b> and to <b>10 seconds for intranet connections</b> or connections over a dedicated line.</p>
<b>Authentication</b>	Defines the used algorithm for authentication. Available methods are <ul style="list-style-type: none"> <li>➤ <b>MD5</b> Message Digest 5. Hash length: 128 bit.</li> <li>➤ <b>SHA</b> Secure Hash Algorithm. Hash length: 160 bit.</li> <li>➤ <b>NOHASH</b> Have a look at 1.4.6 Excursion: Description of VPN NoHash Security Issues, page 203.</li> <li>➤ <b>RIPemd160</b> RACE Integrity Primitives Evaluation Message Digest. Hash length: 160 bit.</li> <li>➤ <b>SHA256</b> Secure Hash Algorithm. Hash length: 256 bit.</li> <li>➤ <b>SHA512</b> Secure Hash Algorithm. Hash length: 512 bit.</li> </ul>
<b>Key Traffic Limit</b>	This parameter defines the amount of traffic after which the re-keying process is started. Possible settings are: <ul style="list-style-type: none"> <li><b>No Limit</b></li> <li><b>50 MB</b></li> <li><b>10 MB</b> (default)</li> <li><b>5 MB</b></li> <li><b>1 MB</b></li> </ul>

#### Step 4 Set the tunnel parameters

The tunnel parameters section is split into the following tabs:

- **Identify** tab  
This tab defines the identification type (**Public Key, X509 Certificate (CA signed)** or **X509 Certificate (explicit), Box SCEP Certificate (CA signed)**).
- **Partner** tab  
Depending on whether the tunnel direction is passive or active, the partner server can be a whole subnet (passive mode) or it has to be defined by single IPs (active and bi-directional mode). The case of more IPs for redundant tunnel enveloping connections is described in 5.4 Redundant VPN Tunnels, page 239.  
  
Import the public key of the tunnel partner via clipboard or file. Principally, the public key is not needed. However, it is strongly recommended, that you use strong authentication to build up the tunnel enveloping connection.  
  
If you have two different tunnel connections configured

between the same two peers, the keys are mandatory.

The **Accepted Ciphers** section is used for defining the accepted encryption methods.


- **Partner Networks** tab  
The VPN tunnel makes partner networks accessible through the assigned VPN interfaces.  
  
Insert the address(es) of the partner network(s) into the **Addr/Mask** list.

The tunnel is fed through **vpn0** by default. You may use another VPN interface by adjusting the **VPN Device Index**.

**Note:**

You have to create indexed VPN interfaces first if you want to use this option (2.3.2 Server Key/Settings Tab, **Device Index**, page 207).

Select the **Advertise Route** checkbox to propagate routes to the partner networks with OSPF/RIP.

- **Local Networks** tab  
The local networks that should be able to reach the partner networks. It can be a list of networks or single IP addresses. Since this settings is typically shared by several tunnels it can be defined in menu item  **Local Networks** and referenced in the single tunnel configurations.
- **Parameter** tab  
Use this tab to define the connection type.
- **Tunnel Parameter Template**  
can be used to activate templates (predefined in the Parameter templates tab) or to define values explicitly. With scheme **-explicit-** the fields below are available.
- **IP Address or Device used for Tunnel Address**  
Option **First Server IP** serves to inherit the first server IP by the server settings.

Option **Second Server IP** serves to inherit the second server IP by the server settings.

Option **Dynamic (via routing)** causes that the IP will be chosen by the routing table.

Option **Explicit (ordered list)** causes that the explicit IPs or device names (to be entered below) will be used in the given order. This is important for redundancy on the active side of the tunnel.

- **Proxy Type**  
Option **Direct (no Proxy)** indicates the standard connection.  
  
Option **HTTP Proxy** causes the use of a HTTP proxy server with optional user/password authentication  
  
Options **Socks 4 Proxy / Socks 5 Proxy** cause the use of a Socks 4/5 server.

- **Scripts** tab  
This tab offers two separate sections called Start Script and Stop Script. It allows defining certain processes that are started when connecting via VPN and/or stopped when disconnecting.

- **TI** tab  
Options in this tab are only of interest in combination with Traffic Intelligence configuration (2.7.1.2 Traffic Intelligence (TI)). See the **TI** tab description below (page 226).

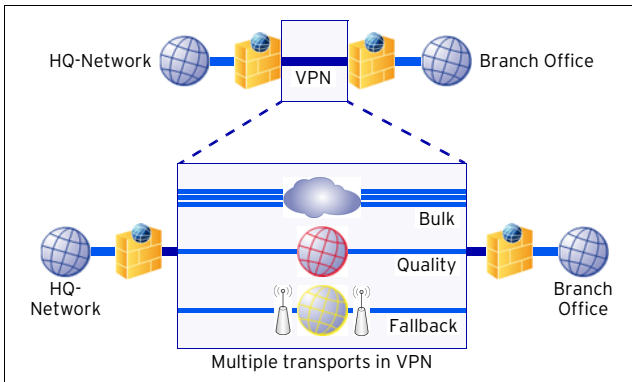
### 2.7.1.2 Traffic Intelligence (TI)

The aim of VPN traffic intelligence employment is a multi-transport construct within a VPN tunnel allowing for reliable and failsafe network connectivity. Multi transport TI implementation in phion netfence gateway accommodates the following needs:

- Transports can be identified and classified. Transport classes are broken down into **Quality**, **Bulk** and **Fallback** traffic.
- Multiple transport methods (TCP, UDP, ESP, IP addresses, Cipher, Hash, Compression, ...) may be used in one tunnel at the same time.
- Transports can either be used simultaneously or on demand.
- Transport selection policies can be defined to steer network traffic.
- Standard routing may be used for uncritical traffic.

Using different lines for different transport classes, for example provider lines for bulk transport (top), a frame relay for quality transport (middle), and UMTS (bottom) for fallback transport:

**Fig. 5-37** Traffic Intelligence (TI)

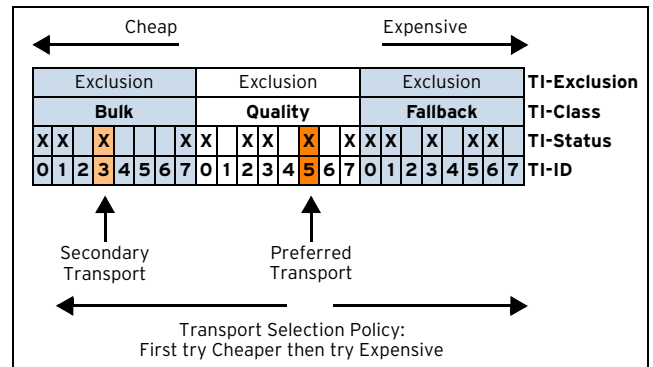


TI employment relies upon the following mechanisms to achieve consistent transport selection policies:

- Transport quality is defined through firewall connection objects (see Step 6 Configure Connection Objects for use with Traffic Intelligence, page 224). Firewall rules referencing to these connection objects have to be created in order to activate TI settings.
- Connection objects define primary and secondary transport class, and they determine general policy behaviour if the preferred transports fail.
- Connection objects allow protecting from "expensive" transports by explicitly excluding their usage.
- Connection objects may be handled in the context of a master-slave concept by the tunnel endpoints. The connection object can be configured to advertise its settings (see parameter TI Learning Policy, page 225).

Have a look at figure 5-38 to understand the mechanism of transport selection policy:

**Fig. 5-38** Transport Selection Policy



Multiple transport classes have been created for a TINA tunnel. As shown in figure 5-38 the following transports are available: Quality transport (TI-IDs 0, 2, 3, 5, 7), Bulk transport (TI-IDs 0, 1, 3, 7), Fallback transport (TI-IDs 0, 1, 3, 5, 6).

A connection object has been configured to use **Quality** transport with TI-ID **5** (Q5) as preferred transport and **Bulk** transport with TI-ID **3** (B3) as secondary transport. If both transport mechanisms fail, first the cheaper, then the more expensive transport shall be tried.

This policy will have the following effect, when the connection object is referenced by a firewall rule:

- Q5 will be tried first.
- If the line is not available B3 will be tried next.
- If this line as well is not available the next transport class with a smaller TI-ID than the preferred transport will be tried. In this this means Q3. The succession to the "cheaper" end would now proceed to Q2, Q0, B7, B3, B1, and B0.
- If none of these lines are available, tries will proceed to the more "expensive direction", which means that again the next higher class to the preferred transport, Q7, will be tried. The succession would then reach further from F0, F1, F3, ...


**Note:**  
Transport classification is a prerequisite to traffic classification. See below for a detailed description of available configuration values.

#### Step 5 Configure Transport Classification

A new transport mode is initially added to a tunnel through selecting the tunnel in the TINA Tunnels tab and choosing **Add Transport ...** from the context menu. This action opens the TINA Tunnel configuration window with the Partner tab (see above) pre-selected.

First of all, values in list 5-44 have to be defined:

List 5-44 VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... - section TI Transport Classification

Parameter	Description
<b>TI Classification</b>	<p>This setting classifies the transport rating into</p> <ul style="list-style-type: none"> <li>➤ <b>Bulk</b></li> <li>➤ <b>Quality</b> and</li> <li>➤ <b>Fallback</b></li> </ul> <p>traffic. Each transport inherits the Identification type from its "parent". Thus keys and certificates may be shared among multiple transports. Transports may be equipped with unique keys/certificates, though.</p>
<b>TI-ID</b>	<p>A Traffic Intelligence ID must be assigned to each added transport class in order to determine the transport selection policy succession. The values <b>0-7</b> are available, whereas lower numbers mean lower cost. The primarily created tunnel, which is the first tunnel transport, is automatically regarded as <b>Bulk</b> transport with <b>TI-ID 0</b>. Each transport classification/ID combination is unique in order to guarantee a consistent routing rule set. See figure 5-38 for a description of transport quality handling.</p>
<b>Compression</b>	<p>Compression support may be provided by the VPN engine for VPN client connections using entegra VPN client R8. Generally, compression can be requested by the user. The server may or may not accept to serve the request depending on both its configuration and the license type assigned to the VPN client. Client compression is only available to those clients that have assigned a secure connector license. The following settings are available:</p> <ul style="list-style-type: none"> <li>➤ <b>No</b> (default) Denies VPN client compression requests.</li> <li>➤ <b>Packet Compression (Low Latency)</b> This setting may be used for compression of all transport types.</li> <li>➤ <b>Stream Compression (Large Latency)</b> This setting may only be used for compression of TCP based data streams. The attainable compression rate will be higher than can be achieved with packet compression.</li> </ul> <p><b>Note:</b> The gateway hosting the VPN server must have a valid BOB license to use this feature. Refer to the Product Guide for license details. If your system is licensed for compression usage, can be viewed in the <b>License Values</b> field in the  <b>Control &gt; Licenses</b> tab (<b>Control Centre</b> - 2.5 Licenses Tab, page 37).</p> <p><b>Note:</b> To activate compression operability, the VPN service has to be restarted after BOB license installation.</p>
<b>Routing Next-Hop</b>	<p>This parameter is only available with <b>Transport type Routing</b> selected (page 221). The direction must be set to "Active" to be able to modify the Transport type. After the Transport type is set to "Routing" you may change the direction to "Passive" again. Enter the next-hop address for forwarding of unencrypted data payload. Note that a next-hop IP address must be configured for both active and passive VPN partner.</p>


**Note:**

For each transport general tunnel settings and tunnel parameters may as well be specified individually.

Confirming the settings made by clicking the **OK** button at the bottom of the configuration window inserts a new data set into the TINA Tunnel tab.

Fig. 5-39 TINA Tunnel with multiple transport modes added

Name	Enabled	Direction	Partner	Partner Networks	Transport	Encryption	Auth.	Partner ID
tunnelt	Yes	Active	10.0.1.0/8	10.0.2.0/8 OSPF+NO	UDP	AES	MD5	Public Key
tunnelt-1	Yes (B1)	Active	10.0.1.0/8		UDP	AES	MD5	Public Key
tunnelt-18	Yes(F2)	Active	10.0.1.0/8		UDP	AES	MD5	Public Key
tunnelt-23	Yes(F7)	OnDemand (0.60)	10.0.1.0/8		UDP	AES	MD5	Public Key
tunnelt-8	Yes(Q0)	Active	10.0.1.0/8		TCP	AES	MD5	Public Key

TI transport modes of a TINA tunnel are flagged with the following icon  in the listing. Additionally, the specified transport mode and TI-ID are displayed in the **Enabled**

column whereas B stands for **Bulk**, Q for **Quality** and F for **Fallback** transport.

**Note:**

Modifying the TI Classification setting retroactively is not possible.

Before proceeding to traffic classification in the TINA tunnel transport classes themselves, let us have a look at connection objects configuration.

**Step 6 Configure Connection Objects for use with Traffic Intelligence**

For transport and traffic classifications to become effective connection objects defining utilisation of transport and traffic mechanisms have to be inserted into rule sets. Connection objects are described in detail in **Firewall** - 2.2.6 Connection Elements, page 145. Values of interest for TI are the **VPN Traffic Intelligence (TI) Settings** described below. Click Edit/Show ... to open the **TI Settings** window:

List 5-45 Firewall Connection Object - VPN Traffic Intelligence (TI) - section TI Transport Selection

Parameter	Description
<b>Preferred Transport Class/ID</b>	<p>These parameters define the first transport class and ID to use when the connection object is processed in a rule set. Available transport classes are</p> <ul style="list-style-type: none"> <li>➤ <b>Bulk</b></li> <li>➤ <b>Quality</b> and</li> <li>➤ <b>Fallback (On Demand)</b></li> </ul> <p>whereas each transport class can have a transport ID ranging from <b>0-7</b>.</p>
<b>Second Try Transport Class/ID</b>	<p>These parameters define the second transport class and ID to use when the connection object is processed in a rule set if the first transport fails. Again, available transport classes are</p> <ul style="list-style-type: none"> <li>➤ <b>Bulk</b></li> <li>➤ <b>Quality</b> and</li> <li>➤ <b>Fallback (On Demand)</b></li> </ul> <p>each with transport ID from <b>0-7</b> possible. If no further transport try is desired</p> <ul style="list-style-type: none"> <li>➤ <b>None (Not Used)</b></li> </ul> <p>can be chosen as configuration value. If only one transport is in use (BO) leave settings at the default values.</p>
<b>Further Tries Transport Selection Policy</b>	<p>This section defines further transport tries if first and second transport classes fail. Configurable values are:</p> <ul style="list-style-type: none"> <li>➤ <b>First try Cheaper then try Expensive</b></li> <li>➤ <b>Only try Cheaper</b></li> <li>➤ <b>First try Expensive then try Cheaper</b></li> <li>➤ <b>Only try Expensive</b></li> <li>➤ <b>Stay on Transport (No further tries)</b></li> </ul> <p>Configuring this section is important because it allows exact specification when to abort transport. Correctly configured, it protects you from processing less important traffic over expensive lines (figure 5-38, page 223 for better understanding).</p>
<b>Balance Preferred and Second</b>	<p>Select <b>Yes</b> or <b>No</b>.</p> <p><b>Note:</b> Session based load balancing does not balance packets from one single connection but instead dispatches multiple connections to one of the defined transports.</p>



**List 5-45** Firewall Connection Object - VPN Traffic Intelligence (TI) - section TI Transport Selection

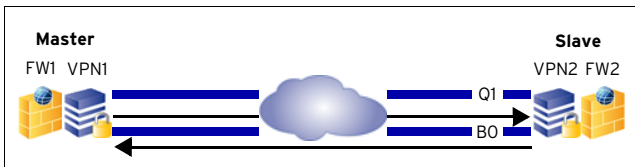
Parameter	Description
<b>TI Learning Policy</b>	<p>This parameter setting determines general VPN tunnel endpoint firewall behaviour this connection object is utilised in. Generally, it makes sense configuring connection objects on both firewalls synchronously. TI Learning Policy Settings apply per connection session. The following configuration options exist:</p> <ul style="list-style-type: none"> <li>➤ <b>Slave (learn TI settings from partner)</b> With this setting, the connection object adapts settings from the partner connection object when answering a request.</li> <li>➤ <b>Master (propagate TI settings to partner)</b> With this setting the connection object propagates TI settings to the partner, thus forcing it to override its own configuration when answering a request.</li> </ul> <p><b>Note:</b> Make settings with deliberation. Both partner objects set to Master might lead to unwanted transport effects, both set to Slave will miss information trim. Have a look at the process workflow in the <b>Example for TI Learning Policy</b> below.</p>
<b>Allow Bulk/Quality/Fallback Transports</b>	<p>Ticking these checkboxes generally enables/disables transport classes for this connection object. By excluding expensive transports, this feature offers protection from unwanted transport utilisation.</p>

**List 5-46** Firewall Connection Object - VPN Traffic Intelligence (TI) - section TI Traffic Prioritisation

Parameter	Description
	Only relevant if VPN transport is bandwidth protected.
<b>When using BULK transports/When using QUALITY transports</b>	<p>These parameter settings steer traffic priority assignment.</p> <p><b>Note:</b> For this to work Bandwidth Protection settings have to be configured in the TI tab (see Step 7 below) of the corresponding transport.</p>

**Example for TI Learning Policy:**

**Fig. 5-40** TI Learning Policy scheme



**Table 5-5** Example for TI Learning Policy

	Connection Object1	Connection Object1
<b>Preferred Transport Class/ID</b>	B0	Q1
<b>Secondary Transport Class/ID</b>	Q1	B0
<b>TI Learning Policy</b>	Master	Slave

In the setup displayed in figure 5-40 firewall rules have been introduced allowing traffic from VPN1 to VPN2 and vice versa. Connection objects on both tunnel endpoints were initially configured identically, but now the Master connection object on FW1 has changed and been configured with B0 as preferred transport class/ID, and Q1 as secondary transport class/ID. Traffic processing is now attempted from Master to Slave. The Master propagates its settings to the slave. The slave adapts the information and answers the connection request on B0, though this is not its own preferred transport.

**Note:**

The TI Settings window can be accessed from the Status tab in the Firewall Operative GUI (**Firewall - 6.2.2 Status List**, page 170) through right-clicking an active transport session and selecting **Change TI Settings** from the context menu. Changes apply for the active session only.

**Step 7** **Configure Traffic Classification**

In addition to classification of transports, traffic may be categorised to enable individual handling for specific purposes.

To configure traffic classification settings for a transport, open the corresponding data set in the TINA Tunnel window and select the **TI** tab in the tunnel parameters section.

Differentiated traffic classification options are available in the following:

**Bandwidth Protection**

**List 5-47** VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... > TI tab - section Bandwidth Protection

Parameter	Description
	<p><b>Note:</b> Bandwidth protection within a transport relies upon a connection object being classified as low or high priority traffic. Configure this in the connection object itself (list 5-46, page 225).</p>
<b>Bandwidth Policy</b>	<p>These settings specify how much of the available bandwidth traffic may "grab" within a transport. The following settings are available:</p> <ul style="list-style-type: none"> <li>➤ <b>Best Effort (No Protection)</b> In this mode, all traffic is processed through the transport with equal rights. An object's classification into low or high priority traffic is ignored. Full transport capacity might lead to bad response times and data loss.</li> <li>➤ <b>Dynamic Bandwidth (TCP Transport only)</b> This setting is only available with parameter transport set to <b>TCP</b>, as this is the only transport mode allowing for dynamical bandwidth assignment.</li> </ul> <p><b>Note:</b> When using TCP this is the recommended policy.</p> <p>Nonetheless, limits for <b>Low Priority</b> traffic have to be specified, as it is otherwise going to be discarded completely when it cannot allocate any bandwidth at traffic peak times. Default values are 60 % for the <b>Upper Limit</b> and 20 % for the <b>Lower Limit</b>. See below for a description how limits are calculated.</p> <p><b>Attention:</b> Under-running the lower limit of 20 % will cause low priority traffic discarding.</p> <ul style="list-style-type: none"> <li>➤ <b>Fixed Bandwidth</b> A fixed bandwidth has to be specified for all non TCP transports, as for these bandwidth cannot be calculated dynamically. A disadvantage of this method is, that already the initial bandwidth is subject to a limitation. A rule of thumb is required to set the value correctly. The fixed bandwidth (in kbit/s) has to be defined through the <b>Estimated Bandwidth</b> parameter. Again, values for <b>Low Priority Upper</b> and <b>Lower Limit</b> have to be specified. See below for a description how limits are calculated.</li> </ul> <p><b>Attention:</b> Under-running the lower limit of 20 % will cause low priority traffic discarding.</p>

**Calculation of Low Priority Traffic Upper and Lower Limits**

The Dynamic Bandwidth method assumes a maximum available bandwidth of 100 %; the Fixed Bandwidth method operates with a statical maximum available bandwidth according to the value specified through the Estimated Bandwidth parameter.

In the default setting, 60 % of the maximum bandwidth is assigned as Low Priority Upper Limit and 20 % as Low Priority Lower Limit. This means:

- Low priority traffic may utilise up to 60 % of the bandwidth as long as high priority traffic does not claim any bandwidth.

- The Low Priority Lower Limit of 20 % applies as soon as the sum of high and low priority traffic rises above the Low Priority Upper Limit of 60 %. Low priority traffic will not be processed any further, if it already consumes 20 % of the bandwidth. It will be discarded, even if bandwidth in fact is still available. The available bandwidth theoretically can be consumed by 80 % high and 20 % low priority traffic. When high priority traffic requires capacity beyond this point it displaces low priority traffic because high priority traffic is always privileged. Thus, in the worst case it might happen that at times low priority traffic is discarded completely.

**Note:**


The Low Priority Lower Limit setting does not imply a guaranteed bandwidth reservation. It can be rather looked upon as a measure to prevent immediate low priority traffic discarding at peak traffic times.

**VPN Envelope Policy**

**List 5-48** VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... > TI tab - section VPN Envelope Policy

Parameter	Description
<b>TOS Policy</b>	<p>This policy setting specifies how to deal with the <b>Type of Service (ToS)</b> information in a packet's IP header. In networks the ToS may be utilised to define the handling of the datagram during transport. If the ToS is enveloped, this information is lost. The following settings are available:</p> <ul style="list-style-type: none"> <li>➤ <b>Copy TOS From Payload to Envelope</b></li> </ul> <p><b>Note:</b> This setting can only be used with non TCP transports.</p> <p>In this mode the packet's original ToS information is copied to the envelope and thus remains available for utilisation.</p> <ul style="list-style-type: none"> <li>➤ <b>Fixed Envelope TOS</b></li> </ul> <p>In this mode the ToS information is masked by enveloping it without consideration. This setting activates parameter <b>Envelope TOS Value</b> (default: <b>0</b>) where a fixed ToS value has to be specified. All packets will thus be assigned the same ToS information.</p>
<b>Band Policy</b>	<p><b>Note:</b> Traffic Shaping (<b>Configuration Service - 2.2.6 Traffic Shaping</b>, page 81) has to be configured for Band Policy settings to apply. Band Policy settings work independently from Bandwidth Protection settings (see above).</p> <p>Band Policy settings rely on connection objects being allotted to Bands in firewall rule sets. Band Policy settings specify bandwidth assignment to transports as a whole. Multiple transports may share a single band when they are processed through the same interface. The following settings determine behaviour:</p> <ul style="list-style-type: none"> <li>➤ <b>Use Band According to Rule Set</b></li> </ul> <p>This setting uses the band from the firewall rule allowing traffic between the tunnel endpoints.</p> <ul style="list-style-type: none"> <li>➤ <b>Copy Band From Payload To Envelope</b></li> </ul> <p>This setting uses the band from the firewall rule redirecting traffic to the VPN tunnel entry point. The band setting for the rule configuring traffic between the tunnel endpoints is then ignored.</p> <ul style="list-style-type: none"> <li>➤ <b>Fixed Envelope Band</b></li> </ul> <p>This setting specifies a band statically. It activates the parameter <b>Envelope Band Value</b> below, where one of the available bands (System, Band A-G) has to be selected.</p>

**List 5-48** VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... > TI tab - section VPN Envelope Policy

Parameter	Description
<b>Replay Window Size</b>	<p>The <b>Replay Window Size</b> is designed for sequence integrity assurance and avoidance of IP packet "replaying", when due to ToS policies assigned to VPN tunnels and/or transports packets are not forwarded instantly according to their sequence number. The window size specifies a maximum number of IP packets that may be on hold until it is assumed that packets have been sent repeatedly and sequence integrity has been violated. The replay window size may be defined globally (see <b>Global Replay Window Size</b>, page 207). If not specified in this place, without a global value being defined, the default value of <b>32</b> packets is used, and with a global value defined, the global value is used. The effective Replay Window Size is visualised in the Transport Details window (Attribute: transport_replayWindow), which can be accessed by double-clicking the tunnel in the  <b>VPN Monitoring</b> GUI &gt; <b>Active</b> tab (see 3. Monitoring, page 229).</p>

**List 5-49** VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... > TI tab - section Transport (complement)

Parameter	Description
<b>On Demand Transport Timeout</b>	<p>This parameter is only available with <b>Direction mode OnDemand</b> (page 221). It specifies the period of inactivity after which to terminate the tunnel (default: <b>60 seconds</b>).</p>
<b>Delay</b>	<p>This parameter is only available with <b>Direction mode OnDemand</b> (page 221). When set, traffic is not processed the moment it arrives. Instead, it is delayed for the time span specified, until more traffic has accumulated (default: <b>0 seconds</b>, no delay).</p>

## 2.7.2 Configuring IPsec Tunnels

**Note:**

For further information concerning the configuration of IPsec with phion netfence and for third-party appliances have a look at the documentation **phion netfence IPsec Configuration**.

### 2.7.2.1 Overview

The IPsec suite of protocols is used to provide encryption and authentication at IP-Layer, this means authentication of data origin and integrity, as well as data content confidentiality and replay protection are transparent to any application which operates on a higher layer than IP.

**Note:**

For general information concerning IPsec, please have a look at [www.netbsd.org/Documentation/network/ipsec/](http://www.netbsd.org/Documentation/network/ipsec/)

IPsec consists out of three Standards, namely:

- **ESP (Encapsulating Security Payload)**

**Note:**

Since ESP provides everything AH is capable of but also provides data confidentiality and limited traffic flow confidentiality, we do not support AH yet.

- **AH (Authentication Header)**
- **ISAKMP (Internet Security Association and Key Management Protocol)** consists out of two Steps:
  - Phase 1 (Main-Mode)
  - Phase 2 (Quick-Mode)

Establishing an IPsec Tunnel usually consists of the following steps:

**Step 1 The "Active" IPsec Peer establishes a UDP Port 500 connection to the "Passive" one.**

After that both Peers negotiate a Main-Mode SecurityAssociation using their Pre-Shared Secret, this is done to verify data integrity and confidentiality.

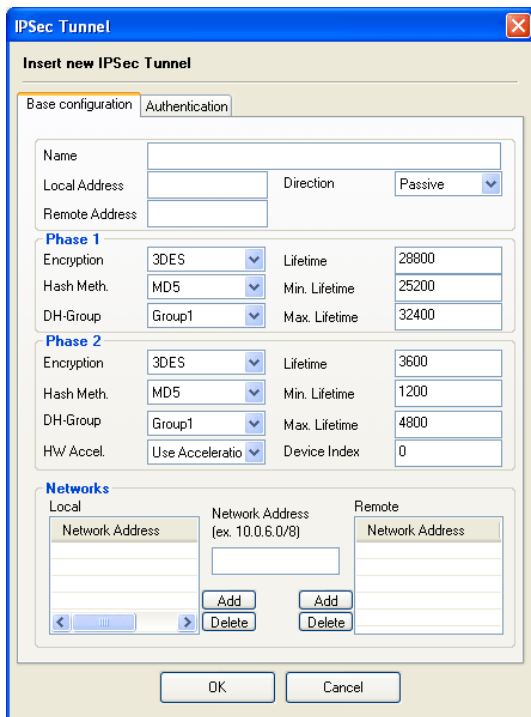
**Step 2 Various Quick-Mode SecurityAssociations are established on top of the existing Phase1(Main-Mode) SecurityAssociation, these provide keying and configuration material for Step 3.**

**Step 3 Any IP Packet which matches a prior established SecurityAssociation will be encrypted and authenticated using the keying and configuration material found in the corresponding Phase2 SecurityAssociation.**

**2.7.2.2 Configuring**

The introduction of IPsec tunnels is very similar to that of phion to phion tunnels. The configuration, however, is rather different.

Fig. 5-41 IPsec Tunnel configuration - Base configuration tab



List 5-50 VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Base configuration tab

Parameter	Description
<b>Name</b>	This is the tunnel name needed for informational and partner identification purpose. <b>Note:</b> IPsec tunnel names may contain a maximum of 26 characters.
<b>Local Address</b>	Used for defining the local IP address. <b>Note:</b> When working with dynamic IPs use 0.0.0.0/32 as local address.
<b>Remote Address</b>	Used for defining the remote IP address.

List 5-50 VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Base configuration tab

Parameter	Description
<b>Direction</b>	Defines whether the tunnel is <b>Active</b> or <b>Passive</b> (default). <b>Note:</b> Direction <b>Active</b> implies accepting ( <b>Passive</b> ), too.

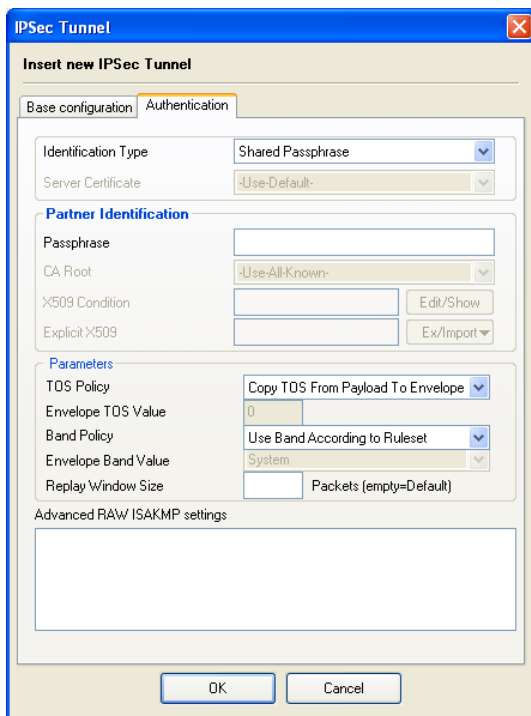
List 5-51 VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Base configuration tab - section Phase 1 and Phase 2

Parameter	Description
<b>Encryption</b>	Defines what kind of encryption is used. Available algorithms for <b>Phase 1</b> are: <b>3DES</b> (default), <b>DES</b> and <b>CAST</b> . Available algorithms for <b>Phase 2</b> are: <b>AES</b> , <b>3DES</b> (default), <b>CAST</b> , <b>Blowfish</b> and <b>DES</b> .
<b>Hash Meth.</b>	Defines the used hash algorithm. Available algorithms are <b>MD5</b> (default) and <b>SHA</b> .
<b>DH-Group</b>	The Diffie-Hellman Group defines the way of key exchange. The available options for this parameter are <b>Group1</b> (default; 768-bit modulus), <b>Group2</b> (1024-bit modulus), and <b>Group5</b> (1536-bit modulus).
<b>HW Accel.</b>	The <b>HW Acceleration</b> parameter allows you to select the preferred encryption engine, - that is the CPU or a hardware accelerator - if present. This allows for load balancing between CPU and an optional crypto card with more than one tunnel in use. <ul style="list-style-type: none"> <li>➤ <b>Use Acceleration Card (if present)</b> (default) Select this option, if you have installed and intend to use a crypto accelerator hardware board. Note that for this to function the corresponding module supporting the card has to be loaded in the local firewall settings (see <b>VPN HW Modules</b>, page 128).</li> <li>➤ <b>Use CPU</b> Select this option to use CPU acceleration.</li> </ul>
<b>Lifetime</b>	Rekeying time in seconds the server offers to the partner.
<b>Min. Lifetime</b>	Minimum rekeying time in seconds the server accepts from its partner.
<b>Max. Lifetime</b>	Maximum rekeying time in seconds the server accepts from its partner.
<b>Device Index</b>	The tunnel is fed through <b>vpn0</b> by default. You may use another VPN interface by adjusting the <b>VPN Device Index</b> . Note, that you first have to create indexed VPN interfaces if you want to use this option (see 2.3.2 Server Key/Settings Tab, <b>Device Index</b> , page 207).

List 5-52 VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Base configuration tab - section Networks

Parameter	Description
<b>Local Networks</b>	Contains the local networks (use phion notation, <b>Getting Started</b> - 5. phion Notation, page 25).
<b>Remote Networks</b>	Contains the remote networks (use phion notation, <b>Getting Started</b> - 5. phion Notation, page 25).

Fig. 5-42 IPSec Tunnel configuration - Authentication tab



List 5-53 VPN configuration - Site to Site - IPSEC Tunnels tab &gt; New IPSec tunnel ... &gt; Authentication tab

Parameter	Description
<b>Identification Type</b>	The following identification types are available for configuration: <ul style="list-style-type: none"> <li>➤ <b>Shared Passphrase</b></li> <li>➤ <b>X509 Certificate (CA signed)</b></li> <li>➤ <b>X509 Certificate (explicit)</b></li> <li>➤ <b>Box SCEP Certificate (CA signed)</b></li> </ul>


List 5-54 VPN configuration - Site to Site - IPSEC Tunnels tab &gt; New IPSec tunnel ... &gt; Authentication tab - section Partner Identification

Parameter	Description
	Depending on the configured identification type different fields are unlocked in the section Partner Identification (see 1.4.2 Authentication, page 201).

List 5-55 VPN configuration - Site to Site - IPSEC Tunnels tab &gt; New IPSec tunnel ... &gt; Authentication tab - section Parameters

Parameter	Description
<b>TOS Policy</b>	This policy setting specifies how to deal with the <b>Type of Service (ToS)</b> information in a packet's IP header. In networks the ToS may be utilised to define the handling of the datagram during transport. If the ToS is enveloped, this information is lost. The following settings are available: <ul style="list-style-type: none"> <li>➤ <b>Copy TOS From Payload to Envelope</b></li> </ul> <p><b>Note:</b> This setting can only be used with non TCP transports.</p> <p>In this mode the packet's original ToS information is copied to the envelope and thus remains available for utilisation.</p> <ul style="list-style-type: none"> <li>➤ <b>Fixed Envelope TOS</b></li> </ul> <p>In this mode the ToS information is masked by enveloping it without consideration. This setting activates parameter <b>Envelope TOS Value</b> (default: <b>0</b>) where a fixed ToS value has to be specified. All packets will thus be assigned the same ToS information.</p>

List 5-55 VPN configuration - Site to Site - IPSEC Tunnels tab &gt; New IPSec tunnel ... &gt; Authentication tab - section Parameters

Parameter	Description
<b>Band Policy</b>	<p><b>Note:</b> Traffic Shaping (<b>Configuration Service</b> - 2.2.6 Traffic Shaping, page 81) has to be configured for Band Policy settings to apply. Band Policy settings work independently from Bandwidth Protection settings (see above).</p> <p>Band Policy settings rely on connection objects being allotted to Bands in firewall rule sets. Band Policy settings specify bandwidth assignment to transports as a whole. Multiple transports may share a single band when they are processed through the same interface. The following settings determine behaviour:</p> <ul style="list-style-type: none"> <li>➤ <b>Use Band According to Rule Set</b> This setting uses the band from the firewall rule allowing traffic between the tunnel endpoints.</li> <li>➤ <b>Copy Band From Payload To Envelope</b> This setting uses the band from the firewall rule redirecting traffic to the VPN tunnel entry point. The band setting for the rule configuring traffic between the tunnel endpoints is then ignored.</li> <li>➤ <b>Fixed Envelope Band</b> This setting specifies a band statically. It activates the parameter <b>Envelope Band Value</b> below, where one of the available bands (System, Band A-G) has to be selected.</li> </ul>
<b>Replay Window Size</b>	<p>The <b>Replay Window Size</b> is designed for sequence integrity assurance and avoidance of IP packet "replaying", when due to ToS policies assigned to VPN tunnels and/or transports packets are not forwarded instantly according to their sequence number. The window size specifies a maximum number of IP packets that may be on hold until it is assumed that packets have been sent repeatedly and sequence integrity has been violated. The replay window size may be defined globally (see <b>Global Replay Window Size</b>, page 207). If not specified in this place, without a global value being defined, the default value of <b>32</b> packets is used. If not specified in this place with a global value defined, the global value is used.</p> <p>The effective Replay Window Size is visualised in the Transport Details window (Attribute: transport_replayWindow), which can be accessed by double-clicking the tunnel in the  <b>VPN Monitoring</b> GUI &gt; <b>Active</b> tab (see 3. Monitoring, page 229).</p>
<b>Advanced RAW ISAKMP settings</b>	<p>This field allows you to define additional parameters for establishing IPsec tunnels. When appending such an additional parameter start with entering the section the parameter assigned to. The next line then contains the new parameter itself (ONE value, ONE line). for example [Section] key=value</p> <p>The new sections are added to the end of the <code>isakmpd.conf</code> file. New parameters, however, are added on the top of the according section.</p> <p><b>Note:</b> For detailed information concerning the syntax that has to be used within this field, please consult <a href="http://www.openbsd.org/cgi-bin/man.cgi">www.openbsd.org/cgi-bin/man.cgi</a> (man page: <code>isakmpd.conf</code>).</p>

## 3. Monitoring

### 3.1 Active Tab

After successful connection to the VPN service the VPN Status is displayed in this window.

The status shows the VPN sessions and the firewall-to-firewall tunnels that are currently open as well as their respective data in the following columns:

- **Tunnel**  
Either FW2FW (**F**irewall **t**o **F**irewall Tunnel), PERS (**P**ersonal License), IPSec, PGRP (**P**hion **G**roup), or IGRP (**I**PSec **G**roup).
- **Name**  
Displays the name of the user.
- **Type**  
Displays the type of tunnel.
- **Group**  
Shows the VPN group the user is assigned to.
- **Local**  
Displays the local IP address/network
- **Peer**  
Displays client internet IP address
- **Virtual IP**  
Displays client's virtual IP address.
- **Info**  
Shows the type of tunnel, the state, or the certificate subject (depending on the tunnel type). For FW2FW and IPSec here the entry **firewall tunnel** is shown. As soon as a tunnel is a passive one and is in down-state, the entry **DOWN (passive)** is shown. For "group" tunnels with certificate, the x.509 subject is displayed.
- **Tunnel Mode**  
Shows transport mode, type of encryption, and the authentication algorithm (MD5/SHA1), separated with -.
- **bps10**  
Shows current transfer speed in bytes per 10 seconds.
- **Total**  
Shows total amount of traffic in kB/key.
- **Idle**  
Period of time in which the connection is resting (in seconds).
- **Start**  
Duration of VPN connection in minutes (m) or days (d).
- **Key**  
Age of issued key in minutes (m) or days (d).

Double-clicking an entry opens a new window with detailed information about the selected session's connection (such as the assigned **Group**, **Rekeying Time**, **Access Time**, **Peer IP Address**, ...).

Select the connection, right-click the selected row and choose **Terminate Tunnel** from the context menu to terminate a session. The tunnel gets terminated after an additional confirmation.

To re-establish a tunnel manually, select **Initiate Tunnel** from the context menu.

An IPSec tunnel can as well be terminated with the option **Hardkill Tunnel**. The difference between the two termination methods is the following:

#### **Terminate Tunnel**

This method kills Phase2 of the IPSEC tunnel. Phase2 can be re-initialised immediately as the tunnel partners exchange information with each other.

#### **Hard Kill Tunnel**

This method kills Phase1 of the IPSEC tunnel. As there is no exchange between the tunnel partners Phase1 can only be re-established if the partner kills his own Phase 1.

#### **Attention:**

Do not use **Hardkill Tunnel** until it is absolutely necessary. In case of doubt seek assistance by phion Support.

### 3.2 Status Tab

The **Status** tab provides information on all configured VPN connections on this machine.

You can enable/disable or temporarily enable configured connections by right-click on a license and selection of **Enable Tunnel**, **Disable Tunnel**, or **Temporary Enable Tunnel**. When selecting the latter, enter the period (in minutes) the tunnel should be enabled.

The button **Update List** refreshes the display.

The button **Show CRL ...** displays the Certificate Revocation List. The lines with blank first columns contain status information about the last CRL fetch (also displayed in the log).

The following columns are used for display:

- **Tunnel**  
Shows the name of the tunnel.
- **Name**  
Shows the name of the user.
- **Type**  
Shows the tunnel type.
- **Group**  
Shows the VPN group the user is assigned to.
- **Info**  
Displays information concerning the current connection (for example, **Access Granted**, **Disconnect**, ...)
- **State**  
Shows the status of the VPN connection (**ACTIVE/Ready**)
- **Succ.**  
Shows the number of successful connections.
- **Fail**  
Shows the number of failed connections.



- **Last Access**  
Shows expired amount of time since the last access.
- **Last Peer**  
Shows client IP address of last connection.
- **Last Info**  
Displays the last information concerning the connection (for example, **Access Granted**, **Disconnect**, ...).
- **Last Duration**  
Shows the duration of the last connection.
- **Last Client**  
Shows the client (inclusive version number) used for the last connection.
- **Last OS**  
Shows the operating system (inclusive kernel number) from which the last connection was carried out.

### 3.3 Access Tab

#### Status list (upper part of the **Access** tab)

The number of succeeded and aborted connections per license is listed in the status list. A maximum of 512 entries can be made.

The button **Update list** serves to refresh the view

The following columns are used for display:

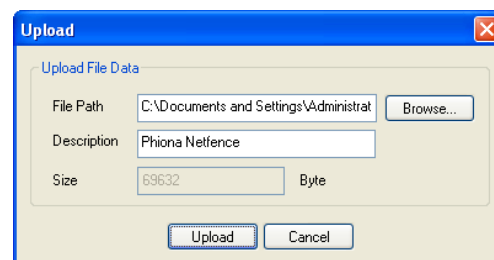
- **AID**  
Access ID
- **Tunnel**  
Either FW2FW (**F**irewall **t**o **F**irewall Tunnel), PERS (**P**ersonal License).
- **Name**  
Name of the user
- **Peer**  
Displays client internet IP address
- **Info**  
Shows name of person (defined during configuration) and IP address assigned by the license, separated with @, or alternatively the certificate subject.
- **Last**  
Shows duration in seconds (s), minutes (m) and days (d) since the last connection attempt.
- **Success**  
Shows total number of successful connections.
- **Fail**  
Shows total number of unsuccessful connections.
- **Last Status**  
Shows status of the last connection/connection attempt.

**Table 5-6** Possible "last connection" states

Status	Description
Root certificate not valid	
Certificate did not verify	phion certificate does not correspond with the one of the server
Certificate signature did not verify	The digital phion certificate shelf mark does not correspond with the one of the server
Certificate is expired	
Certificate not yet valid	The phion certificate has not yet obtained validity
Certificate does not belong to server	The phion certificate is valid for a different VPN server
Certificate index exceeds number of licenses	More phion certificates were issued than can be found on the server
Certificate issuer does not match	Personal license certificate issuer does not correspond with issuer of server certificate issuer
Certificate subject does not match	Subject of personal certificate license does not correspond with subject of server certificate
Unknown certificate error	
Mode not supported	Decoding / Compressing wrong
Invalid Peer	The client tunnel address does not correspond with the one entered on the server.
Requested Source IP does not match	The client address does not correspond with the one entered on the server
No client IP address assigned	Client address could not be issued
License or peer already in use	
Client IP address already in use	

- **VPN Client Downloads** (lower part of the **Access** tab)  
The VPN client Downloads area allows making arbitrary software downloads available to VPN clients connecting to the VPN Server.  
Clicking the **Upload ...** button opens the Upload window. Use the **Browse ...** button in this window to select the desired installation file and click **Upload** to copy it to the phion netfence. The next time a entegra VPN client connects to the VPN Server, it will be offered the installation file for download.

**Fig. 5-43** Upload dialogue



When obsolete, select an uploaded file and click the **Delete** button to remove the file from the VPN client Downloads list.

**Table 5-6** Possible "last connection" states

Status	Description
Granted	Successful connection
Already connected	
Access Denied (No license or invalid peer)	Connection denied due to missing license or wrong client address
Invalid Password	

## 4. SSL-VPN

### 4.1 Introduction

phion SSL-VPN gives you the opportunity of encrypted access to your internal networks without installing a software at your client.

From your client you will have access to

- internal websites
- Outlook Web Access
- WebDav / Sharepoint
- RDP
- VNC
- SSH
- Telnet
- SMTP
- POP3
- IMAP4
- SMB
- Generic Application Tunnels

RSA Next Token is supported, that means SSL-VPN provides an easy and secure solution to gain protected access to your internal network structure. Also dynamic firewall rules can be switched on / off via SSL-VPN.

### 4.2 Parameters

The configuration parameters for SSL-VPN are located at:  
**Config** > **Box** > **Virtual Servers** > <server> > **Assigned Services** > <service> (*vpnserver*) > **SSL\_VPN**

#### 4.2.1 Basic Setup

##### 4.2.1.1 General Service Settings

List 5-56 VPN configuration - SSL-VPN - Basic Setup - section General Service Settings

Parameter	Description
<b>Enable SSL-VPN</b>	Set this parameter to <b>yes</b> to enable SSL-VPN at the VPN server.
<b>Bind IPs</b>	Enter the IPs that should be used (they have to be configured as server IPs). <b>Note:</b> At all these IPs the port 443 has to be idle. Otherwise SSL-VPN cannot start.
<b>Allow SSLv2</b>	Selecting this checkbox enables SSLv2.

##### 4.2.1.2 Service Identification

List 5-57 VPN configuration - SSL-VPN - Basic Setup - section Service Identification

Parameter	Description
<b>Use Self-Signed Certificate</b>	Set to <b>yes</b> and you will use a self-signed certificate, with <b>no</b> you will use an external-signed certificate. <b>Note:</b> Self-signed certificates often cause a warning from the browser.
<b>Self-Signed Private Key</b>	Use this parameter to create or export a self-signed key.
<b>Self-Signed Certificate</b>	Use this parameter to view, create, edit, or export a self-signed certificate.
<b>External-Signed Private Key</b>	Use this parameter to create, import, or export an external-signed key.
<b>External-Signed Certificate</b>	Use this parameter to view, import, or export an external-signed certificate.

### 4.2.2 Authentication & Login

#### 4.2.2.1 User Authentication

List 5-58 VPN configuration - SSL-VPN - Authentication & Login - section User Authentication

Parameter	Description
<b>Authentication Scheme</b>	This parameter defines the authentication scheme for login (user/password combination). Choose between <ul style="list-style-type: none"> <li>➤ <b>MSNT</b></li> <li>➤ <b>MS_ACTIVE_DIRECTORY</b></li> <li>➤ <b>LDAP</b></li> <li>➤ <b>RADIUS</b></li> <li>➤ <b>RSA_SECUREID</b></li> </ul> RSA Next Token mode is also supported. <b>Note:</b> Authentication Scheme OCSP is not supported.
<b>Use Group Policies</b>	Setting this parameter to <b>yes</b> (default: <b>no</b> ) enables parameters <b>Allowed User Groups</b> and <b>Blocked User Groups</b> for defining access restrictions according to group information.
<b>Allowed User Groups</b>	Enter groups for which access is granted into this field and click <b>Insert...</b> in order to add them to the listing on the right.
<b>Blocked User Groups</b>	Login names of users which are not allowed to use the proxy. This setting allows more fine grained control of access refusal than a group based option. The user will not be refused access by the authentication subsystem but the proxy engine itself. The user will receive an appropriate message instructing her/him that no valid authorization to use the service could be determined. Enter groups for which access is denied into this field and click <b>Insert...</b> in order to add them to the listing on the right. <b>Note:</b> Policy enforcement parameters <b>Allowed User Groups</b> and <b>Blocked User Groups</b> have the following preferences: <ul style="list-style-type: none"> <li>➤ <b>Blocked User Groups</b> overrules <b>Allowed User Groups</b> (having a user in both groups causes a block)</li> <li>➤ leaving both fields empty results in allow all</li> </ul>
<b>Use Max. Tunnels</b>	Set this parameter to <b>yes</b> to be able to use the parameter <b>Max. Tunnels</b> .
<b>Max. Tunnels</b>	Enter the value for the maximum of tunnels you want to allow (max. 256)
<b>Cookie Timeout (Min.)</b>	This is the time in minutes, how long the cookie is valid. Range: 5 to 180, default is 30. When this time has passed, the client will be redirected to the login page.

**List 5-58** VPN configuration - SSL-VPN - Authentication & Login - section User Authentication

Parameter	Description
<b>Browser Cleanup</b>	Setting this parameter to <b>yes</b> forces the browser (Microsoft IE6 and IE7, Mozilla Firefox 2 and 3) to clean up when exiting via the <b>Sign Out</b> button. Default is <b>yes</b> .  <b>Cleanup Firefox:</b> <ul style="list-style-type: none"> <li>➤ All global history pages of the SSL-VPN host</li> <li>➤ Downloaded files in the download manager</li> <li>➤ All cache entries</li> <li>➤ Cookies SSL-VPN</li> <li>➤ Form history (search bar)</li> <li>➤ Passwords SSL-VPN</li> </ul> <b>Note:</b> Cleanup process will be initiated after agreeing to a browser enquiry.  <b>Cleanup Internet Explorer:</b> <ul style="list-style-type: none"> <li>➤ <b>All (!)</b> entries in the browser history</li> <li>➤ <b>All (!)</b> passwords</li> <li>➤ Navigation</li> <li>➤ Internet cache</li> <li>➤ Registry history</li> </ul> <b>Note:</b> ActiveX has to be enabled.  <b>Note:</b> Cleanup process will be initiated after agreeing to a browser enquiry.  <b>Note:</b> Cleanup process will only be initiated if there is a connection to the internet. Due to this behaviour and that all entries and passwords will be erased when the browser is cleaned up, we recommends to use Mozilla Firefox instead of Internet Explorer.

### 4.2.2.2 Corporate ID

**List 5-59** VPN configuration - SSL-VPN - Authentication & Login - section Corporate ID

Parameter	Description
<b>Logo</b>	Import a logo via the the <b>Ex/Import</b> button. Best size is 200x66 pixel.
<b>Login Greeting Text</b>	This text will be shown as a greeting message.
<b>Help Text (html)</b>	Enter here your customized help text for your users.

## 4.2.3 entegra Access Control

### 4.2.3.1 entegra Access Control Setup

**List 5-60** VPN configuration - SSL-VPN - entegra Access Control - section entegra Access Control Setup

Parameter	Description
<b>Active</b>	Activate here the possibility to do a health check on clients which will connect with SSL-VPN.
<b>Policy Server IP</b>	Enter here your Policy Server IP.
<b>User Groups</b>	Enter here the user groups, which should use this resource to do a health check.

## 4.2.4 Web Resources

### 4.2.4.1 Web Resource Configuration

**List 5-61** VPN configuration - SSL-VPN - Web Resources - section Web Resource Configuration

Parameter	Description
<b>Web Resources</b>	To edit an already existing entry, select it and click <b>Edit....</b> To create a new entry, click <b>Insert</b> and give it a <b>Name</b> . To remove an existing entry, select it and click <b>Delete</b> . See list 5-62 for parameter description.

**List 5-62** Web Resources - section Web Resource Access Authorization

Parameter	Description
<b>Active</b>	Setting this to <b>yes</b> enables the link, which will be shown later in the web page.
<b>Visible Name</b>	Configure here the name of the link, which will be shown in the web page.
<b>Link Description</b>	Enter here a description of the link, which will be shown in the web page.
<b>Kind of Application</b>	Choose between <ul style="list-style-type: none"> <li>➤ <b>Other</b></li> <li>➤ <b>Mail</b></li> <li>➤ <b>Web</b></li> </ul>
<b>Protocol Type</b>	This parameter is only configurable when parameter <b>Kind of Application</b> is set to <b>Mail</b> or <b>Web</b> . Choose between <ul style="list-style-type: none"> <li>➤ <b>HTTP</b></li> <li>➤ <b>HTTPS</b></li> </ul>
<b>URL</b>	Enter here the URL to which the link will follow.
<b>Must Be Healthy</b>	Selecting the checkbox means that a positive health check is required to enable the link.
<b>Active Content Rewrite</b>	The SSL-VPN gateway acts similar to a HTTP proxy. Therefore, all HTTP requests must be forwarded to the SSL-VPN and not to the web server directly. This is only possible if <b>Active Content Rewrite</b> is enabled. This will cause the SSL-VPN gateway to manipulate URLs appearing within HTTP packets on the fly (e.g. IP addresses or domain names of foreign web servers are replaced by the appropriate SSL-VPN gateways bind IP address). Hence, all HTTP requests will be forwarded to the SSL-VPN gateway. The SSL-VPN itself establishes the HTTP connection to the web server and sends the HTTP replies back to the client.
<b>Allowed User Groups</b>	Enter here the user groups which will be allowed to use this resource.

## 4.2.5 Outlook Web Access

### 4.2.5.1 Outlook Web Access Authorization

**List 5-63** VPN configuration - SSL-VPN - Outlook Web Access - section Outlook Web Access Authorization

Parameter	Description
<b>Active</b>	Setting this to <b>yes</b> enables the link, which will be shown later in the web page.
<b>Visible Name</b>	Configure here the name of the link, which will be shown in the web page.
<b>OWA URL</b>	Enter here the internal URL to which the link will follow. For example: <code>https://hq-mx/owa</code>
<b>Must Be Healthy</b>	Selecting the checkbox means that a positive health check is required to enable the link.
<b>Allowed User Groups</b>	Enter here the user groups which will be allowed to use this resource.

## 4.2.6 WebDAV / Sharepoint

### 4.2.6.1 WebDAV Resource Configuration

**List 5-64** VPN configuration - SSL-VPN - WebDAV/Sharepoint - section WebDAV Resource Configuration

Parameter	Description
<b>WebDAV Resources</b>	To edit an already existing entry, select it and click <b>Edit....</b> To create a new entry, click <b>Insert</b> . To remove an existing entry, select it and click <b>Delete</b> . See list 5-65 for parameter description.

**List 5-65** WebDAV Resources - section WebDAV Resource Access Authorization

Parameter	Description
<b>Active</b>	Setting this to <b>yes</b> enables the link, which will be shown later in the web page.
<b>Visible Name</b>	Configure the name of the link, which will be shown in the web page.

**List 5-65** WebDAV Resources - section WebDAV Resource Access Authorization

Parameter	Description
<b>Link Description</b>	Enter a description of the link, which will be shown in the web page.
<b>WebDAV Address</b>	Enter here the IP address of the WebDAV resource.
<b>WebDAV Sharename</b>	Enter the name of the desired share.
<b>Must Be Healthy</b>	Selecting the checkbox means that a positive health check is required to enable the link.
<b>Allowed User Groups</b>	Enter the user groups which will be allowed to use this resource.

## 4.2.7 Application Tunneling

### 4.2.7.1 Application Tunneling Configuration

**List 5-66** VPN configuration - SSL-VPN - Application Tunneling - section Application Tunneling Configuration

Parameter	Description
<b>Service Configuration</b>	To edit an already existing entry, select it and click <b>Edit...</b> To create a new entry, click <b>Insert</b> . To remove an existing entry, select it and click <b>Delete</b> . See list 5-67 for parameter description.
<b>Generic Application Tunneling</b>	To edit an already existing entry, select it and click <b>Edit...</b> To create a new entry, click <b>Insert</b> . To remove an existing entry, select it and click <b>Delete</b> . See list 5-68 for parameter description.

**List 5-67** Application Tunneling Configuration - Service Configuration - section Application Access Authorization

Parameter	Description
<b>Active</b>	Setting this to <b>yes</b> enables the link, which will be shown later in the web page.
<b>Visible Name</b>	Configure here the name of the link, which will be shown in the web page.
<b>Link Description</b>	Enter here a description of the link, which will be shown in the web page.
<b>Application Server IP</b>	Enter here the IP of the back-end server application, which will be tunnelled by SSL-VPN.
<b>Application Protocol</b>	Choose here the type of protocol, which should be tunnelled by the SSL-VPN. Possible are: <b>RDP, VNC, SSH, Telnet, SMTP, POP3, IMAP4, SMB</b> <b>Note:</b> If you set this parameter to <b>VNC</b> , make sure that VNC doesn't require <b>MS Logon</b> for authentication.
<b>Application TCP Port</b>	Configure here the port on which you want to connect at the back-end server.
<b>RDP Application Path</b>	With the SSL-VPN delivered RDP-applet it is possible to configure a so called <b>Application Path</b> . This means it is possible that only one application is started and shown in the RDP-applet. For example: <code>phiona</code> <b>Note:</b> This parameter is only enabled when <b>Application Protocol</b> > <b>RDP</b> is specified. When using this option no client program is possible.
<b>SMB Path</b>	Enter here the Samba path on which the delivered SMB browser will start on the SMB server. <b>Note:</b> This parameter is only enabled when <b>Application Protocol</b> > <b>SMB</b> is specified.
<b>Tunnel Client Application</b>	Setting this parameter to <b>yes</b> , the link in the SSL-VPN web page gets an additional link where a port-forwarding applet is starting, and opens on a loopback address a listening socket, which could be connected by (for example: RDP) a client program. <b>Note:</b> This parameter is only enabled when <b>RDP, VNC, SSH, Telnet</b> or <b>SMB</b> is configured at <b>Application Protocol</b> . When choosing <b>SMTP, POP3</b> or <b>IMAP4</b> this parameter is disabled and set to <b>yes</b> .
<b>Client Loopback TCP Port</b>	Enter here the port on which the port-forwarding applet will listen on the client machine, and then could be connected with the client program. For example: RDP.
<b>Must Be Healthy</b>	Selecting the checkbox means that a positive health check is required to enable the link.

**List 5-67** Application Tunneling Configuration - Service Configuration - section Application Access Authorization

Parameter	Description
<b>Allowed User Groups</b>	Enter here the user groups which will be allowed to use this resource.

**List 5-68** Application Tunneling Configuration - Generic Application Tunneling - section Generic Application Tunneling Authorization

Parameter	Description
<b>Active</b>	Setting this to <b>yes</b> enables the link, which will be shown later in the web page.
<b>Visible Name</b>	Configure here the name of the link, which will be shown in the web page.
<b>Link Description</b>	Enter here a description of the link, which will be shown in the web page.
<b>SSL Tunnels</b>	To edit an already existing entry, select it and click <b>Edit...</b> To create a new entry, click <b>Insert</b> . To remove an existing entry, select it and click <b>Delete</b> . See list 5-69 for parameter description.
<b>Must Be Healthy</b>	Selecting the checkbox means that a positive health check is required to enable the link.
<b>Allowed User Groups</b>	Enter here the user groups which will be allowed to use this resource.

**List 5-69** Generic Application Tunneling Authorization - SSL Tunnels - section SSL Tunnel Configuration

Parameter	Description
<b>Server IP</b>	Configure here the server IP of the application which you would like to tunnel.
<b>Client Loopback TCP Port</b>	Enter here the port on which the port-forwarding applet will listen on the client machine, and then could be connected with the client program.
<b>Application TCP Port</b>	Configure here the port on which the server application is listening on.

## 4.2.8 Dynamic Firewall Rules

### 4.2.8.1 Dynamic Firewall Rules

**List 5-70** VPN configuration - SSL-VPN - Dynamic Firewall Rules - section Dynamic Firewall Rules

Parameter	Description
<b>Firewall Rule Activation</b>	To edit an already existing entry, select it and click <b>Edit...</b> To create a new entry, click <b>Insert</b> . To remove an existing entry, select it and click <b>Delete</b> . See list 5-71 for parameter description.

**List 5-71** Firewall Rule Activation - section Dynamic Firewall Rule Activation Authorization

Parameter	Description
<b>Active</b>	Setting this to <b>yes</b> enables the link, which will be shown later in the web page.
<b>Visible Name</b>	Configure here the name of the link, which will be shown in the web page.
<b>Link Description</b>	Enter here a description of the link, which will be shown in the web page.
<b>Dynamic Rule Selector</b>	Enter here the name of the firewall rules, which should be shown on this Firewall Resource page.
<b>Must Be Healthy</b>	Selecting the checkbox means that a positive health check is required to enable the link.
<b>Allowed User Groups</b>	Enter here the user groups which will be allowed to use this resource.

## 4.2.9 Access Rights Query

### 4.2.9.1 Access Rights Query

**List 5-72** VPN configuration - SSL-VPN - Access Rights Query - section Access Rights Query

Parameter	Description
<b>Username</b>	Insert the designated username and click the <b>Query</b> button.

List 5-72 VPN configuration - SSL-VPN - Access Rights Query - section Access Rights Query

Parameter	Description
<i>Userlinks</i>	All links of the user entered at <i>Username</i> are listed here.

## 4.3 Setup Examples

### 4.3.1 Basic Setup

#### 4.3.1.1 Requirements

- A VPN service must be established at the box. SSL-VPN is a part of the VPN server.
- To start this server, parameter **Enable SSL-VPN** has to be set to **yes**.
- An additional IP has to be used for SSL-VPN, otherwise the service cannot start (port 443 would be busy by the VPN server). Configure this IP in the server properties.

#### 4.3.1.2 Certificates

- For testing or internal SSL-VPN access you may use a **Self-Signed Certificate** and a **Self-Signed Private Key** and add the certificate to the respective browsers (otherwise the browser will pop up an error message).
- For external SSL-VPN access it is recommended to use an **External-Signed Certificate** (so browsers won't pop up an error message).

### 4.3.2 Authentication & Login

#### 4.3.2.1 MSAD User Groups

- in **Config > Box > Infrastructure Services > Authentication Service** set the parameter **Activate Scheme** to **Yes**
- Check that the **Method** is **ACTIVE\_DIRECTORY**
- At **Basic** insert a data set and configure all parameters
- Browse to **Config > Box > Infrastructure Services > Authentication Service > Virtual Servers > <server> > Assigned Services > <service> (vpnserver) > SSL\_VPN**
- In view **Authentication & Login** set the parameter **Authentication Scheme** to **MS\_ACTIVE\_DIRECTORY**

#### 4.3.2.2 Customizing the SSL-VPN Point-of-entry

You may customize the appearance of the web page (see Corporate ID, page 232) with these parameters:

- **Logo**, to place a company logo
- **Login Greeting Text**,
- **Help Text (html)**, to describe your own help instructions for your users

### 4.3.3 entegra Access Control

The configuration of entegra takes place at the policy server and not at the SSL-VPN parameters. No virus

scanner or updates to firewall rule sets can be executed by the SSL-VPN.

- But SSL-VPN is capable of executing a health check. In succession the access to sensible resources can be prohibited.

### 4.3.4 Web Resources

For example, we want to configure an access to an internal portal.

- In the **Web Resources** dialogue (see list 5-62, page 232) select the checkbox **Active** (or the web resource won't show up on the web page).

#### Note:

This is true for all configurable resources.

- Every resource has a **Name** (see parameter **Web Resources**) and a **Visible Name**. The name of the resource should differ from name that the user knows (For example server name `sales-portal` and the users would know it as `intranet`).
- The **Link Description** will be shown on the web page.
- Insert the **URL**
- **Active Content Rewrite** is selected by default (For parameter description see parameter **Active Content Rewrite**, page 232.)
- In parameter **Allowed User Groups** we leave the default asterisk (\*) to enable access for all users.

### 4.3.5 WebDAV / Sharepoint

#### 4.3.5.1 Scenario

We want to establish an SSL-VPN access for all sales staff members to the sales server. Files will be up-and downloaded, so there will be a potential risk of virus infiltration.

- Server name: salesshare
- Server IP address: 192.168.10.100
- Health check required

#### 4.3.5.2 Required Settings

- At the **WebDAV Resources** click **Insert** and assign the name `salesshare`
- Select checkbox **Active** (is default)
- As **Visible Name** enter `Sales-Share`
- At **Link Description** enter `This is the share server of the Sales Department`
- At **WebDAV Address** enter `192.168.10.100`
- Select checkbox **Must Be Healthy**
- At **Allowed User Groups** delete the asterisk (\*) and enter the MSAD group name of the Sales Department, for example `CN=sales*`



## 4.3.6 Application Tunneling - Service Configuration

### 4.3.6.1 RDP Scenario 1

We want to establish an SSL-VPN access for all accounting staff members to the terminal server (name: hq-account, IP address: 10.0.0.100) of the accounting department.

We want to offer 2 variants,

- one to connect with the phion applet
- one to connect with the windows RDP application

### 4.3.6.2 Required Settings

- At the **Service Configuration** click **Insert** and assign the name `hq-account`
- Select checkbox **Active** (is default)
- As **Visible Name** enter `Terminal Server - Accounting`
- At **Link Description** enter `This is the terminal server of the Accounting Department`
- As **Application Server IP** enter `10.0.0.100`
- At **Application Protocol** select **RDP**
- At **Application TCP Port** no changes are necessary if port 3389 is configured at the terminal server. If not, select checkbox **Other** and enter the appropriate port number.
- **RDP Application Path** leave empty (used in scenario 2)
- At **Tunnel Client Application** select **yes**, because we want to provide port forwarding.
- At **Client Loopback TCP Port** enter `3390`
- At **Allowed User Groups** delete the asterisk (\*) and enter the MSAD group name of the Accounting Department, for example `CN=accounting*`

### 4.3.6.3 RDP Scenario 2

We want to establish an SSL-VPN access for all sales staff members to the SAP application at the sales terminal server. It should only be possible to execute the SAP application.

- Sales terminal server IP address: `192.168.10.10`
- Path to SAP application: `C:\\SAP\\sap.exe`

### 4.3.6.4 Required Settings

- At the **Service Configuration** click **Insert** and assign the name `terminalsales`
- Select checkbox **Active** (is default)
- As **Visible Name** enter `SAP`
- At **Link Description** enter `This is the terminal server of the Sales Department`
- As **Application Server IP** enter `192.168.10.10`
- At **Application Protocol** select **RDP**
- At **RDP Application Path** enter `C:\\SAP\\sap.exe`

- At **Allowed User Groups** delete the asterisk (\*) and enter the MSAD group name of the Sales Department, for example `CN=sales*`

## 4.3.7 Application Tunneling - Generic Application Configuration

### 4.3.7.1 Scenario

We want to establish an SSL-VPN port forwarding access for all staff members to the citrix server (IP address: 10.0.0.112). All staff members working at a home office have to have a virus scanner and a firewall running.

Due to the fact that application browsing is based on UDP, this task can not be solved only with SSL-VPN. So, the applications have to be configured.

### 4.3.7.2 Required Settings

- At **Generic Application Tunneling** click **Insert** and assign the name `Citrix`
- Select checkbox **Active** (is default)
- As **Visible Name** enter `Citrix`
- At **Link Description** enter an appropriate description for your users
- As **SSL Tunnels** we insert the required connections, in this example all TCP ports. Click **Insert** and assign the following SSL tunnels.

Table 5-7 SSL tunnels

Name	Server IP	Client Loopback TCP Port	Application TCP Port
ICA	10.0.0.112	1494	1494
IMA	10.0.0.112	2512	2512
SSL	10.0.0.112	443	443
STA(ISS)	10.0.0.112	80	80
Citrix License Management Console	10.0.0.112	8082	8082
Presentation Server Licensing	10.0.0.112	27000	27000
ICA session w/ Session Reliability enabled	10.0.0.112	2598	2598
Access Gateway Standard and Advanced Editions	10.0.0.112	9001	9001
		9002	9002
		9005	9005
Manager service daemon server	10.0.0.112	2897	2897

- Select checkbox **Must Be Healthy**
- At **Allowed User Groups** leave the asterisk (\*) so all members of staff have access
- Configure the connections of the client software to the loopback address.

## 4.3.8 Dynamic Firewall Rules

### 4.3.8.1 Scenario

With SSL-VPN it is possible to enable/disable dynamic firewall rules at the netfence gateway.

We want to establish an FTP access from the intranet to the internet via a dynamic firewall rule.

- Firewall rule name: ftp-dynamic
- intranet address: 172.0.0.0

### 4.3.8.2 Required Settings

- Create a dynamic rule in the forwarding firewall and call it ftp-dynamic
  - **Source:** 172.0.0.0
  - **Service:** FTP (TCP 21 ftp)
  - **Destination:** 0.0.0.0
- Browse in the SSL-VPN settings to the **Dynamic Firewall Rules**
- At **Firewall Rule Activation** click **Insert** and assign the name FTP
- Select checkbox **Active** (is default)
- As **Visible Name** enter FTP
- At **Link Description** enter an appropriate description for your users, for example Here you can activate the dynamic firewall rule ftp-dynamic
- As **Dynamic Rule Selector** delete the asterisk (\*) and enter ftp-dynamic
- At **Allowed User Groups** delete the asterisk (\*) and enter the MSAD group name of the Administrators, for example CN=admin\*

## 4.4 Hints

- only **Java Runtime version 1.6.0** and higher is supported. To find out which version you have, type `java -version` on the command line.

Fig. 5-44 Java runtime version query



```

C:\WINDOWS\system32\cmd.exe
C:\>java -version
java version "1.6.0_07"
Java(TM) SE Runtime Environment (build 1.6.0_07-b06)
Java HotSpot(TM) Client VM (build 10.0-b23, mixed mode, sharing)
C:\>_
  
```

- Supported browsers are:
  - **Internet Explorer 6 and 7**
  - **Firefox 2 and 3**
- Up to **250 concurrent SSL-VPN connections** are supported. More are possible, but not recommended. Due to encryption performance and other system limitations this may cause technical difficulties, even when 250 are active.
- Both actions (manual and autoremediation) for the Antivirus and Antispy settings in the policy server config trustzone can be triggered automatically at the **Health Agent** with the **Do it** function from the context menu.
- Big messages and pictures may lead to a delay after download from the remediation server. Delay means, that the client needs some time to display them. Recommended pictures size is 30 kB. Large pictures will be scaled down, so it makes no sense of using them.
- SSL-VPN integra:

**Note:**

There is no enforcement of rules regarding personal firewalls.

- User authentication is only performed if local machine state is healthy, same applies to the integra client.
- If **Use Group Policies** is set to **yes** and a user is listed in **Allowed User Groups** and in **Blocked User Groups**, then this user has no access. The policy is **blocking in favor of allowing**.
- Info according to webpages and webservers:
  - Only domains and subdomains are allowed as URLs. That means a URL which is terminated by an ending `site.html` won't work. Allowed is for example `http://webservername.domain.subdomain` or `http://webservername/path1/path2`
  - HTTP redirects from one webserver to another webserver via SSL-VPN is not possible. Only weblinks are allowed (**no relaying**).
- The SSL-VPN server is not designed to rewrite all different kind of webservers out in the internet. So
  - it may happen that pictures, frames etc. will not be shown
  - no redirects are recommended
  - use the SSL-VPN interface as portal rather than linking from it to an internal portal
- Do not re-use links or send them via e-mail/messenger. These links won't work when a user that should not

have access to a web resource tries to reach the web resource by copy/paste the corresponding web resource URL into the browser: depending on the used application/application protocol a **404 not found** is send by the SSL-VPN (i.e. for RDP not a denied page is displayed but a status message).

- Rules are displayed in the browser firewall tab, if the configured `rulename` matches a rule. Only dynamic / timed rules are evaluated. If a dynamic rule of a cascaded rule list wants to be used the SSL-VPN portal one must use the **rule lists name** as matching criteria (rule name is generated as `rulelist:name`)  
You may use the character `*` as wildcard for a string in **Dynamic Rule Selector**, also use character `?` for a single character wildcard.
- You have to have local **administrative rights** for some actions, that the Health Agent wants you to carry out, for example
  - enable real time protection for Antivirus and Antispyware
  - enable Antivirus and Antispy
  - perform a system scan for Antivirus and Antispy
- SSL-VPN in combination with **entegra Health Agent**:
  - If the client is healthy, and the next health check fails, all opened connections will not be terminated until cookie timeout (see parameter **Cookie Timeout (Min.)**). New connections will not be initialized.
  - If the next Health Check fails, the client will be redirected to a `denied.html` page when he wants to open a new connection.
- When closing the browser all tunnels will remain open until cookie timeout (see parameter **Cookie Timeout (Min.)**) is reached.

## 5. Examples for VPN Tunnels

### 5.1 Fully Transparent Tunnel

The simplest possible tunnel configuration is a transparent connection of two networks with different address ranges. In effect, the tunnel configuration should not be noticeable by the connected networks.

Fig. 5-45 illustrates a fully transparent tunnel. Routing configuration between the two VPN servers is not considered in the setup, in order to keep the example simple. Except for scenarios with overlapping addresses, the VPN tunnels will not interfere with the routing configuration.

Fig. 5-45 Fully Transparent Tunnel

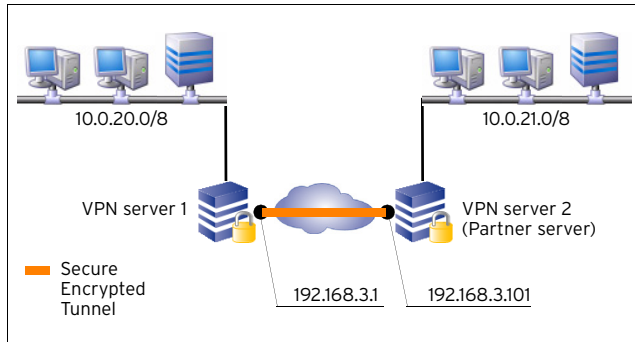


Table 5-8 Fully Transparent Tunnel - VPN Configuration on VPN server 1

Object	Configuration	Comment
Direction Mode	active or passive	Converse to the partner's configuration.
Timeout	10 for intranet, 30 for internet-like connections	
Encryption Mode	AES (or whatever is needed)	Can be unencrypted for intranet connections only aiming at routing assistance.
Transport Mode	UDP&TCP (or whatever is needed)	
Partner Server	192.168.3.101	
Partner Network	10.0.21.0/8	
Local Network	10.0.20.0/8	
Parameters	Dynamic	Only one IP address is assumed on the outside interface.

Table 5-9 Fully Transparent Tunnel - VPN configuration on VPN server 2

Direction Mode	Configuration	Comment
	active or passive	converse to the partner's configuration
Timeout	10 for intranet 30 for internet-like connections	
Encryption Mode	same as local side	
Partner Server	192.168.3.1	
Partner Network	10.0.20.0/8	
Local Network	10.0.21.0/8	
Parameters	Dynamic	Only one IP address is assumed on the outside interface.

#### Firewall configuration on VPN server 1 and VPN server 2

As the tunnel terminates before the firewall engine, rules have to be introduced allowing the local and partner networks to pass in both directions.

### 5.2 Stealth Tunnel

A further popular example for tunnelling is the so-called **stealth mode** or **half-side transparent tunnel**. In this case, a local network is granted access to a partner network but not vice versa. Moreover, the local networks internal IP structure is hidden from the partner network. In the example setup only one IP address (10.0.35.32) is explicitly directed into the tunnel.

#### Note:

The stealth tunnel shown in figure 5-46 masks the network on the left side from the network on the right side. Thus, firewall settings become crucial for functionality.

Fig. 5-46 Stealth Tunnel

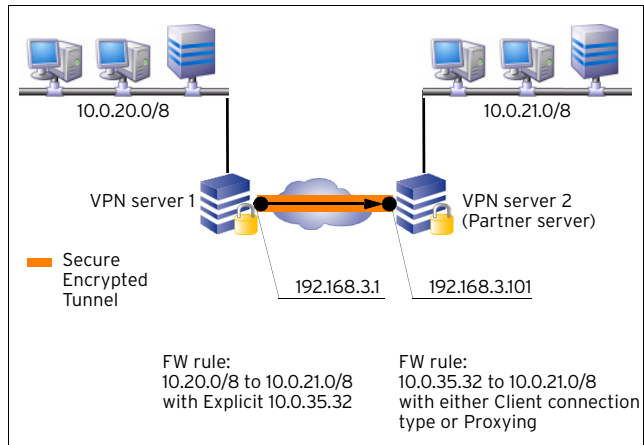


Table 5-10 Stealth Tunnel - VPN Configuration on VPN server 1

Object	Configuration	Comment
Direction Mode	active or passive	Converse to the partner's configuration.
Timeout	10 for intranet, 30 for internet-like connections	
Encryption Mode	AES (or whatever is needed)	Can be unencrypted for intranet connections only aiming at routing assistance.
Transport Mode	UDP&TCP (or whatever is needed)	
Partner Server	192.168.3.101	
Partner Network	10.0.21.0/8	
Local Network	10.0.35.32	Only this IP address is directed into the tunnel.
Parameters	Dynamic	Only one IP address is assumed on the outside interface.

#### Firewall configuration on VPN server 1:

Rules which are meant to direct traffic into the tunnel have to use connection type **Explicit**: 10.0.35.32.

Table 5-11 Stealth Tunnel - VPN configuration on VPN server 2

Object	Configuration	Comment
Direction Mode	active or passive	Converse to the partner's configuration.
Timeout	10 for intranet 30 for internet-like connections	
Encryption Mode	same as local side	

**Table 5-11** Stealth Tunnel - VPN configuration on VPN server 2

Object	Configuration	Comment
Partner Server	192.168.3.1	
Partner Network	10.0.35.32	
Local Network	10.0.21.0/8	
Parameters	Dynamic	Only one IP address is assumed on the outside interface.

### Firewall configuration on VPN server 2

As the tunnel terminates before the firewall engine, a rule has to be introduced allowing the IP address 10.0.35.32 to pass into the local network.

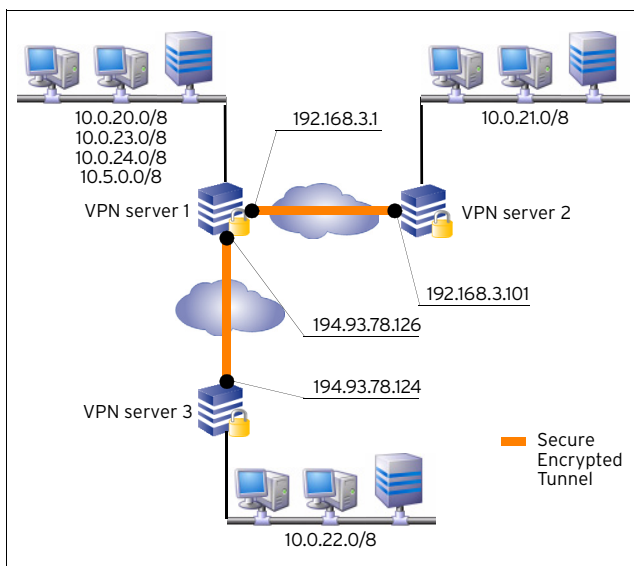
#### Further Remarks:

The proxy address may be chosen without restriction. Half-side transparent tunnelling is suited as alternative to personal VPN access. The local network IP address then derives from the personal VPN networks. Anyway, stealth mode tunnels may as well be operated without personal access configuration. As they are not fully transparent, there is no need to set up network routes, proxy ARPs, ...

Optionally, a local IP, for example 10.0.21.156, may be defined as right tunnel endpoint. In this case, the VPN server has to be instructed to request traffic, which is directed to this address. This can happen by either introducing the IP address 10.0.21.156 as personal access network, or by creating a standalone proxy ARP for it.

## 5.3 Star-shaped Topologies

Most real world VPN topologies comprise a headquarters structure, which means many VPN tunnels terminate on one VPN server. Traffic between outposts is typically routed via the headquarters, thus reducing the number of tunnels, which have to be managed.

**Fig. 5-47** Star-shaped topology with one HQ and two outposts


In the star-shaped topology depicted in figure 5-47, a VPN connection can be established from 10.0.22.0/8 to 10.0.21.0/8 without the need to configure a tunnel between VPN servers 2 and 3. The table below illustrates the relationship between Local and Partner Networks:

**Table 5-12** Relationship between Local and Partner networks

Tunnel	VPN server	Local network	Partner network
Tunnel 1 - 2	Server 1	10.0.0.0/24	10.0.21.0/8
	Server 2	10.0.21.0/8	10.0.0.0/24
Tunnel 1 - 3	Server 1	10.0.0.0/24	10.0.22.0/8
	Server 3	10.0.22.0/8	10.0.0.0/24

Redirection of traffic for VPN networks to the VPN server engine is usually handled through a policy routing table, which the VPN server introduces. This policy routing table will not work properly, if the local network is part of the partner network, as it is in the example shown in figure 5-47. Traffic originating from the local network itself would incorrectly be rerouted into the VPN engine. This condition can be circumvented by introducing a throw route, which explicitly excludes the local network from the policy routing table.

## 5.4 Redundant VPN Tunnels

### 5.4.1 Overview

Redundant VPN tunnels contribute to maintaining un-interruptible connectivity between netfence gateways (for example, between HQ and branch). They are apt to minimising the threat hardware crashes and interruption of internet connections might pose to reliability and stability of VPN tunnels over the internet. In addition, they might eliminate the need for upgrading the existing infrastructure (frame relay, dedicated line) when this is suffering a load off the limits but upgrading is out of question due to high costs.

The phion netfence makes its decision, which kind of traffic to send through which tunnel, by the Service object that is utilised in a firewall rule. This way response critical traffic (like SSH, Telnet, Citrix, ...) can be directed to the tunnel via dedicated line/frame relay (usually having shorter delays), and bulk traffic (like SQL server replication, Lotus Notes replication, ...) can be directed to the internet tunnel.

However, the aim is that all traffic appears with the original Source IP address, regardless of the used tunnel and direction.



## 5.4.2 Configuring Redundant VPN Tunnels

Fig. 5-48 Configuring redundant VPN tunnels - example environment

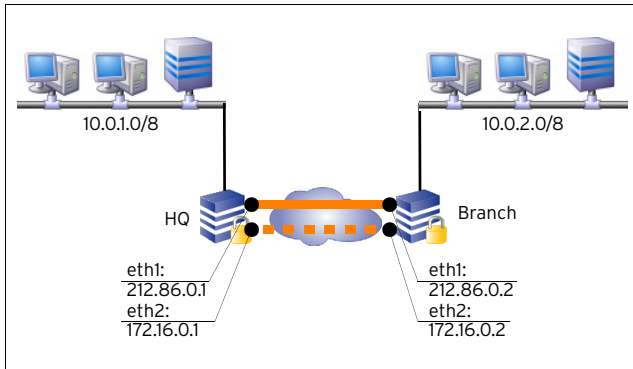


Figure 5-48 illustrates a redundant VPN tunnel setup with two links on each side of the tunnel. This results in four ways to build up the tunnel enveloping connection.

The algorithm determining the succession of retries works as follows:

- First local IP to first peer IP
- First local IP to second peer IP
- Second local IP to first peer IP
- Second local IP to second peer IP

When establishment of the preferred tunnel enveloping connection fails, no measure can be taken automatically to rebuild it. The tunnel has to be terminated manually. It will then immediately be rebuilt following the described algorithm.

The example setup depicted in figure 5-48 relies upon the following settings.

Table 5-13 Redundant VPN tunnel - Example

Tunnel 1 - 2	Peer IP address	Local Bind IP address
HQ	212.86.0.2 172.16.0.2	212.86.0.1 172.16.0.1
Branch	212.86.0.1 172.16.0.1	212.86.0.2 172.16.0.2

### Note:

It is assumed that a VPN service has been introduced on both, HQ and Branch.

### Step 1 Creating a new Firewall to Firewall tunnel

To configure the example shown above, enter the VPN tunnel configuration (through **Config** > **Box** > **Virtual Servers** > <servername> > **Assigned Services** > <servicename> (**vpnserver**) > **Site to Site** > **TINA Tunnels** tab).

Lock the configuration dialogue and select **New TINA tunnel ...** from the context menu.

### Step 2 Configuring the tunnels

Configure the tunnels as described in 2.7 Configuring VPN Tunnel Settings, page 220.

The following values have to be entered for the example setup:

Table 5-14 Redundant VPN tunnel - Example parameter settings

Parameter	HQ	Branch
<b>Tunnel Direction</b>	passive	active
<b>Peer IP</b>	172.16.0.2, 212.86.0.2	172.16.0.1, 212.86.0.1
<b>Tunnel IP</b>	172.16.0.1, 212.86.0.1	172.16.0.2, 212.86.0.2
<b>Partner Network</b>	10.0.2.0/8	10.0.1.0/8
<b>Local Network</b>	10.0.1.0/8	10.0.2.0/8

### Step 3 Configuring the routing

The default routes for establishing the VPN tunnels are configured in the **Section Main Routing Table (Configuration Service - 2.2.5 Network, page 61)**.

The following values have to be entered for the example setup:

Table 5-15 Redundant VPN tunnel - Direct Routes for VPN server 1

Parameter	1	2
<b>Target Network Address</b>	212.86.0.0/8	172.16.0.0/8
<b>Type</b>	direct_route	direct_route
<b>Interfacename</b>	eth1	eth2

Table 5-16 Redundant VPN tunnel - Direct Routes for VPN server 2

Parameter	1	2
<b>Target Network Address</b>	212.86.0.0/8	172.16.0.0/8
<b>Type</b>	direct_route	direct_route
<b>Interfacename</b>	eth1	eth2

As soon as one of the VPN tunnels has been established successfully, the network routes needed for communication through the tunnel are introduced by the system itself. These routes are displayed in the **ROUTES** section of **Control** > **Network** tab.

### Note:

In former versions of netfence gateway, redundant VPN tunnels with intermediate networks were needed for traffic intelligence configuration. This configuration method has been replaced in netfence 3.4. Firewall Connection Objects may now be equipped with settings defining Traffic Intelligence (TI) behaviour in the **VPN Traffic Intelligence (TI) Settings** section (see 2.7.1.2 Traffic Intelligence (TI), page 223). It is recommended to use this new method. Already existing redundant tunnel configurations will remain fully functional though and do not necessarily have to be replaced.

## 6. Configuring the Personal Firewall

### 6.1 General

The Personal Firewall Configuration determines the behaviour of the entegra VPN client's Personal Firewall when connected via VPN. netfence gateway 4.2 supports netfence entegra VPN client R8 and netfence entegra clients, as well as, entegra VPN client versions R6/R7.

**Note:**

For further information see the appropriate documentation **netfence entegra** (on your Application & Documentation CD-ROM).

## 7. entegra VPN client

### 7.1 Installation & Configuration

**Note:**

For further information see the appropriate documentation **netfence entegra** (on your Application & Documentation CD-ROM).

### 7.2 Troubleshooting

If you are facing problems with your entegra VPN client in a MS Windows environment, it might be a good idea to take a look at the Windows event viewer. All problems the VPN client is facing are logged there.

You can find the event viewer under:

***Start > Control Panel > Administrative Tools > Event Viewer***



# Mail Gateway

<b>1.</b>	<b>Overview</b>	
1.1	General .....	245
<b>2.</b>	<b>Installation</b>	
2.1	Procedure .....	245
<b>3.</b>	<b>Configuration</b>	
3.1	Service Properties .....	245
3.2	MailGW Settings .....	246
3.2.1	Basic Setup .....	246
3.2.2	Extended Domain Setup .....	247
3.2.3	POP3 Setup .....	249
3.2.4	Advanced Setup .....	250
3.2.5	Content Adaptions .....	253
3.2.6	Limits .....	255
3.2.7	Reporting .....	256
<b>4.</b>	<b>Spam Filtering</b>	
4.1	Theory .....	257
4.2	Configuration .....	258
4.2.1	Configuring the Spam Filter Client .....	258
4.2.2	Configuring the Spam Filter Server .....	259
4.2.3	Configuring the Training .....	261
4.2.4	Archiving and Updating .....	262
<b>5.</b>	<b>Mail Gateway Operation</b>	
5.1	MailGW Operation via GUI .....	263
5.2	General Characteristics of the Graphical Interface .....	263
5.2.1	Filters .....	263
5.2.2	Title Bar(s) .....	263
5.2.3	Context Menu Entries .....	263
5.3	Mail Queue Tab .....	263
5.3.1	Context Menu Entries .....	264
5.4	Access Tab .....	265
5.4.1	Context Menu Entries .....	265
5.5	Spam Tab .....	265
5.6	Processes Tab .....	266
5.6.1	Context Menu Entries .....	266
5.7	Attachments Tab .....	266
5.7.1	Context Menu Entries .....	267
5.8	Grey Listing Tab .....	267
5.8.1	Grey List .....	267
5.8.2	White List .....	268
5.8.3	Context Menu Entries .....	268
5.9	Logs, Statistics, Events .....	268
5.9.1	Logs .....	268
5.9.2	Statistics .....	268
5.9.3	Events .....	269

## **6. E-mail Synchronisation after HA Handover**

6.1	Automatic Synchronisation .....	269
6.2	Manual Synchronisation .....	269



# 1. Overview

## 1.1 General

With this service you can set up a powerful and secure mail gateway according to the SMTP (Simple Mail Transfer Protocol), RFC 2821.

**Note:**

For further details on this protocol see [www.ietf.org/rfc/rfc2821.txt](http://www.ietf.org/rfc/rfc2821.txt).

The phion netfence mail gateway service is, of course, completely maintainable via the management console phion.a. The service provides several features such as mail traffic control, spam filtering, statistics, event notification, and many more. The installation, configuration, and operation of this service is described in the following.

# 2. Installation

## 2.1 Procedure

To install the netfence mail gateway service you already need to have installed a server on your box.

Choose **Create Service ...** in the context menu of the corresponding server and select a name for this service (for example mailgw).

Configure the service definition settings (**Service Name**, **Description**, **Software Module**) of the mail gateway service in the following window.

Select **Mail-Gateway** as software module. Click **OK** to create the service. Now you can activate the changes by clicking **Activate**, and your newly installed mail gateway service is ready for configuration.

The mail gateway service generates three log files, which can be viewed in the **Logs** GUI (**Log Viewer**, page 289) of the graphical administration tool phion.a:

➤ **servicename**

This file contains the general logging data of the mail gateway service.

➤ **pop3**



This file belongs to the POP3 scanner and is only generated when POP3 scanning is set to enabled (Use POP3, page 249).

➤ **qspool**


This file records transactions processed between the configuration and monitoring areas of the mail gateway service and the graphical administration tool phion.a.

# 3. Configuration

The config tree of your box provides all configuration options for your mail gateway service and contains the following entries (listed according to their sequence of usage):

-  Service Properties
-  MailGW Settings, Page 246

## 3.1 Service Properties

To enter the configuration, select the  **Service Properties** entry in the config tree.


**General-** section **Service Definition**.

The fields **Service Name** and **Software Module** are read-only fields displaying the settings made when the service was created.

**Note:**

Due to software module **Mail-Gateway** the fields **Bind Type** and **Explicit Bind IPs** are not available.

**Note:**


If there is only one (or even no) bind IP configured in your server configuration, an error message **Cannot bind to IP ...** will be displayed in  **Logs** (see 5.9 Logs, Statistics, Events, page 268).

It is strongly recommended that your official IP addresses are reverse DNS resolvable. You might otherwise experience problems concerning your mail gateway. For example, other mail servers might deny communicating with it.

### Statistics and Notification.

These configuration options in the service configuration window do not have any effect on the actual behaviour. Statistics and Event settings of the mail gateway are configured in the MailGW settings (see 3.2.7 Reporting, page 256).

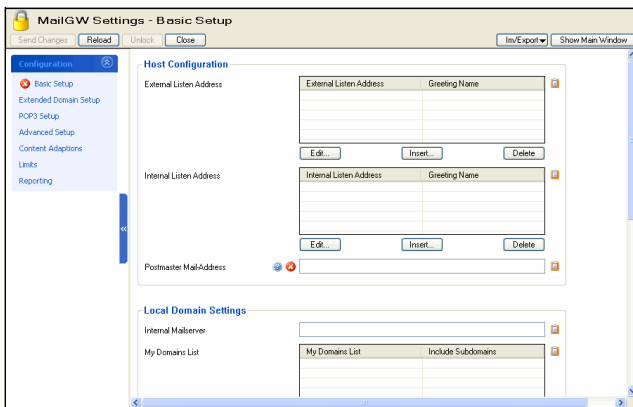
## 3.2 MailGW Settings

To enter the configuration, select the  **MailGW Settings** entry in the config tree.

The **MailGW Settings** configuration window is divided into two organisational areas:

- a **navigation bar** on the left side and
- the **configuration area** in the main window.

Fig. 6-1 MailGW Settings configuration area



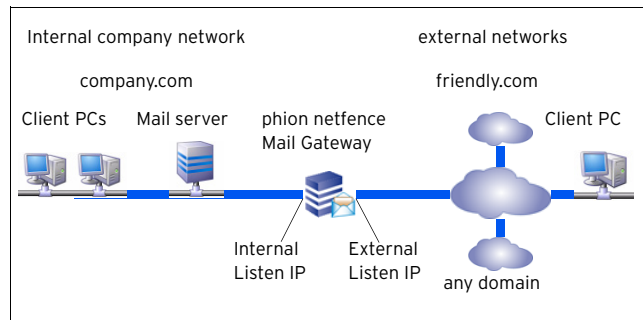
The following organisational segments are made available through the navigation bar:

Table 6-1 Items of the Navigations Bar's main element "Configuration"

View	Comment	described on
<b>Basic Setup</b>	For configuration of general settings of the Mail Gateway.	page 246
<b>Extended Domain Setup</b>	For settings applying to specific mail domains. This section is deactivated by default. If activated, <b>Local Domain Settings</b> in the <b>Basic Setup</b> are overwritten.	page 247
<b>POP3 Setup</b>	For handling of POP3 protocol processing.	page 249
<b>Advanced Setup</b>	For relaying, specific operational, and expert settings.	page 250
<b>Content Adaptions</b>	For the definition of mail specific content filters.	page 253
<b>Limits</b>	For the definition of mail processing limits.	page 255
<b>Reporting</b>	For reporting and eventing settings bound to e-mail traffic.	page 256

### 3.2.1 Basic Setup

Fig. 6-2 Mail gateway positioning in a network



#### Section Host Configuration

A mail gateway's fundamental configuration part are its Listen IP addresses. Listen IP addresses are addresses the server listens to on the standard SMTP port 25. A mail gateway operating in both directions has to listen to two IPs at least. The **internal** listen IP usually connects your LAN clients. The **external** listen IP connects your LAN to a foreign network.

For the following reasons it is essential to distinguish between these two listening IP types:

- The mail gateway determines the transportation direction by the e-mail's incoming IP address. Mail rules are only interpretable when internal and external listening IPs are configured properly (see Section Local Domain Settings, page 247 and Section Extended Domain Setup, page 247).
- Differentiation between inbound and outbound mail traffic in statistics collection is determined by the listening IP type.

If you are operating a mail server in your internal LAN, the mail gateway's internal listening IP address can be specified as mail relaying address. If a dedicated mail server does not exist, clients may specify the gateway's internal listening IP address as **outgoing SMTP server address** in the configuration of their e-mail client programs.

A listen IP is characterised by the following detail parameters:

List 6-1 MailGW Settings - Basic Setup - section Host Configuration

Parameter	Description
<b>External / Internal Listen Address</b>	<b>Listen Address</b> Insert the respective external and internal listening IP addresses (IPv4) here. Either choose the <b>First-</b> or <b>Second-</b> (Server) <b>IP</b> from the pull-down menu, or select the checkbox <b>Other</b> to specify another IP address.  <b>Note:</b> Listen IP addresses must be part of the server network configuration as well. If you choose option <b>Other</b> , do not forget to configure the inserted address(es) as server address(es) ( <b>Configuration Service - 3. Configuring a New Server</b> , page 94).
	<b>Greeting Name</b> This is the SMTP "helo / ehlo" greeting name which is sent after the SMTP connection to a mail server has been established (see <a href="http://www.ietf.org/rfc/rfc2821.txt">www.ietf.org/rfc/rfc2821.txt</a> ). This field can take letters from the Latin alphabet excluding special characters, ciphers, ".", "-", and "_".
<b>Postmaster Mail-Address</b>	Enter the e-mail address of the postmaster in this field. If an e-mail to the postmaster is sent, it will be re-written to the herein specified e-mail address.

### Section Local Domain Settings

Use this section to provide the mail gateway with information about trust relationships in your internal network, such as the mail server it should forward incoming mail to, and specification of local domains for which it should process mail traffic.

List 6-2 MailGW Settings - Basic Setup - section Local Domain Settings

Parameter	Description	
<b>Internal Mail Server</b>	Specify your internal mail server in this field. The mail gateway will redirect incoming mail to this server.	
<b>My Domains List</b>	Domains defined as <b>My Domains</b> are treated as trusted internal domains by the mail gateway. It is vital to specify trusted domains, as the mail gateway will only accept mail relaying for these domains on its internal listening address (see External / Internal Listen Address).  <b>Note:</b> The mail gateway will redirect incoming mail to the specified <b>Internal Mail Server</b> (see above). If you require another delivery policy setting, consider configuring your mail gateway through the <b>Extended Domain Setup</b> configuration options instead (see below).  <b>Note:</b> Security restrictions applying to <b>My Domains</b> are identical to the formerly known <b>Protection Profile</b> internal (see Protection Profile, page 248). If higher protection from fake e-mail addresses is required, consider configuring your mail gateway through the <b>Extended Domain Setup</b> configuration options instead (see below).	
	<b>My Domains List</b>	Enter the name of the internal trusted domain in this place (for example, phion.com). Wildcards may be used as supplement for the .tld ending to include multiple domains (for example, phion.*). Keep in mind, though, that a wildcard placed at the end of the domain name involves a potential security risk, as the top level domain might be interpreted as sub-domain (for example, phion.anyname.net). Consider creating one entry per domain instead.
	<b>Include Subdomains</b>	Set to <b>yes</b> , if subdomains of the specified domain should be treated as trusted mail domains as well (default: <b>no</b> ).

### Section Global Domain Parameters

List 6-3 MailGW Settings - Basic Setup - section Global Domain Parameters

Parameter	Description
<b>Default Recipient DB</b>	This parameter holds the relative path and <b>Default Recipient DB</b> name of the default database for recipient verification (MailGW Settings - section Extended Domain Setup - Domains, page 248). Please see Recipient DB, page 249 for detailed information on the correct use of this parameter.  <b>Note:</b> If parameters <b>Default Recipient DB</b> and <b>Default Recipients Lookup</b> are in use at the same time, the recipient email address has to match both databases.
<b>Default Recipients</b>	This parameter allows importing recipients into the <b>Default Recipient DB</b> specified in the field above. Please see <b>Recipients</b> , page 249 for detailed information on the correct use of this parameter.
<b>Default Recipients Lookup</b>	Select one of the phibs authentication schemes in the combo box to enable an online mail recipient lookup in a meta directory just in time when the mail arrives. Only authentication schemes of type MSAD or LDAP are allowed as recipient lookup scheme.  <b>Note:</b> The recipients email address is checked against the meta directory attribute named <b>mail</b> .  <b>Note:</b> If parameters <b>Default Recipient DB</b> and <b>Default Recipients Lookup</b> are in use at the same time, the recipient email address has to match both databases.  <b>Note:</b> When this parameter is set to <b>MSAD</b> or <b>LDAP</b> the list <b>Recipients Lookup req. Groups</b> may be filled. If filled, the authentication scheme config (Group Attribute) has to be set accordingly.
<b>Recipients Lookup req. Groups</b>	Define here group patterns which the recipient has to match that the recipients email address will be accepted.
<b>Allow Relaying from</b>	E-mails are only accepted for relaying on the internal listen address if they have been forwarded by one of the hosts specified here.

## 3.2.2 Extended Domain Setup

A freshly installed version of netfence 4.2 aims at simplest possible configuration and expects domain specific configuration in the **Section Local Domain Settings** within the Basic Setup (see 3.2.1 Basic Setup). Thus, the Extended Domain Setup is disabled (set to **no**) by default. Enabling it deactivates and overwrites settings configured in the **Section Local Domain Settings**.

**Note:**  
The Extended Domain Setup section is utilised when migrating Mail Gateway settings from netfence gateway version 3.2.

### Section Extended Domain Setup

This is a complex and powerful rule feature. It protects your mail gateway from fake e-mail sender domains which could abuse it for relaying spam mail.

List 6-4 MailGW Settings - section Extended Domain Setup

Parameter	Description
<b>Enable Extended Domain Setup</b>	Select <b>Yes</b> to enable.
<b>Domains</b>	see list 6-5
<b>Default Internal MX</b>	You can specify a default DNS-resolvable mail exchange in this field. Incoming mail will be redirected to this default MX. Usable for load balancing via DNS Round Robin.

List 6-4 MailGW Settings - section Extended Domain Setup

Parameter	Description
<b>Default Internal Mail Server</b>	You can specify one or more default internal mail servers in this field. Incoming mail will be redirected to this default mail server. If you specify more mail servers, the mail gateway will try them subsequently until delivery is successful (for example, if the first default mail server is unreachable, ...). Enter the IP address and select <b>Insert ...</b> and to add it to the list of default mail servers.

### Domains:

Select **Insert** to insert a new trusted domain and enter the domain name into the **Name** field.

The following parameters are available for configuration:

List 6-5 MailGW Settings - section Extended Domain Setup - Domains

Parameter	Description
<b>Additional Domain Pattern</b>	If your trusted domain has additional patterns (for example several top level domains such as .com or .net ...) you can add the additional pattern to the list. For the additional pattern, it is also possible to enter wild cards such as * or ? (like sample.*).
<b>Protection Profile</b>	<p>Protection profiles determine a mail domain's trust scope. Domains impersonating the highest trust level may only be forwarded by a gateway's internal listen IP, domains with the lowest trust level may be used to communicate outside the company LAN only.</p> <p>Have a look at figure 6-2, page 246 to understand the impacts of protection profile configuration. The following trusted domain definitions apply:</p> <ul style="list-style-type: none"> <li>➤ <b>strictly_internal</b> E-mail senders using a domain defined as strictly internal are only accepted from within the company network at the mail gateway's internal listen IP. This configuration offers the highest protection level against fake e-mail addresses, as it is not possible to forward e-mails through any external, Internet-accessible mail relay.</li> <li>➤ <b>internal</b> E-mail senders using a domain defined as internal are accepted from within the company network at the mail gateway's internal listen IP and as well from outside the company network at the mail gateway's external listen IP. This configuration is of interest for mobile workers wishing to send e-mails with official company addresses when they are connected to the Internet via any ISP.</li> <li>➤ <b>foreign</b> E-mail senders using a domain defined as foreign are accepted at both listening interfaces. Foreign domains can be defined if some of your clients want to use an external mail account (like a web mail account) company-wide and from the Internet. As foreign domains are accepted as senders and recipients on both listening interfaces on the mail gateway, it makes sense to specify allowed clients explicitly (parameter <b>Accept Policy</b> &gt; <b>Explicit ACL</b>), so the foreign domain setting is only valid for these clients and not for the whole internal client network.</li> <li>➤ <b>strictly_foreign</b> E-mail senders using a domain defined as strictly foreign are only allowed at the mail gateway's external listening interface.</li> </ul>

#### Rules controlling mail traffic

	strictly_internal	internal	foreign	strictly_foreign
<b>Allow as sender on internal</b>	pass	pass	pass	DENY
<b>Allow as sender on external</b>	DENY	pass	pass	pass
<b>Allow as recipient on internal</b>	pass	pass	pass	pass
<b>Allow as recipient on external</b>	pass	pass	DENY	DENY

List 6-5 MailGW Settings - section Extended Domain Setup - Domains

Parameter	Description
<b>Delivery Policy</b>	<p>This parameter determines the handling of <b>incoming e-mails</b> addressed to the specified recipient domain. The following setting options define the mail gateway's e-mail forwarding mechanism:</p> <ul style="list-style-type: none"> <li>➤ <b>MX</b> (default) The mail gateway tries to resolve a DNS MX (mail exchange) record for the specific domain.</li> <li>➤ <b>Default_Internal</b> The mail gateway redirects incoming mail for a trusted domain to the respective default mail server as outlined on page 248 (<b>Default Internal Mail Server</b>).</li> <li>➤ <b>Default_MX</b> The mail gateway redirects incoming mail for a trusted domain to a MX-resolvable domain as outlined on page 247 (<b>Default Internal MX</b>).</li> <li>➤ <b>Explicit_Peer_IP</b> Activates the field <b>Delivery IPs</b> where one or more IP addresses can be entered (parameter <b>Delivery IPs</b>, see below). The mail gateway redirects matching incoming mail to the specified IP address.</li> <li>➤ <b>Explicit_MX_Domain</b> The mail gateway redirects responsibility for e-mail forwarding to another MX-resolvable domain. Enter the MX domain into the <b>Delivery IPs</b> field below. E-mail distribution to the final recipients will then be handled by the other domain's mail servers. This option can be used when multiple internal mail servers are in use.</li> </ul>
<b>Delivery IPs</b>	This field only expects input if <b>Delivery Policy</b> has been set to <b>Explicit_Peer_IP</b> or <b>Explicit_MX_Domain</b> . If having done so specify delivery IP address(es) or MX domain(s) explicitly in this place.
<b>Local Deliver IP</b>	This parameter should be used when having multiple Listen IPs because it allows selecting one of the available IPs as binding one.
<b>Allow Relaying from</b>	<p>This setting specifies which peers are allowed to use the specified domain as sender domains. There are three different accept policies:</p> <ul style="list-style-type: none"> <li>➤ <b>Any_Peer</b> The specified domain can be used by any peer</li> <li>➤ <b>Basic_Relaying_Setup</b> The specified domain can only be used by peers specified in parameter <b>Allow Relaying from</b>.</li> <li>➤ <b>Explicit_ACL</b> Activates the field <b>ACL</b> where ACL IPs can be entered. Specified domains can only be used by these peers.</li> </ul>
<b>ACL</b>	Explicit access list (allowed peer IPs)
<b>Recipient Lookup</b>	<p>This parameter allows verifying each mail recipient in a database. If the recipient cannot be found in the database the mail is dropped. The following options are available:</p> <ul style="list-style-type: none"> <li>➤ <b>Disabled</b> (default) Deactivates the parameter, that means no verification is carried out.</li> <li>➤ <b>Default_DB</b> Uses the database configured in parameter <b>Default Recipient DB</b> (see Section Global Domain Parameters, page 247).</li> <li>➤ <b>Explicit</b> In case the sum of queried users in the <b>Default_DB</b> causes performance problems, it is sensible to specify an individual Recipient DB for each domain.</li> </ul>

List 6-5 MailGW Settings - section Extended Domain Setup - Domains

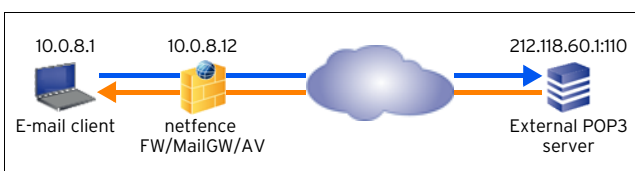
Parameter	Description
<b>Recipient DB</b>	<p>This field is only available when the parameter <b>Recipient Lookup</b> is set to <b>Explicit</b>. It holds the relative path and <b>Recipient DB</b> name of the explicit database for recipient verification.</p> <p>A Recipient DB is always expected in <code>/var/phion/spool/mgw/*server*_*service*/</code> or a folder below this one. You may specify an already existing database through this field. If the database does not yet exist, it will be created.</p> <p>For a database that has been or is expected to be created in <code>/var/phion/spool/mgw/*server*_*service*/</code> enter <code>my_recipient.db</code> into this field. For a database that has been or is expected to be created in <code>/var/phion/spool/mgw/*server*_*service*/myfolder/</code> enter <code>myfolder/my_recipient.db</code> into this field.</p> <p><b>Note:</b> If you wish to create a database in a subfolder of <code>/var/phion/spool/mgw/*server*_*service*/</code> the subfolder already has to exist, as it will not be created by phion.a automatically.</p> <p><b>Attention:</b> If specified, the mail gateway is always going to query the recipient DB before processing an e-mail. Thus, make sure to immediately configure the contents of the Recipients DB after creation, as an empty Recipient DB will block all e-mail traffic.</p>
<b>Recipients</b>	<p>This parameter allows importing recipients into the Recipient DB specified in the field above. The import routine takes a text file with e-mail addresses arranged one per line.</p> <p><b>Attention:</b> Only use the import routine when you have specified an existing database in the parameter <b>Recipient DB</b> above.</p> <p><b>Attention:</b> Do not use the import routine to update the Recipient DB with solitary users, as the content of the Recipient DB is deleted prior to update.</p> <p><b>Note:</b> If you need to update the Recipient DB at regular intervals, do so by using an always up-to-date text file containing the total amount of used e-mail addresses.</p> <p><b>Attention:</b> The content of the Recipient DB is not saved to the <code>.par</code> file when creating a backup of the box configuration. Thus, you should always keep the contents of your Recipient DB in a safe place in case restoring it becomes necessary.</p>
<b>Default Recipients Lookup</b>	<p>Phips scheme for lookup of a recipients e-mail address in a meta-directory.</p> <p><b>Note:</b> Only MS-Active-Directory and LDAP schemes may be used.</p>
<b>Recipients Lookup req. Groups</b>	<p>Define Meta-Directory group patterns to restrict allowed e-mail addresses. Only persons which are assigned at least one of the here defined groups are allowed recipients. Patterns are allowed.</p>

### 3.2.3 POP3 Setup

E-mail clients use the Post Office Protocol version 3 (POP3) to retrieve mail from a remote server over a TCP/IP connection. Especially in small companies, which do not operate an internal mail server, mail traffic is sometimes limited to fetching and forwarding of e-mails to an externally hosted POP3 mail server.

For enhanced measure of security when collecting e-mails from this mail server over the Internet the netfence may be configured to scan data streams processed over POP3 for viruses and spam.

Fig. 6-3 POP3 scanning example setup



**Note:**

Do not mistake this configuration section as POP3 mail server setup. The configuration options in this place are limited to scanning of traffic between an e-mail client and an external POP3 server.

The following conditions have to be met to enable scanned POP3 data streams between e-mail client and POP3 server:

- **Firewall configuration**  
A rule has to be configured in the firewall settings allowing communication on the POP3 port (default: 110) (**Firewall - 2.2 Rule Set Configuration**, page 132).
- **Antivirus settings**  
the AVIRA AntiVir virus scanner service has to be installed (**Anti-Virus**, page 367). The use of an external virus scanner is not possible.
- **Mail scanning settings**  
Mail Scanning (**Anti-Virus - 2.4.2 Mail Gateway Integration**, page 371) has to be activated. Settings (**Anti-Virus**, page 367) apply to POP3 scanning.
- **Spam Filter settings**  
If SPAM checking is desired the Spam filter service has to be installed (4. Spam Filtering, page 257).
- **E-mail client configuration**  
User specific login data has to be entered into the e-mail client that collects mail from the POP3 server. This login data has to be adapted so that the e-mail client addresses the netfence gateway instead of the POP3 server directly. According to the example scenario in figure 6-3, the data has to be entered in the following way:

Table 6-2 E-mail client configuration

Field	Value	Example
<b>Username</b>	username#POP3serverIP:port	phion#212.118.60.1:110
<b>Password</b>	POP3 account password	*****
<b>POP3 server</b>	Listening IP of the POP3 scanning service (see <b>Listen on</b> , page 249)	10.0.8.12

The following configuration options are available for POP3 scanning:

List 6-6 MailGW Settings - Pop3 Setup - section POP3 Setup

Parameter	Description
<b>Use POP3</b>	Set to <b>yes</b> (default: <b>no</b> ) to enable scanning of data processed over POP3. Activating this option automatically enables virus scanning.
<b>Listen on</b>	<p>The mail gateway listens for POP3 requests on the IP address(es) specified here. Either choose the First- or Second- (Server) IP from the pull-down menu, or select the checkbox <b>Other</b> to specify another IP address. Multiple addresses may be entered in a comma separated list.</p> <p><b>Note:</b> Listen IP addresses must be part of the server network configuration as well. If you choose option Other, do not forget to configure the inserted address(es) as server address(es) (<b>Configuration Service - 3. Configuring a New Server</b>, page 94).</p>
<b>Maximum Children</b>	This is the maximum number of concurrent connections the mail gateway accepts for POP3 sessions (default: <b>10</b> ). Connection attempts exceeding this value will be dropped.



List 6-6 MailGW Settings - Pop3 Setup - section POP3 Setup

Parameter	Description
<b>Timeout (s)</b>	This is the time span after which connection between e-mail client and mail gateway times out. This value is of importance because too long processing times caused by communication or connectivity problems between mail gateway and POP3 server can lead to connection loss between mail gateway and e-mail client. You may leave the default setting at <b>30</b> seconds if you are not experiencing any problems.
<b>Check Spam</b>	Set to <b>yes</b> (default: <b>no</b> ) to activate spam checking of e-mails retrieved via POP3. <b>Note:</b> In order to perform a spam check the Spam filter service has to be installed (4. Spam Filtering, page 257).
<b>Template</b>	When the virus scanner finds a virus, it immediately drops the e-mail and attempts forwarding an informational message to the e-mail's recipient instead of the original e-mail. Use the <b>Template</b> field to define a global template for these notifications. Variable parameters such as e-mail address, virus information, mail subject ... are inserted into the template when the notification is generated. Valid variable parameters are: <ul style="list-style-type: none"> <li>➤ <b>%USERNAME %</b> - name of the user</li> <li>➤ <b>%VIRUSNAME %</b> - virus information</li> <li>➤ <b>%MAILFROM %</b> - sender e-mail address</li> <li>➤ <b>%MAILTO %</b> - recipient e-mail address</li> <li>➤ <b>%MAILDATE %</b> - date of the e-mail</li> <li>➤ <b>%SUBJECT %</b> - mail subject</li> </ul>
<b>Subject</b>	This string is inserted into the alert e-mail's subject header (default value: <b>[VIRUS found]</b> ).
<b>Delete Infected Mails</b>	Virus infected e-mails are immediately deleted and not stored on the netfence gateway when this option is set to <b>yes</b> (default: <b>no</b> ). E-mails are saved to the path <code>/var/phion/run/mailgw/&lt;servername&gt;_&lt;servername&gt;/root/virus-rejected</code> .
<b>Use HTML Tag Removal</b>	Set to <b>yes</b> (default: <b>no</b> ) to enable HTML tag removal. For a short description of HTML tag removal see Section HTML Tag Removal (page 255).

### 3.2.4 Advanced Setup

The following parameters define the mail gateway's general behaviour:

List 6-7 MailGW Settings - Advanced Setup - section Operational Settings

Parameter	Description
<b>Mail Transfer Agents (MTAs)</b>	Mail transfer agents are service processes that deliver mails received from a client to other mail servers (see 5.1 MailGW Operation via GUI, page 263). You can specify the maximum number of MTAs here (default: <b>5</b> ) <b>Attention:</b> This number must not be 0). MTA processes are only started when the mail gateway system needs them for mail delivery. They are after delivery has succeeded.
<b>MTAs for Urgent Mail</b>	This parameter defines the number of MTAs that are reserved for mail classified as urgent (default: <b>1</b> ). The definition what kind of mails have the scheduling priority urgent is made within the Section Expert Settings (use with care) (page 251).
<b>Admin Connections</b>	This is the maximum number of GUI connections allowed to the box where the mail gateway service is installed (default: <b>5</b> ).
<b>DNS Query</b>	The local box firewall blocks DNS reply packets from slow DNS servers because the mail gateway already received an answer from a fast DNS server (when selecting option <b>parallel</b> , default). The option <b>sequential</b> causes that DNS servers are queried one after the other.

List 6-7 MailGW Settings - Advanced Setup - section Operational Settings

Parameter	Description
<b>Spool Queue Sync</b>	This parameter activates/deactivates the synchronisation of mails between a HA pair. When activated, the active mail gateway sends mail-bundles to the passive mail gateway for synchronisation each 10 sec. <b>Note:</b> Enabling this parameter requires a restart of the mail gateway service due to the HA specific startup procedure. Disabling works without restart. <b>Attention:</b> Having this option activated may cause extensive load during synchronisation.
<b>DSN Mails in MIME-Format</b>	Select <b>yes</b> to send DSN messages in MIME format, according to RFC1891 (SMTP Service Extension for Delivery Status Notifications; for details see <a href="http://www.ietf.org/rfc/rfc1891.txt">www.ietf.org/rfc/rfc1891.txt</a> ).
<b>MTA Retry Sequence</b>	Due to a variety of reasons (for example a target server is unreachable), an e-mail might possibly not be delivered at once. If this is the case, the mail gateway service starts a further delivery attempt after a certain period specified through this field. Multiple retry attempts can be entered in a space separated list. The following characters may be used: <ul style="list-style-type: none"> <li>➤ Digits</li> <li>➤ <b>m</b> = minute(s)</li> <li>➤ <b>h</b> = hour(s)</li> <li>➤ <b>d</b> = day(s)</li> </ul> Adding the character <b>w</b> to a time parameter in the list causes generation of DSN ( <b>Delivery Status Notification</b> ) messages addressed to the original e-mail's sender. As long as further retry attempts still are to follow, a <b>delay</b> message is generated. The last message of the retry sequence is a <b>delivery failure</b> notification.  <i>Example messages for the MTA retry sequence: '1m 5m 10m 1hw 1dw':</i>  <i>Delay message generated after 1 hour:</i> Your Message to the following recipients <recipient@sample.com> (reason: [reason for delivery delay]) has been delayed. You do NOT have to resend your message!!! The mail server will keep trying to deliver your message and you will be notified if delivery is impossible. Received: from [IP] ([hostname]) by [mail gateway] id [JOB ID Number]; [Day Date Time] From: "Sender" <sender@sample.com> Subject: [Subject of mail message]  <i>Delivery failure notification generated after 1 day:</i> Your Message to the following recipients <recipient@sample.com> (reason: [reason for delivery failure]) - maximum retries reached - could not be delivered. Received: from [IP] ([hostname]) by [mail gateway] id [JOB ID Number]; [Day Date Time] From: "Sender" <sender@sample.com> Subject: [Subject of mail message]
<b>Priority Switch after (minutes)</b>	The phion netfence mail gateway schedules all mail jobs received from the clients (for more information on the scheduling mechanism see 5.1 MailGW Operation via GUI, page 263). This setting specifies the period of time (default: 60 minutes) after which the mail gateway automatically changes scheduling priority to the next higher level. <b>Note:</b> This setting has nothing to do with the priority flag you can set in your e-mail client software; this priority flag concerns the mail application only.

List 6-8 MailGW Settings - Advanced Setup - section Allowed Relaying

Parameter	Description
<b>Internal IP-Addresses</b>	These internal IP addresses are allowed to forward mail traffic. <b>Attention:</b> Use this parameter with great care as incorrect settings may cause security violation.



List 6-9 MailGW Settings - Advanced Setup - section Cloning and Archiving

Parameter	Description
	By means of the configuration options in the Cloning and Archiving section, e-mail addresses can be manipulated before a mail is forwarded to its recipient(s). E-mails can be duplicated ( <i>cloned</i> ) by inserting multiple recipients in a comma separated list into the recipient related rewrite field. They can thus be forwarded ( <i>archived</i> ) to an external e-mail archiving system. <b>Note:</b> Delivery classification options configured in the <b>MailGW Settings - section Extended Domain Setup - Domains List 6-5</b> (page 248) also apply to e-mail addresses that have been rewritten. For example, if the sending domain address of an e-mail, which has been accepted for delivery at the mail gateway's external listen address, is rewritten to a strictly internal sender domain, the mail will be discarded due to policy restrictions.
<b>Enable Cloning and Archiving</b>	Set to <b>yes</b> to activate Cloning and Archiving and click the <b>Set ...</b> button to open the following configuration window.
<b>Archiving Settings</b>	Sender as well as recipient addresses can be rewritten. Click the <b>Insert ...</b> button to add new rewriting patterns. Wildcards such as <b>*</b> or <b>?</b> may be used in the <b>Pattern</b> columns. <ul style="list-style-type: none"> <li>➤ <b>Sender/Recipient - Full Address Manipulation</b> manipulate full e-mail address</li> <li>➤ <b>Sender/Recipient - Local Part Manipulation</b> manipulate local part (string preceding '@')</li> <li>➤ <b>Sender/Recipient - Domain Manipulation</b> manipulate domain name (string following '@')</li> </ul>

Section **Expert Settings (use with care)**

**Attention:**  
Expert settings should be used with care. Do not use expert settings unless you exactly know what you are doing and/or have contacted phion Support.

By means of the configuration options that **Expert Settings** make available, rule settings may be added to the netfence mail gateway service manually. In the **Pre Settings** section rules are configurable that are considered before other mail gateway settings, in the **Post Settings** section rules are configurable that are considered after all other mail gateway settings have been processed. To enable configuration options, set **Enable Pre Settings** or **Enable Post Settings** respectively to **yes** and then click the corresponding **Edit** button to open the configuration dialogue.

Expert Settings can be added to all 5 levels of a SMTP mail transmission (refer to RFC 2821 for details):

Table 6-3 SMTP Levels

Level	Type	Description
1	Connect	This is the connection level of the mail gateway server (like that banned hosts rule will affect the connect level).
2	Helo	This is the SMTP greeting level (SMTP "helo" or "ehlo" command).
3	Sender	In this level the sender of a mail is announced (SMTP "mail from:" command, for example, banned sender rule will affect the sender level).
4	Recipient	The recipient of a mail is announced in this level (SMTP "rcpt to:" command; for example, banned recipient or re-write recipient rule will affect the recipient level).
5	Data	In the last level of a SMTP transmission the mail body (data) is transmitted, for example the subject is part of the mail body (banned subjects rule will therefore affect the data level).

**Abstract Rule Language**

Configuration of Expert Settings requires syntactical knowledge of the applicable abstract rule language.

**General syntax**

- // Comment line (comment lines are ignored by the abstract rule parser)
- Separate expressions with space (for example, a double-slash // must be followed by space)
- Quote string variable values ("string").
- Separate parameters with a comma sign ( , ).

**Variables**

Table 6-4 Variables used in the Expert Settings section

Variable	Type	Level	Description	Special value
result	integer	all	return code of rule parser	
peerip	string	connect (1)	IP address of peer (client)	
peername	string	connect (1)	hostname of peer (client)	
inbound	boolean	connect (1)	0=outbound; 1=inbound (that is mail reception on internal IP)	
helo	string	helo (2)	SMTP greeting name (ehlo/helo)	
from	string	sender (3)	sender e-mail address after re-writing	null
fromuser	string	sender (3)	sender e-mail address local part after re-writing	
fromdomain	string	sender (3)	sender e-mail address domain after re-writing	
to	string	rcpt (4)	recipient e-mail address after re-writing	postmaster
touser	string	rcpt (4)	recipient e-mail address after local part re-writing	
todomain	string	rcpt (4)	recipient e-mail address domain after re-writing	
orig_[...]	string	sender (3) rcpt (4)	adding <b>orig_</b> to e-mail address variable (for example <b>orig_fromdomain</b> ; reflects e-mail address before re-writing)	
subject	string	data (5)	subject of mail body	

**Operators**

Table 6-5 Operators used in the Expert Settings section

Operator	Description
=	Text Operator; Equality
<>	Text Operator; Inequality
" "	Numerical Operator
AND	Logical Operator
OR	Logical Operator

**Usage:**

<variable> <operator> <expression>

**Example:**

fromdomain <> "sample.com"

**IF statements**

Table 6-6 IF statements used in the Expert Settings section

Statement	Description
IF	Begin IF test block
ELSE	Begin ELSE block

**Table 6-6** IF statements used in the Expert Settings section

Statement	Description
ELSEIF	Begin ELSEIF block
ENDIF	END IF block
THEN	THEN statement for IF tests

**Usage:**

```
IF (<test-expression(s)>) THEN
<statement>;
ENDIF
```

**Example:**

```
IF (fromdomain = "sample.com") OR
(fromuser = "spammer") THEN
ACTION ("deny", "Banned Sender");
ENDIF
```

**ACTION**

This command is used to let the mail gateway service perform various actions.

**Table 6-7** Actions used in the Expert Settings section

Action	Level	Parameter	Description
ruledbug	all		view rule debug messages in logs
smtpdebug	all		view SMTP debug messages in logs
deliverdirect	>2	target IP address	when specified in level 3 it has an effect on the whole mail objects, else on current rcpt
Bind	>2	extern intern bind IP [inbound-flag]	when specified in level 3 it has an effect on the whole mail objects, else on current rcpt <ul style="list-style-type: none"> <li>• extern: use first configured external bind IP</li> <li>• intern: use first configured internal bind IP</li> <li>• specify an explicit bind IP [inbound-flag is either 0 (default, outbound) or 1 (inbound)]</li> </ul>
Quit	all		close connection
Deny	>2	description	deny mail delivery of current mail
Drop	4		drop current recipient
rewrite rewriteuser rewritedomain	>2	mailbox localparts rewritedomains	if specified in level 3 re-write sender (-part), else re-write current recipient (-part)
clone cloneuser clonedomain	4	list of mailboxes, local-parts or domains	clone current recipient (-part)
Priority	>2	priority	scheduling priority; allowed values: low, normal, high, urgent
Event	all	event-type, description	trigger an event allowed values: 0=info, 1=notice, 2=error description of event: will be displayed in <b>Events</b> if event triggered
None	all		do nothing

**Usage:**

```
ACTION ("<action>", "<parameter(s)>");
```

If there is no parameter required (this is the case when quit action is used), you need to enter the quotation marks anyway, like for example `ACTION ("quit", "");`.

**Example:**

```
ACTION ("rewrite", "test@sample.com");
```

**or**

```
ACTION ("event", "1, Event has been triggered!");
```

**RETURN**

The return command exits the current level function, so subsequent instructions will no longer be performed.

Usage: `RETURN ;`

**Note:**

Lines with ACTION and RETURN commands require a semicolon (;) at the end of the line; expressions with ACTION/RETURN command are space separated (this is also valid for the semicolon after the RETURN command as shown above).

**Examples for expert settings****Example 1**

Mail delivery from mail servers that send "spam" as greeting name should be denied. Insert the following rule language code into the **Helio** field of Pre or Post Settings:

```
IF (helo = "spam") THEN
ACTION ("quit", "");
RETURN;
ENDIF
```

**Example 2**

Priority of e-mails arriving from a specific address should be changed to "high". Insert the following rule language code into the **Sender** field of Pre or Post Settings:

```
IF (from = "boss@company.com") THEN
ACTION ("priority", "HIGH");
ENDIF
```

**Example 3**

E-mails arriving from a specific address should be cloned and distributed to multiple recipients. Insert the following rule language code into the **Recipient** field of Pre or Post Settings:

```
IF (from = "sender@company.com") THEN
ACTION ("clone", "rcp1@company.com,  
rcp2@company.com,rcp3@company.com");
ENDIF
```

**Example 4**

Spam e-mails should be redirected. The following rule language code can be entered in any expert pre settings. The following syntax applies:

```
ACTION ("redirect", "<program>,[<optional_params>]");
```

A corresponding configuration entry could read as follows:

```
ACTION ("redirect", "/opt/phion/bin/spam_redirect.sh");
```

The script itself that is required for e-mail redirection (spam\_redirect.sh in the example) could read as follows:

```
#!/bin/bash
# $1 ... path to mail files
# $2 ... spoolid
## this script redirects mails with "[SPAM]" within subject
# to an archive mail account
```

```
DSTMAILBOX=mailboxname
```

```
DSTDOMAIN=domainname
DSTIP=serverip
BODY_FILE=$1$2".body"
ENV_FILE=$1$2".env"
TMP_FILE="/tmp/"$2".env"
SUBJECT=`cat $BODY_FILE | formail -c -x subject | grep "[SPAM]" |
sed -e 's/.\*[SPAM\].*/[SPAM]/g`

if [ "$SUBJECT" = "[SPAM]" ]; then
# redirect to spam mail box
# 1. remove lines that start with "rcpt"
# 2. insert infos for delivery to spam archive
# (assumption: $DSTIP is an internalmailserver)
mv $ENV_FILE $TMP_FILE
cat $TMP_FILE | grep -v -e "rcpt" -e "recipient" -e "numrcpts" >
$ENV_FILE
echo "numrcpts 1" >> $ENV_FILE
echo "recipient" >> $ENV_FILE
echo "rcpt id 0" >> $ENV_FILE
echo "rcpt user $DSTMAILBOX" >> $ENV_FILE
echo "rcpt domain $DSTDOMAIN" >> $ENV_FILE
echo "rcpt status 0" >> $ENV_FILE
echo "rcpt deliverdirect $DSTIP" >> $ENV_FILE
echo "rcpt bindtype 1" >> $ENV_FILE
echo "rcpt bind intern" >> $ENV_FILE
rm -f $TMP_FILE
fi
echo "0"
```

**Note:**

The script has to be made executable. Enter `chmod 777 /opt/phion/bin/spam_redirect.sh` in this example)

### 3.2.5 Content Adaptions

#### Section *Spam Detection*

Through this section the spam filter client is configured. For detailed information about configuring see 4.2.1 Configuring the Spam Filter Client, page 258.

#### Section *Virus Protection*

This section is used for integrating the virus scanner into the mail gateway. See 2.4.2 Mail Gateway Integration, List 16-10 MailGWSettings - Virus Scanning - section Virus Protection, page 371 for a description of the available configuration parameters and integration into a mail gateway.

#### Section *Attachment Stripping*

This section allows configuring file attachments to be cut from e-mails before forwarding the e-mail to its recipient. Filters can be set by sender's and/or recipient's e-mail addresses and domains, and by file type.

To access the configuration dialogue, set **Enable Attachment Stripping** to **yes** (default: **no**) and then click the **Set** button to the right of the **Advanced Attachments**

**Options.** The following parameters define attachment stripping behaviour in detail:

**List 6-10** MailGW Settings - Content Filter - Attachment Stripping - section Advanced Attachment Options

Parameter	Description
<b>Cut Whitelists</b>	<b>Sender/Recipient Whitelist</b> E-mail addresses and domain patterns inserted into this list are excluded from Attachment Stripping execution. Senders and recipients may either be inserted with their full addresses or wildcards may be used (like user@phion.com, @phion.com, phion.com). The <b>Sender Whitelist</b> is processed before the <b>Recipient Whitelist</b> . An incoming e-mail will thus first be scanned for its sender. If the sender is in the whitelist, the e-mail will be forwarded untrimmed. If the sender is not in the whitelist, the e-mail will be scanned for its recipient(s). If the e-mail is addressed to multiple recipients, it will only be forwarded untrimmed, if all its recipients reside in the Recipient Whitelist. Attachments will otherwise be cut.
<b>MIME-Type</b>	This parameter determines to strip all attachments belonging to a specific MIME-Type. For MIME-Type specification, the following syntax applies (wildcards (*) are allowed): <i>MIME-Type/MIME-Subtype</i> (for example, <i>*/*, application/*, application/activemessage</i> ). For an authoritative listing of all MIME-Types, refer to <a href="http://www.iana.org/assignments/media-types/">http://www.iana.org/assignments/media-types/</a> . <b>Note:</b> If wildcards are applicable the <b>MIME-Type Exceptions</b> parameter below allows you to exclude specific subtypes from attachment stripping.
<b>MIME-Type Exceptions</b>	Specify MIME-Subtypes in this list that should be excluded from attachment stripping, in case the <b>MIME-Type</b> parameter above has been defined globally employing wildcards. For MIME-Subtype specification, the following syntax applies (wildcards (*) are allowed): <i>MIME-Type/MIME-Subtype</i> (for example <i>application/pdf, image/*</i> ).
<b>Automatically Detect MIME-Type</b>	Setting to <b>yes</b> (default) triggers use of the UNIX <b>file</b> command to detect a file's MIME-Type automatically. If set to <b>no</b> , the MIME-Type propagated by the sender's e-mail client applies for determination of attachment stripping conditions. It is recommended not to change the default setting.
<b>File Extension Filter</b>	Determines files with a specific ending to be stripped off e-mails. If the desired file type is not in the list, select checkbox <b>Other</b> and specify the ending explicitly.
<b>Message to Recipient</b>	Supply a message in this place informing the e-mail's recipient that file attachments have been cut from the original e-mail. This message is inserted into the e-mail before it is forwarded to the actual recipient.

#### Section *Grey Listing*

**Grey listing** is a feature allowing for reduction of unsolicited SPAM e-mail. Grey listing works by rejecting the first arrival of a new message and telling the remote site to try again. Grey listing relies upon correctly configured legitimate mail transfer agents, attempting at least one further delivery try. Non RFC conformant mail servers ignore error reports and do not try re-sending their mails. As spam is most frequently delivered through such servers, grey listing reduces acceptance of unwanted messages.

When a new message, comprising an unknown sender-recipient pair, arrives, the grey lister rejects mail acceptance, passes a rejection notice to the sending mail server and places the sender-recipient pair into its grey list. This list is visualised in 5.8 Grey Listing Tab, page 267. If the mail has been delivered by a legitimate MTA, it will be resent most likely. The second delivery attempt is accepted by the grey lister and the e-mail is delivered.

Two side effects of grey listing have to be taken into account:

- Depending on the sending MTAs configuration, the e-mail sender might be issued a report about the initial delivery failure.
- As e-mails are temporarily rejected, they experience a slight delivery delay.
- Wanted e-mails might not be delivered due to incorrectly configured MTAs on the sender's side. This misconfiguration may be corrected through the **White List Peers** and **Senders** parameters (see below).

To access the configuration dialogue, set **Enable Grey Listing** to **yes** (default: **no**) and then click the **Edit** button to the right of the **Advanced Grey Listing Options**. The following parameters define grey listing behaviour in detail:

**List 6-11** MailGW Settings - Content Filter - Grey Listing - section Advanced Grey Listing Options

Parameter	Description
<b>Grey Listing Time (Min)</b>	This is the time (in minutes) expected to have passed between the first and the second SMTP delivery attempt (default: <b>1</b> ). Higher values increase message delivery delay.
<b>White List Peers</b>	Grey listing does not apply to the MTAs defined here. Use this parameter to exclude known peers from grey listing explicitly, in order not to interfere with immediate mail delivery. A peer may be defined with its full IP address or domain name. Wildcards may be used (like <code>host.mailsrv.com</code> , <code>*.mailsrv.com</code> , <code>172.16.1.*</code> ). <b>Note:</b> Do not enter network address ranges.
<b>White List Senders</b>	Grey listing does not apply to the sender addresses defined here. Use this parameter to exclude known senders from grey listing explicitly, in order not to interfere with immediate mail delivery. A sender may be defined with his full e-mail address. Wildcards may be used (like <code>*@phion.com</code> ).
<b>Auto White List (Senders)</b>	When set to <b>yes</b> (default: <b>no</b> ) a sender is automatically added to the sender's white list, after a successful mail transfer. The sender-recipient pair is stored in the white list for a maximum of days as configured through parameter <b>Remove from White List after (d)</b> (see below) and is thereafter deleted. Manual deletion of white list entries is possible in the visualised list (see 5.8 Grey Listing Tab, page 267).
<b>Remove from Grey List after (h)</b>	Sender-recipient pairs, which have been added to the Grey List (see 5.8 Grey Listing Tab, page 267), are automatically removed from the list after the number of hours specified here (default: <b>24</b> ).
<b>Remove from White List after (d)</b>	Sender-recipient pairs, which have been added to the <b>Auto White List (Senders)</b> , are automatically removed from the list after the amount of days specified here (default: <b>30</b> ).
<b>Daily Report Mail to</b>	Specify a recipient for a daily report e-mail regarding grey listing utilisation in this place. By default, reports are sent to <b>Postmaster</b> (see Postmaster Mail-Address). With <b>Nobody</b> selected no report mails are generated. If any other report recipient is desired, select the checkbox <b>Other</b> and specify an e-mail address. Multiple recipients have to be entered in a space separated list.

## Section **Blacklists**

This section represents a sort of "emergency-off-button", which means the administrator of the mail gateway is able to block certain hosts, subjects, sender, or recipients explicitly very fast (for example, virus warning: known

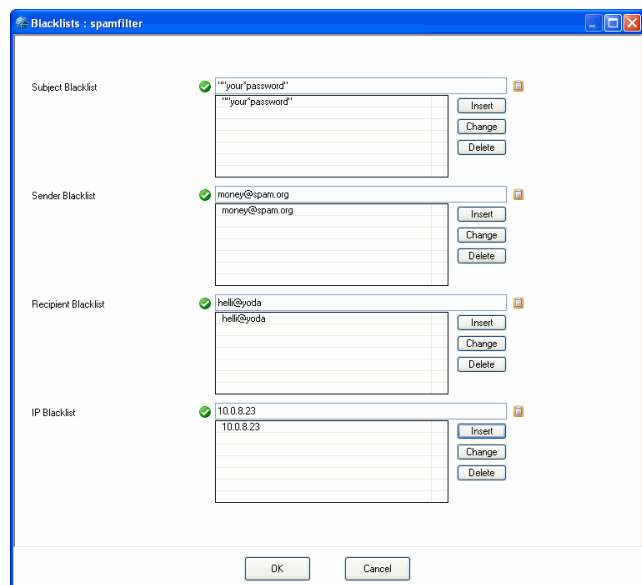
subjects of the virus may be entered in order to block before even receiving).

### Note:

This is a very static way of defining the behaviour of the mail gateway on certain mail. Therefore it should not be used as a spam filter in general but for such "emergency-overrides" as mentioned above. However, if you want to configure a spam filter, have a look at 4. Spam Filtering, page 257.

To access the configuration dialogue, set **Enable Blacklist** to **yes** (default: **no**) and then click the **Edit** button to the right of option **Blacklists**. The following parameters define blacklist behaviour in detail:

**Fig. 6-4** Blacklist configuration



**List 6-12** MailGW Settings - Content Filter - Blacklists

Parameter	Description	
<b>Subject / Sender / Recipient Blacklist</b>	Unwanted subjects / senders / recipients can be banned using these fields. The mail gateway will deny e-mails each matching with one of the phrases specified. <b>Note:</b> To ban subjects that are composed of multiple items including space characters consider the following case insensitive syntax rules to allow for correct interpretation of the banned subject: ? Use a question mark to identify space. * Use an asterisk to identify an arbitrary number of phrases. Space can be identified by an asterisk, too. " " Use quotation marks to identify a complete phrase. See below for a banned subjects interpretation example:	
Phrase to be banned	Syntax of banned subject	Interpretation
your password	your password	The filter will be ignored, because there is no applicable rule.
	"your?password"	All e-mails with the exact subject <i>your password</i> will be blocked.
	**your?password**	All e-mails with <i>your password</i> being a part of the subject phrase will be blocked regardless of the other phrases' content(s).
	**your*password**	All e-mails with the words <i>your</i> and <i>password</i> in the given succession will be blocked regardless of other phrases' contents before, between, or behind these two words.

List 6-12 MailGW Settings - Content Filter - Blacklists

Parameter	Description
<b>IP Blacklist</b>	Mail delivery coming from the host(s) inserted here will be refused. Multiple IP addresses can be specified.

### Section HTML Tag Removal

To protect your network from HTML e-mails with annoying or potentially dangerous content, such as hyperlinks leading to faked websites, images with objectionable content, ... the mail gateway may be configured to alter HTML tags in e-mails, so that the tags lose their function. Links thus lose their link characteristic and images can no longer be loaded from the servers they are lying on. By this means users can be prevented from clicking on links unintentionally or thoughtlessly.

**Note:**

Keep in mind that HTML tag removal applies for incoming and outgoing e-mails likewise.

List 6-13 MailGW Settings - Content Filter - HTML-Tag Removal

Parameter	Description
<b>Remove HTML Tags</b>	Set to <b>yes</b> (default: <b>no</b> ) to enable HTML tag altering.
<b>Remove HTML Link Tag</b>	When set to <b>yes</b> (as it is by default) link ( <code>a href</code> ) tags in HTML e-mails are altered, so that the link uses its function. The string of the link itself, though, remains unchanged. The linked destination can be viewed by copying the link from the e-mail and pasting it into the address field of the browser.
<b>Remove HTML Img Src Tag</b>	When set to <b>yes</b> (default: <b>no</b> ) image source ( <code>img src</code> ) tags in HTML e-mails are altered so that they lose their function. Linked images will no longer be loaded from the servers they are placed on. Keep in mind that this function destroys the design of HTML e-mails (like in newsletters), outgoing, and incoming likewise.

### Section Misc

List 6-14 MailGW Settings - Content Filter - Misc

Parameter	Description
<b>Strip Received Lines</b>	Every SMTP server or relay registers itself within the mail header (Received Lines). These entries typically reflect the company-internal mail infrastructure. Setting this parameter to <b>yes</b> (default: <b>no</b> ) causes that this internal and confidential information is stripped from the mail header. The number of "received" lines in the header stays the same but the content is replaced by dummy entries and thus no longer contains security critical information. <b>Note:</b> Be aware that mail header modification makes mail loop detection less efficient.
<b>Strip Received Lines Text</b>	The text entered here replaces the original text stripped from the e-mail header.
<b>Remove Phion ID</b>	When activated this parameter removes the phion ID from the mail header of dispatched e-mails. Aim of this setting is security enhancement through mail gateway identity concealment and decreased software traceability.

## 3.2.6 Limits

This section allows for configuration of various mail gateway service limits.

List 6-15 MailGW Settings - Limits - section Mail Gateway Limits

Parameter	Description
<b>Limit Mail Data Size</b>	This option activates/deactivates mail data (attachments) size limit (default setting: <b>yes</b> ). The attachment size limit is specified in the <b>Mail Data Size (MB)</b> field below.

List 6-15 MailGW Settings - Limits - section Mail Gateway Limits

Parameter	Description
<b>Mail Data Size (MB)</b>	Enter a value > 0 (default: <b>20</b> ). If mail size exceeds the specified value, the mail gateway refuses delivery and returns an error message to the sender. <b>Note:</b> This parameter reflects the actual mail body size because SMTP applies transfer encoding. The actual mail size may be greater than the physical size of the attachment. For example, if you add an attachment of about 5MB size, the total mail size could be up to about 6.5MB.
<b>DSN for Max Data Size Excess</b>	Set to <b>yes</b> (default: <b>no</b> ) if you want the mail gateway to create an extended Delivery Status Notification (DSN) mail, when an e-mail has exceeded the max. allowed size.
<b>Maximum Number of Recipients</b>	This setting reflects the maximum number of recipients of a mail. Since RFC2821 requires at least 100 possible recipients of a mail, this setting cannot be smaller than the required value (default: <b>200</b> ).
<b>DSN for Max Recipients Excess</b>	Set to <b>yes</b> (default: <b>no</b> ) if you want the mail gateway to create an extended Delivery Status Notification (DSN) mail, when an e-mail has been forwarded to more recipients than allowed.
<b>Refuse Empty Mail from</b>	Defines whether e-mails with empty sender information are rejected. By default ( <b>no</b> ) the SMTP server accepts every incoming e-mail.
<b>Accept Loose Domain Name</b>	Domain names may only exist of the following characters: [-.0-9A-Za-z]. Via this parameter incorrect domain names may be accepted: <b>no</b> - an incorrect domain name causes that the e-mail is rejected <b>yes</b> - domain names are not checked, that means e-mails with incorrect domain names will be delivered.
<b>Max. Attachments</b>	Defines the maximum number of to-be-scanned attachments per MIME e-mail.
<b>Drop Mails over Attachment Limit</b>	Defines whether e-mails contain too many attachments (as defined in parameter <b>Max. Attachments</b> ) are rejected.
<b>Drop Fragmented Mails</b>	Defines whether malformed/damaged e-mails are rejected.
<b>Max Age of crashed Mails (d)</b>	A mail in the "crashed" directory stays for this amount of days.
<b>Max. SMTP Line Length</b>	Enter the maximum line length. phion recommends, like RFC defines, a maximum length of 1000 characters.

List 6-16 MailGW Settings - Limits - section DoS Protection

Parameter	Description
<b>Parallel Inbound / Outbound Connections</b>	These fields specify how many parallel inbound or outbound connections for receiving mail to the server are allowed in total (default: <b>5</b> ). If your mail gateway has to handle a lot of mail traffic, you may have to increase this value. <b>Note:</b> This value must not be 0.
<b>Parallel Inbound / Outbound Conn. per Peer</b>	These fields specify how many parallel TCP connections from a single inbound or outbound source IP address are allowed (default: <b>25</b> ). This provides an effective protection against DoS (Denial of Service) attacks. <b>Note:</b> This value must not be 0. <b>Note:</b> The value of maximum parallel connections per peer may not be greater than the maximum number of parallel connections. <b>Note:</b> With parameter <b>Parallel Connection Limit</b> (see page 256) set to <b>yes</b> , the event <b>Resource Limit Exceeded: Max connections (per Peer)</b> [136] is triggered when the limit values are exceeded.



## 3.2.7 Reporting

### Entries in Access Cache

List 6-17 MailGW Settings - section Entries in Access Cache

Parameter	Description
<b>Delivered / Undelivered Entries</b>	Through these fields, a maximum number of Access Cache entries may be defined for successfully delivered ( <b>Delivered Entries</b> ) and undelivered e-mails ( <b>Undelivered Entries</b> ). For every mail job processed by the mail gateway a history entry is stored in a file. This history file is visualised in the <b>Access Cache</b> (see 5.1 MailGW Operation via GUI, page 263). The <b>Access Cache</b> reflects a FIFO ( <b>First In First Out</b> ) list. If the number of entries in the Access Cache gets greater than the value defined through these fields (each with default <b>100</b> ), the oldest entry is deleted according to its reception time.

### Section Event Settings

If you would like your mail gateway service to generate event messages, you may specify those event types, which should trigger events and event notification messages, in this configuration area (for detailed information on eventing, see **Eventing**, page 305). Each event type has its unique event ID number.

The following options are available for configuration:

List 6-18 MailGW Settings - Event Settings

Parameter	Description
<b>Admin Reception Commands</b>	When set to <b>yes</b> (default: <b>no</b> ) the event <b>Mail Operation Changed: [user@peer]</b> [4504] will be triggered when an e-mail is blocked or allowed manually through the admin commands <b>Allow/Block Mail Reception</b> (see 5.6 Processes Tab, 5.6.1 Context Menu Entries, page 266).
<b>Admin Discard Mail Cmd</b>	Administrators with special admin permissions are allowed to discard mails in the mail queue. When set to <b>yes</b> (default: <b>no</b> ) the event <b>Mail Data Discarded: ID [spool-ID Nr.]</b> [4500] will be triggered when an e-mail is discarded with an admin command.
<b>Mail Denied</b>	The phion netfence mail gateway service provides special features for denying mail (spam filter ..., see 3.2.5 Content Adaptions, page 253). When set to <b>yes</b> (default: <b>no</b> ) the event <b>Mail Relaying Denied: Deny [Rule]</b> [4508] will be triggered when an incoming mail is denied according to content filter configuration.
<b>Recipient Dropped</b>	If a mail recipient matches a banned recipient specified in the Blacklist configuration (see 3.2.5 Content Filter, Page 231), delivery to this recipient will be refused; other recipients of the same mail are not affected by this action. When set to <b>yes</b> (default: <b>no</b> ) the event <b>Mail Delivery Refused: Drop recipient &lt;[e-mail address of dropped recipient]&gt;</b> [4506] will be triggered, when e-mail delivery to a banned recipient is refused. <b>Note:</b> Some e-mail client applications disconnect at once after a recipient has been dropped. The e-mail might therefore not be delivered to any of its addressees.
<b>Parallel Connection Limit</b>	When set to <b>yes</b> (default) The events <b>Resource Limit Pending/Resource Limit Exceeded: Max connections (per Peer)</b> [135/136] are triggered when the number of parallel connections allowed to the mail gateway reaches a critical value or exceeds the value specified in the limits configuration window (sections <b>MailGW Settings - Limits - section Mail Gateway Limits</b> and <b>MailGW Settings - Limits - section DoS Protection</b> , see 3.2.6 Limits, page 255).
<b>Spooling Limit</b> (activates parameter <b>Number of Queued Mails</b> ) (triggers event ID 136)	Incoming mail jobs are queued and thereafter delivered by the available MTAs (see 5.3 Mail Queue Tab, page 263). However, during times of heavy incoming mail traffic, the mail queue may start to grow. If <b>Spooling Limit</b> is set to <b>yes</b> (default), you can set a maximum limit for the length of the mail queue in the field below ( <b>Number of queued Mails</b> = Max 10000 Mails). If the spool queue length reaches a critical value or exceeds the maximum limit, the events <b>Resource Limit Pending/Resource Limit Exceeded: Spool Limit Exceeded</b> [135/136] are triggered.

List 6-18 MailGW Settings - Event Settings

Parameter	Description
<b>Mail Data Size Limit</b>	When set to <b>yes</b> (default: <b>no</b> ) the event <b>Mail Size Limit Exceeded</b> [140] is triggered when the size of an e-mail exceeds the value specified in the limits configuration window ( <b>Limit Mail Data Size</b> , see 3.2.6 Limits, page 255).
<b>User Defined Rule Event</b>	It is also possible to define your own events by using the Expert Settings located in the Advanced Setup configuration are (page 251). Feasibility of user defined rule events is activated by default (default: <b>yes</b> ). If no rule events have been defined, this setting is ignored. Personalised events trigger the events <b>Mail Rule Notice</b> [4512], <b>Mail Rule Warning</b> [4513], and <b>Mail Rule Alert</b> [4514].
<b>Bad Rulefile Loaded</b>	Section Global Domain Parameters, <b>Section Local Domain Settings</b> or Section Extended Domain Setup Settings respectively (see 3.2.1 Basic Setup and 3.2.2 Extended Domain Setup) are stored in a rule file. Although config changes are checked before activation, the mail gateway service may be unable to locate the rule file. This is a serious problem because mail reception is no longer possible. When set to <b>yes</b> (default: <b>no</b> ) the event <b>Flawed Configuration Data Activation</b> [2380] is triggered when the rule file is missing or a corrupt rule file has been loaded.
<b>Kill Worker Process</b>	As soon as connection to the mail gateway is established, the mail data receiving process starts. This process is called a <b>worker</b> . Worker processes can be killed with the admin command "Kill Process" (see 5.6 Processes Tab, page 266) if necessary (for example, if you want to abort the transmission of an e-mail with a large attachment). When set to <b>yes</b> (default: <b>no</b> ) killing a worker process triggers the event <b>Subprocess Kill Requested: Kill PROC_SMTP Worker</b> [2054]. <b>Note:</b> Killing a SMTP worker process causes data loss. <b>Minimum configuration:</b> You have to specify at least an internal and external bind IP (both IPs have to be configured as Server IPs), and a postmaster address to start the mail gateway service on your netfence box.

### Section Statistic Settings

This section provides special settings for the statistics module. Select the statistics types that should be created.

For information on the different types of statistics of the mail gateway service see 5.9 Logs, Statistics, Events, page 268; for general information see **Statistics**, page 295).



## 4. Spam Filtering

netfence gateway provides spam filtering by placing the mail filter SpamAssassin™ at the disposal. SpamAssassin™ identifies spam by using mechanisms such as text analysis, Bayesian filtering, DNS blocklists, and collaborative filtering databases.

**Note:**

The complete SpamAssassin™ documentation is available at [www.spamassassin.org](http://www.spamassassin.org).

Spam filter settings are defined in two configuration areas:

- Spam Filter Client - see 4.2.1 Configuring the Spam Filter Client, page 258
- Spam Filter Service - see 4.2.2 Configuring the Spam Filter Server, page 259

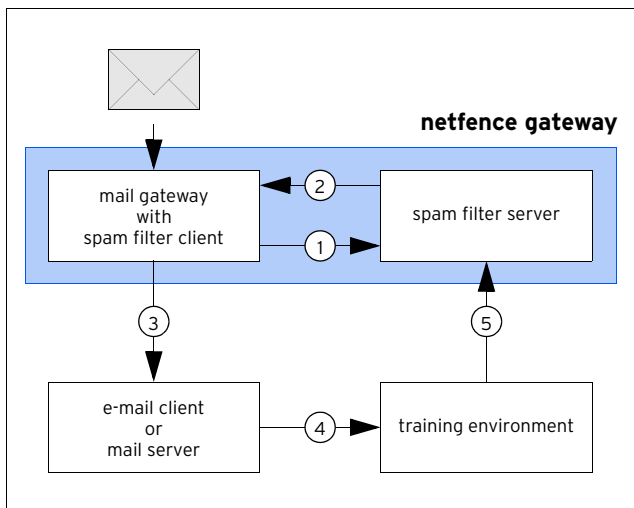
Optionally, a training environment may be introduced to improve the filtering result (4.2.3 Configuring the Training, page 261).

Follow the instructions available in **Configuration Service** - 4. Introducing a New Service, page 97 to set up the spam filter service, and select **SPAM-Filter** as **Software Module**.

### 4.1 Theory

Generally, spam filtering involves the following procedures:

**Fig. 6-5** Overview: Spam filtering process



**Step 1 Mail gateway/spam filter client to spam filter server**

The mail gateway service pipes all mail traffic to the spam filter server. Here, the e-mails are processed through SpamAssassin™. When the spam filter is not available, e-mails are delivered without filtering.

SpamAssassin™ applies a variety of tests to determine the probability that an e-mail is spam: It examines the e-mail's header and body locally, runs through the configured rule set (list 6-23, page 261) and a Bayesian filter. Each single rule adds a value to the overall spam value of the e-mail. If the complete score exceeds a certain threshold (default: **5**), the e-mail is regarded as spam.

**Note:**

As a rule of thumb it can be said that the higher an e-mail's score is, the higher is the probability that it will be classified as spam. For detailed information concerning filtering mechanisms, please refer to [http://spamassassin.apache.org/tests\\_3\\_1\\_x.html](http://spamassassin.apache.org/tests_3_1_x.html).

The spam filter adds a tag to the mail header according to an e-mail's classification as SPAM or HAM (no SPAM).

- for SPAM mail: X-SPAM-STATUS: Yes  
X-SPAM-FLAG: YES
- for HAM mail: X-SPAM-STATUS: No

Additionally, it adds the results of the triggered tests to the e-mails's body.

**Fig. 6-6** Header of an e-mail identified as spam

```
Received: from mailsrv.phion.com ([1.2.3.4] by smtp.phion.com
with Microsoft SMTPSVC(6.0.3790.1830);
    Fri, 24 Mar 2006 08:48:54 +0100
Received: from xxx ([x.x.x.x]) by xxx with xxx;
    24 Mar 2006 08:48:09 -0100
Received: from xxx ([x.x.x.x]) by xxx with xxx;
    Fri, 24 Mar 2006 08:48:09 +0100
X-Message-Info: ZRCPB+dfk02+jvm+QG+760/7861938317196
Date: Fri, 24 Mar 2006 15:48:48 0800
Message-Id: <400357198482.74998@spamdmain.net>
From: "Geoff" <Geoff572@spamdmain.net>
To: <spam@phion.com>
Subject: [SPAM] demehoqlola
MIME-Version: 1.0 (produced by digybdxifut 0.4)
Content-Type: multipart/alternative;
    boundary="-----090708090808030606080206"
X-phion-id: 20060324-084808-02011-00
X-Spam-Prev-Subject: demehoqlola
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 3.0.4 (2005-06-05) on
spamsrv.phion.com
X-Spam-Level: **
X-Spam-Status: Yes, score=2.6 required=2.0
tests=ALL_TRUSTED,BAYES_00,DATE_IN_FUTURE_06_12,HTML_MIME_NO_HTML_TAG,INVALID_DATE,MIME_HTML_ONLY,MIME_HTML_ONLY_MULTI,X_MESSAGE_INFO autolearn=no version=3.0.4
X-Spam-Report: * 0.2 INVALID_DATE Invalid Date: header (not RFC 2822)* 4.2 X_MESSAGE_INFO Bulk email fingerprint (X-Message-Info) found* 1.3 DATE_IN_FUTURE_06_12 Date: is 6 to 12 hours after Received: date* -3.3 ALL_TRUSTED Did not pass through any untrusted hosts* -2.6 BAYES_00 BODY: Bayesian spam probability is 0 to 1 %* [score: 0.0042]* 0.2 MIME_HTML_ONLY BODY: Message only has text/html MIME parts* 0.1 HTML_MIME_NO_HTML_TAG HTML-only message, but there is no HTML tag* 2.4 MIME_HTML_ONLY_MULTI Multipart message only has text/html MIME parts
X-AntiVirus: checked by AntiVir MailGate (version: 2.0.3-25; AVE: 6.33.1.0; VDF: 6.33.1.1; host: spamsrv.phion.com)
Return-Path: geoff572@spamdmain.net
X-OriginalArrivalTime: 24 Mar 2006 07:48:54.0566 (UTC)
FILETIME=[664AD460:01C64F17]
X-TM-AS-Product-Ver: SMEX-7.0.0.1345-3.52.1006-14342.000
X-TM-AS-Result: No-3.150000-8.000000-31
X-UIDL: AAQMd8AAAAQwBNsx5nZbMMwzBBOyqFh
TO: spam@phion.com
CC:
BCC:
```

### Step 2 Spam filter server to mail gateway

After the e-mail has been classified, it is returned to the mail gateway for further processing.

### Step 3 Mail gateway to e-mail client/mail server

E-mail clients may utilise the content of the supplemented mail header to sort e-mails (like moving spam tagged e-mails to a spam directory automatically).

#### Attention:

Moving spam tagged mails into the trash bin without checking is NO good idea (see Step 4).

### Step 4 Improve spam filtering via training environment

As spam filtering is merely based on statistics it may happen that e-mails are tagged wrongly. To minimise the risk for such incidents, training the spam filter is highly recommended.

Training means sorting out misclassified e-mails, re-sorting them into SPAM, HAM and FORGET mailboxes (list 6-26, page 261), and providing them to SpamAssassin™ for filter mechanisms improvement.

### Step 5 Spam filter server update

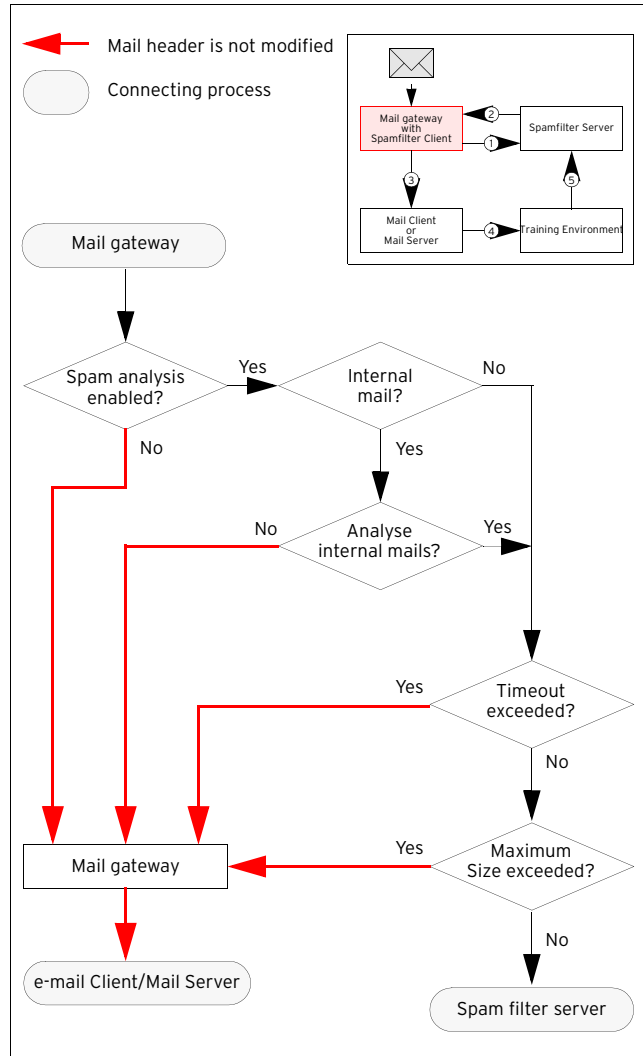
SpamAssassin™ periodically fetches e-mails from the training environment and thus adapts its tests to improve future e-mail classification.

## 4.2 Configuration

### 4.2.1 Configuring the Spam Filter Client

The spam filter client's work process involves the following:

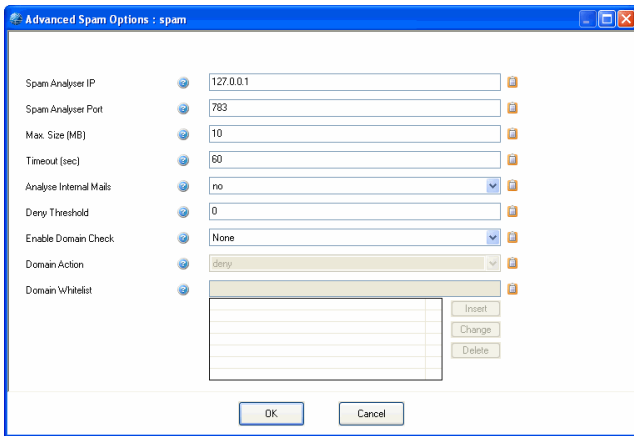
Fig. 6-7 Flowchart - Spam filter client



Spam filter client configuration is done through section **Spam Analysis** within the **MailGW Settings** (see 3.2 MailGW Settings, Section Spam Detection, page 253).

Enable the spam filter through setting **Enable Spam Analysis** to **yes**, and click the **Set ...** button to open the **Advanced Spam Options** configuration window:

Fig. 6-8 Spam Analysis configuration



**Note:**

Only netfence spamfilter services may be used as spam engines.

List 6-19 MailGW Settings - Spam Analysis

Parameter	Description
<b>Spam Analyser IP</b>	This IP address is the Bind IP of the spam filter service (Bind or Additional IP, see 4.2.2 Configuring the Spam Filter Server, page 259). Optionally, you may enter a DNS-resolvable host name. The host name can be used to implement load balancing for high traffic scenarios.
<b>Spam Analyser Port</b>	This value (default: 783) must correspond with the port defined for the spam filter service (Listening Port, see 4.2.2 Configuring the Spam Filter Server, page 259).
<b>Max. Size (MB)</b>	This parameter defines the maximum size an e-mail may have to be processed by the spam filter. If the e-mail exceeds this value (default: 1MB) it will not traverse the filter mechanism and will be delivered to its recipient without header modification (spam tag) instead.
<b>Timeout (sec)</b>	This parameter defines the maximum duration (default: 60 s) it may take to analyse an e-mail. If the value is exceeded, the e-mail is delivered to its recipient without header modification (spam tag).
<b>Analyse Internal Mails</b>	When set to <b>yes</b> (default: <b>no</b> ) mail traffic generated by internal mail domains is also classified. <b>Note:</b> Analysing of internal mail traffic may lead to high CPU load.
<b>Deny Threshold</b>	An e-mail is rejected when it exceeds the threshold configured here. The threshold is calculated from an e-mail's spam score (resulting from the testing sequences) multiplied by factor 100. To deactivate this parameter, enter a threshold of <b>0</b> .
<b>Enable Domain Check</b>	This field allows for checking of sender domains. The following options are available: <ul style="list-style-type: none"> <li>➤ <b>None</b> - sender domains are not checked for validity</li> <li>➤ <b>MX</b> - sender is only accepted if it is one of the domain's MX servers.</li> <li>➤ <b>Host-Domain</b> - sender is only accepted if it is within the mail domain. For example, if the sending e-mail address is e.example@foo.com then the sending host has to be within domain foo.com.</li> <li>➤ <b>All-MX-Domains</b> - sender has to be in a domain of the mail-domain MX servers. For example, if the sending e-mail address is e.example@foo.com and the MX servers of the domain foo.com are server1.foo.com and server1.backupfoo.com then the sending host has to be either in domain foo.com or backupfoo.com.</li> </ul> <p>Domain check failure results in one of the actions configured through parameter <b>Domain Action</b> (see next entry).</p>

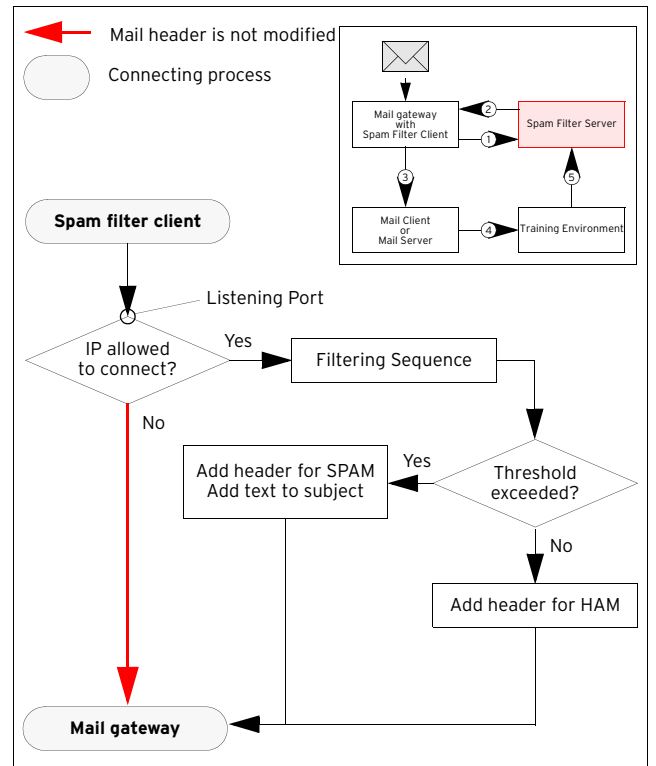
List 6-19 MailGW Settings - Spam Analysis

Parameter	Description
<b>Domain Action</b>	This field only has to be configured, if domain checking (see above) has been enabled. Domain check failure results in one of the following actions: <ul style="list-style-type: none"> <li>➤ <b>logging</b> - the e-mail is delivered and a corresponding log entry is created</li> <li>➤ <b>deny</b> - the e-mail is not delivered and a corresponding log entry is created</li> </ul>
<b>Domain Whitelist</b>	This field takes a list of trusted domains, which should be excluded from spam filtering. This list is consulted before the spam filter is applied. Top-level and sub-domains may be defined (like phion.com and *.phion.com).

## 4.2.2 Configuring the Spam Filter Server

The spam filter services's work sequence involves the following:

Fig. 6-9 Flowchart - Spam filter Server



### Step 1 Introducing the service

To introduce the service, follow the instructions in **Configuration Service - 4. Introducing a New Service**, page 97 and select the software module **SPAM-Filter**.

## Step 2 Configuring the service


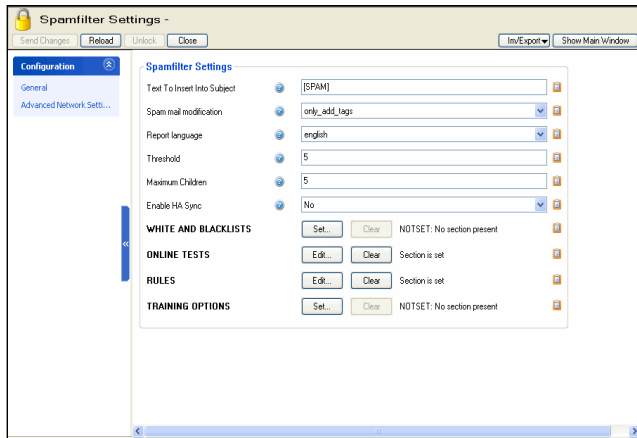
Service configuration takes place in the  **Spamfilter Settings** within the introduced spam filter service.

Fig. 6-10 Spam filter configuration dialogue



### 4.2.2.1 General View

List 6-20 Spamfilter Config - section Spamfilter Settings

Parameter	Description
<b>Text To Insert Into Subject</b>	In case the e-mail is classified as SPAM, the text inserted here is placed at the beginning of the e-mail subject. If this field is left empty, the subject field of the e-mail is left as it is.
<b>SPAM Mail Modification</b>	This setting determines the extent to which an e-mail should be modified if it is classified as SPAM. The followings settings are applicable: <ul style="list-style-type: none"> <li>➤ <b>only_add_tags (default)</b> triggers adding of SPAM tags into the mail header but does not alter the mail body</li> <li>➤ <b>as_attachment</b> triggers insertion of a verbose SPAM report into the mail body and appends the actual e-mail as attachment</li> <li>➤ <b>as_attachment_text</b> triggers insertion of a verbose SPAM report into the mail body and appends the actual e-mail as text attachment</li> </ul>
<b>Report Language</b>	This option determines the language of the SPAM report that is inserted into the e-mail body when <b>as_attachment</b> or <b>as_attachment_text</b> is applicable for parameter <b>SPAM Mail Modification</b> (default: <b>English</b> ). The wording of the report is generated by SpamAssassin and is not customisable. Note that report translations are not yet available completely for all configurable languages.
<b>Threshold</b>	A mail is classified as SPAM when its score exceeds the configured threshold. Increasing the threshold will increase the amount of SPAM missed, but will reduce the risk of false positives (default: <b>5</b> , medium: <b>7.5</b> , high: <b>10</b> , max.: <b>100</b> ).
<b>Maximum Children</b>	This parameter specifies the number of concurrent spam filter servers. When the limit is reached, spam filtering is put on hold until a server is available.
<b>Enable HA Sync</b>	Ticking this checkbox activates spam filter synchronisation between an HA pair. The synchronisation starts at 4:20 am. If this default setting is not acceptable, simply clear the check box and create a cronjob for the required time interval ( <b>Configuration Service</b> - 5.1.3 System Scheduler, page 102) using the following line: <code>/opt/phion/modules/server/spamfilter/bin/hacron.sh SERVER SERVICE</code> <b>Attention:</b> The spam filter is deactivated while synchronisation is running.

List 6-21 Spamfilter Config - section WHITE/BLACK LISTS

Parameter	Description
	<b>Note:</b> Take into consideration that using white/blacklists adds a specific "list value" to the corresponding scan value. This means valid black list entry adds spam value 10; valid white list value lowers the spam value by 6. Both values (10, -6) can be overruled in the rules section (page 261).
<b>Whitelist From</b>	Mail from these senders will not be tagged as SPAM (regardless of an e-mail's score).
<b>Whitelist To</b>	Mail to these recipients will not be tagged as SPAM (regardless of an e-mail's score).
<b>Blacklist From</b>	Mail from these senders will always be tagged as SPAM.
	<b>Note:</b> The whitelist is processed before the blacklist. Thus, it is possible to configure a specific sender <code>user@domain.com</code> in the parameter <b>Whitelist From</b> as allowed, and hence to block all further senders from the domain through entering the value <code>*@domain.com</code> in the parameter <b>Blacklist From</b> .

List 6-22 Spamfilter Config - section ONLINE TESTS

Parameter	Description
	This section serves to gain access to collaborative spam-tracking data bases in the internet. The following services are available: <b>Note:</b> For online tests to function, Internet access has to be enabled on specific ports.
<b>Use DCC</b>	<b>D</b> istributed <b>C</b> hecksum <b>C</b> learinghouse. Does not list domain names or IP addresses but detects bulk mail messages by creating checksums. These checksums include values that are constant across common variations in bulk messages, including personalisation. Internet access on UDP port 6277 has to be enabled for DCC to function. For more detailed information concerning DCC please check <a href="http://www.rhyolite.com/anti-spam/doc">www.rhyolite.com/anti-spam/doc</a> .
<b>Use Razor V2</b>	Razor detects spam by analysing statistical and randomised signatures that spot mutating spam content. Internet access on TCP port 2703 has to be enabled for Razor V2 to function.
<b>Use Pyzor</b>	Pyzor detects spam by calculating digests of e-mail parts and comparing these with other recipient's e-mails. Internet access on TCP port 80 and UDP port 24441 have to be enabled for Pyzor to function properly. Pyzor tries to retrieve an up-to-date server list by accessing the link <a href="http://pyzor.sourceforge.net/cgi-bin/info_rm-servers-0-3-x">http://pyzor.sourceforge.net/cgi-bin/info_rm-servers-0-3-x</a> . If it does not succeed, it uses its internal default server list.
<b>Skip RBL-Tests</b>	<b>R</b> ealtime <b>B</b> lackhole <b>L</b> ist; a list containing server IPs that are responsible for spam or are known to be hijacked for spamming. Ticking this option results in deactivating the IP search in this list.
<b>Use Black List Tests</b>	Checks for domain names appearing in e-mails and compares them against online black lists, in order to detect messages sent by spammers. <b>Note:</b> By enabling DNS blocklists (DNSBL) the spamfilter service uses external servers to verify if specific IP addresses or URIs have already been used by spammers. The usage policy of the external service <a href="http://surbl.org">surbl.org</a> guarantees free use for organizations that have fewer than 1,000 users or scan fewer than 250,000 messages per day. Please do not enable DNSBL checks if your organization exceeds either the number of email users or number of messages per day. <b>Note:</b> To disable this function create a rule in section <b>RULES</b> , parameter <b>Rules</b> , with this contents: <code>score URIBL_BLACK 0 (Rules, page 261).</code>

List 6-23 Spamfilter Config - section RULES

Parameter	Description
<b>Rules</b>	This section allows manual overriding of specific testing sequences. To disable a given test set its score to 0. Especially when a test is known to deliver "wrong" results, adapting the sequence options to one's needs is a vital measure.  <b>Note:</b> For a complete list of available rules, have a look at <a href="http://spamassassin.apache.org/tests_3_1_x.html">http://spamassassin.apache.org/tests_3_1_x.html</a> .

List 6-24 Spamfilter Config - section TRAINING OPTIONS

Parameter	Description
	see list 6-26, page 261

### 4.2.2.2 Advanced Network Settings View

List 6-25 Spamfilter Config - Advanced Network Settings

Parameter	Description
<b>Listening Port</b>	The value in this field specifies the port the service is listening on.
<b>IPs Allowed To Connect (ACL)</b>	This field determines the spam filter clients, which are allowed to connect to the spam filter service. The default IP 127.0.0.1 specifies the internal loopback interface of the phion netfence. This interface has to be used when mail gateway and spam filter reside on the same system.

### 4.2.3 Configuring the Training

Because spam filtering is merely based on an e-mail's classification according to specific iterative attributes, SpamAssassin™ will most possibly fail in detecting all SPAM, and eventually tag non-SPAM e-mails as SPAM. This efficiency factor is utterly normal. The filter has to be trained, to improve filtering mechanisms.

Training is done by sorting out misclassified e-mails and providing them to SpamAssassin™ in SPAM, HAM and FORGET mailboxes for collection.

**Attention:**

Create a separate mail account for testing. If you use a real mail account, it will be classified as spamming one.

**Note:**

The spam filter training environment has to be configured on the mail server, not on the netfence gateway.

SpamAssassin™ modifies several ratings of the filter mechanisms in order to improve the chance of recognising spam e-mails.

SpamAssassin™ bases on statistical evaluations that have to react very stable on outliers. To guarantee such a behaviour, SpamAssassin™ adapts its filter mechanisms in small steps. Therefore, each learned spam e-mail increases the chance of recognising this e-mail as SPAM, but does not guarantee that the e-mail is considered a SPAM when re-sending it.

The configuration takes place in the 🍌 **Spamfilter Settings** within the introduced spam filter service.

Ticking the check box **Enable Training** activates the training options.

List 6-26 Spamfilter Config - section TRAINING OPTIONS

Parameter	Description
<b>Enable Training</b>	Ticking the checkbox activates spam filter training.
<b>Mailserver (IMAP)</b>	This parameter specifies the IP address/name of the external mail server.  <b>Note:</b> The mail server has to be capable of IMAP.
<b>Account</b>	In this field the user name/account name has to be entered.
<b>Password</b>	This field takes the the mail account's password.  <b>Note:</b> Take into consideration to use english characters and digits only and to avoid blanks in the password. For security reasons this password must be entered twice (field <b>Confirm</b> ).
<b>Mailbox SPAM</b>	SPAM mail that was delivered without being tagged as SPAM has to be put into this mailbox.
<b>Mailbox HAM</b>	HAM mail that was wrongly tagged as SPAM has to be put into this mailbox.
<b>Mailbox FORGET</b>	Mail, which should not be classified as either SPAM or HAM, has to be put into this mailbox.  <b>Note:</b> For the correct path for the three mail boxes please consult your mail server administrator. Depending on the directory structure it might be necessary to enter a name space (for example ~/mail/SPAM). By default, if the folder names are simply specified as SPAM, HAM and FORGET, the user's home directory in (/home/<username>) will be queried.
<b>Keep Mails In Mailbox</b>	Select this checkbox, if for some reason (especially when using multiple spam filter servers), it is necessary to keep the e-mails in the mailbox in order to provide something to learn for the other servers.  <b>Note:</b> The mail box's content, however, is trained only once. This means, when you add new e-mails to a bundle of e-mails in a mailbox, which have already been processed, only the added e-mails will be trained.
<b>Time (h)/Time (min)</b>	Defines the time of day for spam filter training. For example entering <b>Time (h) 4</b> means 4 am, whereas 16 indicates 4 pm. At the set time the spam filter collects mail from the SPAM, HAM, and FORGET mailboxes and processes the retrieved e-mails for training.

#### 4.2.3.1 Setting up the Training Environment

**Note:**

Spam filter training can only be configured with a mail server capable of IMAP.

The training environment consists of an IMAP mail server and e-mail clients, which can directly access the mail server's folder structure (like Microsoft Outlook, Mozilla, Evolution, ...). All that has to be done, is to create three mailboxes on the mail server (one each for HAM, SPAM, and FORGET e-mails), either for all mail server users in whole (if their judgement is reliable) or for each mail user separately.

**Attention:**

Connectivity between IMAP server and netfence gateway is stringently required. To test connectivity, enter the following commands at the command line interface:

```
telnet IMAPServer imap2 (tests the connection itself)
A001 CAPABILITY
A002 LOGIN username pwd (verifies the user and password)
```

Training environment suitable for **RELIABLE** users:



- All users have access to the "training area" on the mail server and file their mis-tagged mails into the corresponding directories.

**Note:**

To maintain privacy on this "public" file structure, you may configure user access rights, so that each user only sees his own e-mails.

- Each user has his own HAM-SPAM-FORGET folder structure and sorts the mis-tagged mails accordingly. E-mails for training area update are collected from these folders with a script (figure 6-11, page 262).

Training environment suitable for **UNRELIABLE** users:

All users share a HAM-SPAM-FORGET folder structure, which is detached from the training environment, and sort their mis-tagged mails accordingly. The mail server administrator has to check the folder contents for correct classification before moving the e-mails to the training environment.

This approach may be additional work for the administrator but it guarantees a "clean" training environment because poisoning of the database with incorrect entries can be avoided.

**Fig. 6-11** Example script for e-mail collection

```
#!/bin/bash
# assumptions:
# HAM and SPAM live under /home/$USER/mail/
# TARGETDIR should not be /tmp/, but a more secure location
# no filelocking, etc
# 2003-12-18 j.radinger@phion.com

TARGETDIR=/tmp/

SPAM=`find /home/*/mail/ -type f -name SPAM`
HAM=`find /home/*/mail/ -type f -name HAM`

for a in $SPAM $HAM; do
  if [ -f $TARGETDIR/$a ]; then
    rm -f $TARGETDIR/$a
  fi
done

for a in $SPAM; do
  cat $a >> $TARGETDIR/SPAM
done

for a in $HAM; do
  cat $a >> $TARGETDIR/HAM
done
```

## 4.2.4 Archiving and Updating

Because it may grow to non assessable size, the SpamAssassin database is not included in box PAR files. If desired, it has to be archived manually.

**Note:**

Because of the highly dynamic behaviour of SpamAssassin it is not recommended to restore the archived database, for example crash recovery.

### 4.2.4.1 Archiving the Database on a Single Box

To archive the database, create a backup of the directory `/var/phion/preserve/spamd/<server_servicename>/root`.

The much more elegant and easier way of archiving and restoring is to create a backup of the training environment (the messages in the SPAM, HAM and FORGET folders). In a new setup, the spam filter may then be re-trained with the original files. This method provides additional security

because the service does not have to be stopped and restarted for archiving - the database takes care of the updating/restoring procedure.

### 4.2.4.2 Updating the Database on the HA Partner

For updating purposes copy the contents of the folder `/var/phion/preserve/spamd/<server_servicename>/root` from the primary box to the HA box.

## 5. Mail Gateway Operation

### 5.1 MailGW Operation via GUI

To administer operative processes on the mail gateway, log on the box hosting the mail gateway service. As well on MC administered boxes, log on the box itself and not on the management centre. Access the administration GUI by clicking **MailGW** in the box menu.

**Note:**

The following mail gateway operation windows are only available after a minimum of values has been specified in the **MailGW Settings** configuration (Minimum configuration, Page 256).

The following tabs are available for operational purposes:

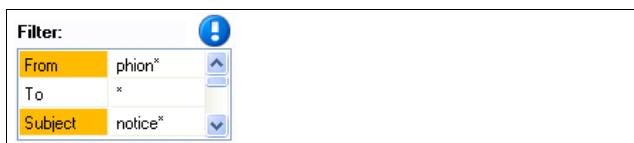
- Mail Queue Tab, see 5.3 Mail Queue Tab
- Access Tab, see 5.4 Access Tab
- Spam Tab, see 5.5 Spam Tab
- Processes Tab, see 5.6 Processes Tab
- Attachments Tab, see 5.7 Attachments Tab
- Grey Listing Tab, see 5.8 Grey Listing Tab

### 5.2 General Characteristics of the Graphical Interface

#### 5.2.1 Filters

In each tab, e-mail entries are arranged in an ordered list. This list is topped by a filter section area. Filters may be applied to each available column to narrow down the view. By default, all columns are marked with an asterisk (\*), which stands for a character string of any length. Press Enter or click the reload button to refresh the view after having defined a filter. As soon as a filter applies the filtered value is displayed highlighted in yellow and the filter is flagged with an exclamation mark.

Fig. 6-12 Filter settings



#### 5.2.2 Title Bar(s)

➤ **Changing the column sequence**

Information situated in the main window of each operational tab is captioned with a title bar. The data sets themselves are arranged in columns. The column sequence may be adjusted to personal needs either by

using the standard context menu (see 4.2 Standard Context Menu, page 395) or by dragging and dropping the respective column to another place.

➤ **Ordering data sets**

Data sets may be arranged ascending or descending respectively by clicking into the column labelling of the respective title bar. The information may not only be sorted alphabetically, but also with regard to a specific status.

#### 5.2.3 Context Menu Entries

- Right-clicking into any configuration area without selected item, makes the standard context menu available through the menu item **Tools** (see 4.2 Standard Context Menu, page 395).
- A menu item **Show in Sections** is included in most operational tabs. It allows switching between two views, the classical view, a continuous list, or a list combining groups of elements. In the section view, each section is topped by a *section header*.

### 5.3 Mail Queue Tab

This register displays pending mail jobs. In section view mails jobs are arranged according to their spam classification state. They are classified into the following categories:

- **Spam State Unknown**
- **Spam**
- **No Spam**

**Note:**






If no spam filter has been configured, all e-mails are categorised as Spam State Unknown, regardless of their content.

Information on currently queued jobs covers the following:

- **Spam** column  
E-mails are flagged with an icon according to their spam classification. The following icons are in use:
  - Spam State Unknown
  - Spam
  - No Spam
- **From** column  
Shows the sender address.
- **To** column  
Shows the recipient(s) address(es).
- **Subject** column  
Shows the mail object's subject.





### ➤ **State** column

Shows an icon displaying the current spool activity and a corresponding state description. The following icons are in use:

-  **active pending** - ready for delivery and pending until MTA is ready
-  **active** - delivery is performed right now
-  **giveup** - e-mail could not be delivered due to problems on the recipient's side and no further delivery attempts will be undertaken
-  **crash** - e-mail could not be delivered due to misconfiguration (for example missing MX record, unknown recipient domain ...)
-  **pause** - delivery has been paused due to execution of the admin command **Pause Delivery** (see 5.3.1 Context Menu Entries, page 264)

### ➤ **Prio** column

Shows the priority of the mail object:

-  low
-  normal (default)
-  high
-  urgent

### ➤ **APrio** column

Shows the actual priority of the mail object  
Due to high traffic a mail object can be ready for delivery but cannot be delivered yet. The object's priority continuously rises, until it can finally be sent. Effective priorities in the **APrio** column are the same as in the **Prio** column, except for priority urgent.

### ➤ **Size** column

Shows the size of the mail object.

### ➤ **NumTo** column

Shows the number of recipients for the mail object.

### ➤ **Tries** column

Shows the tries carried out for delivering the mail object.

### ➤ **Last Status** column

Shows the last try's status.

### ➤ **Next Try** column

Shows waiting period until next delivery try (hh:mm:ss).

### ➤ **Last Try** column



Shows time passed since last delivery try.

### ➤ **Receive Time** column

Shows receiving time of the mail object.

### ➤ **Scan State** column

Shows an icon displaying the e-mail objects scan state. The following icons are in use.

-  e-mail scan has been completed successfully
-  e-mail scan could not be executed completely and has been aborted

### ➤ **Spool ID** column

Shows the ID of the mail object.

## 5.3.1 Context Menu Entries

Right-clicking a data set opens a context menu with commands assisting in figuring out why a mail could not be delivered and allowing influence on execution of pending mail jobs.

### Note:

Execution of the commands made available through the context menu requires adequate permissions.

### ➤ **Show Envelope ...**

This command opens a window showing the mail envelope. The mail envelope contains information on the selected mail job, such as sender / recipient address, helo / ehlo name, mail size, scheduling priority ...

### ➤ **Show Log File ...**

This command opens a window showing the mail job's log file. The log file contains information on MTA operation.

### ➤ **Schedule Now**

If an e-mail cannot be delivered at once, the mail gateway retries delivery according to the MTA Retry Sequence (see MTA Retry Sequence, page 250). To skip the MTA Retry Sequence select this option to start a new delivery attempt.

### ➤ **Change Priority ...**

With this option you can change scheduling priority of the selected mail job. Default scheduling priority is **normal**. Jobs with **high** priority will be scheduled first; jobs with lower priorities will be scheduled thereafter. The following scheduling priorities exist:

- low
- normal (default)
- high
- urgent

### ➤ **Change Priority and Schedule ...**

This option combines the two scheduling options **Change Priority** and **Schedule Now**.

### ➤ **Pause/Resume Delivery**

Select **Pause Delivery** to halt delivery of a mail job.  
Select **Resume Delivery** to resume it.

### ➤ **Discard Mail**

Select this option to discard a mail job and to remove the mail object from the mail queue.

### Note:

Mails in active state cannot be discarded.

## 5.4 Access Tab

This register shows the Access Cache of the mail gateway service. The Access Cache contains completed mail jobs, which have been moved to it from the Mail Queue. The Access Cache thus represents a **history** of the mail gateway. The maximum number of entries the Access Cache may contain is specified through parameter sets **MailGW Settings - Limits - section Mail Gateway Limits** and **MailGW Settings - Limits - section DoS Protection** (page 255).

Again, in section view, e-mails are arranged in groups disclosing their spam classification state. Mails are classified into the following categories:

- **Spam State Unknown**
- **Spam**
- **No Spam**

All columns, except the **State** column, can be interpreted in the same way as described in 5.3 Mail Queue Tab, page 263. As the Access tab represents a history, the state column only knows the following three states:

- **State** column
  - deliver** - mail has been delivered successfully
  - ⚠ **giveup** - mail could not be delivered / mail has been discarded by admin command
  - 💣 **crash** - an error has occurred during delivery or internal operation

Furthermore, the following column pays regard to handling of suspicious and malicious attachments:

- **Stripped** column
 

A mail object is tagged with a pair of scissors ✂, if a spam suspicious or malicious virus attachment has been removed from it.

**Note:**

All attachments will be cut out from an e-mail containing multiple attachments, if only one of them is classified as suspicious file because it cannot be scanned. The virus scanner does not generate information, which of the files is the suspicious one. If of interest, a manual scan is necessary, after all attachments have been downloaded. For a definition of suspicious files, please see Delete All Suspicious Attachments ..., page 267 below.

### 5.4.1 Context Menu Entries

**Note:**

Execution of the commands made available through the context menu requires adequate permissions.

Right-clicking a group title makes the following context menu entries available:

- **Delete Items in Category ...**

Deletes all access entries from the selected category Spam State Unknown, Spam or No Spam.

**Note:**

This action does not automatically delete possibly cut attachments from the Attachments tab.

Right-clicking any data set makes the following context menu entries available:

- **Show Logfile / Show Envelope**

see 5.3.1 Context Menu Entries, page 264
- **Remove Entry**

Removes the selected data set (or multiple data sets if selected).
- **Clear All**

Deletes all objects from the Access tab.

Right-clicking a data set flagged with ✂ in the **Attachment Stripped** column makes the following additional option available:

- **Show Stripped Attachments ...**

Clicking this item redirects the administrator to the attachment(s) cut from the mail object, now located for analysis in the **Attachments** tab (see 5.7 Attachments Tab, page 266).

## 5.5 Spam Tab

This tab combines **Mail Queue** and **Access** tab and only displays spam tagged e-mails. As this tab serves informational purpose only, the context menu has no tools for modification/deletion of entries. The only available actions from the context menu are:

- **Show Envelope ...**

opens a view containing basic information concerning the select mail (for example mail size, peer IP address, sender, ...)
- **Show Log File ...**

opens a view containing all log files that were created by the selected mail

**Note:**

The columns building the spam list/spam tab can be interpreted in the same way like the ones used in the Mail Queue Tab (page 263) and Access Tab (page 265).

## 5.6 Processes Tab

The **Processes** register shows the active mail gateway processes. When a multitude of processes is running, use the filter options **Delivery**, **Receiving**, and **Internal** in the filter section area, to limit the amount of processes shown.

### Note:

Internal processes are not shown by default. Adapt the filter setting for **Internal** to display them.

Information on currently active processes covers the following:

- **PID** column  
Shows the **Process ID**entifier.
- **State** column  
Processes can have the following states:
  - **pause** (only available with type **mgw\_main**)
  - **active**
- **Type** column  
The following process types exist:
  - mgw\_main** - This is the parent process of the phion netfence mail gateway service. It provides the SMTP listening sockets and handles the mail receiving processes (SMTP worker processes).
  - qspool\_main** - This process listens for incoming connections from a remote host running the phion netfence administration GUI phion.a.
  - qspool\_worker** - This process is responsible for transferring the visualisation data (Mail Queue, Access Cache, Processes, Logs, Stats ...) to the remote host running the phion netfence administration GUI phion.a.
  - SMTP worker** - This temporary process is activated when a client opens a SMTP connection to the mail gateway. The SMTP worker process is responsible for receiving mail data from the client. It terminates when mail data transfer has ended.
  - spooler** - The spooler process is responsible for scheduling mail jobs. When the Worker Process receives a mail job, its state temporarily changes to **spool**. While it is in this state, the mail job is visualised in the Mail Queue tab. The mail queue becomes larger with every mail job getting spooled. The sequence, by which the spooled items are worked off, is handled by the Spooling Priority.
  - mta** (Mail Transfer Agent) - This process is responsible for mail delivery. When the MTA process receives a mail job from the spooler, it establishes a connection to a foreign target mail server (the mail job's recipient mail server) and delivers the e-mail. After successful delivery, the mail job moves from the Mail Queue to the Access Cache.
  - ha** (High Availability) - This process is needed for synchronising mail traffic between HA partners.
- **Peer** column  
Shows peer IP and port handled by a SMTP or qspool worker.
- **Spool ID** column  
Shows the spool ID of the mail being processed by a Mail Transfer Agent (MTA).

### 5.6.1 Context Menu Entries

#### Note:

Execution of the commands made available through the context menu requires adequate permissions.

Right-clicking a data set makes the following context menu entries available:

#### ➤ **Kill Process**

With administrative permissions single worker processes can be killed. MTA processes are automatically created on demand until the configured maximum number of MTAs has been reached (see Mail Transfer Agents (MTAs), page 250).

#### Note:

Killing a worker process triggers the event **Subprocess Kill Requested: Kill PROC\_SMTP Worker [2054]** when eventing is activated through parameter **Kill Worker Process** (see page 256) (default: no).

#### ➤ **Allow Mail Reception**

Used to resume mail operation after blocking mail reception.

#### ➤ **Block Mail Reception**

Used to block the mail gateway process.

## 5.7 Attachments Tab

The Attachments tab assembles cut e-mail attachments. Its listing arranges mail objects sorted ascending by their Spool ID. Cut attachments are directly assigned to the object they have been cut from.

Use this operative area to decide individually how to proceed with suspicious or malicious files.

#### Note:

File types meant to be cut from e-mails and not forwarded to their recipients are on the one hand defined through the virus scanner (**Anti-Virus**, page 367) and on the other hand specifically appointed through the mail gateway settings (see Section Attachment Stripping, page 253).

Available information is arranged in the following columns:

#### ➤ **Spool**

This column shows the e-mail's spool ID and behind it in brackets the number of attachments which has been cut from it. Click on the **+** symbol to display detail information regarding the attachments.

#### ➤ **From**

Shows the sender address.

#### ➤ **To**

Shows the recipient(s) address(es).

#### ➤ **Subject**

Shows the mail object's subject.

#### ➤ **Receive Time**

Shows the time the message has been arrived at the mail gateway.



- **Filename**  
Shows the name of the file, which has been cut.
- **Reason**  
Displays the reason why the file has been cut.

### 5.7.1 Context Menu Entries

Right clicking any data set makes the following context menu entries available:

- **Delete All Attachments ...**  
Deletes all attachments from all mail objects currently assembled in the listing regardless of the reason why they have been cut.
- **Delete All Normal Attachments ...**  
If the mail gateway has been configured to cut all file attachments regardless of their type (see Section Attachment Stripping, page 253), they will be contained in this tab. This action deletes all mail attachments, which have been stripped off according to mail gateway settings.
- **Delete All Suspicious Attachments ...**  
Deletes all file attachments, which have been classified as suspicious by the virus scanner. Files are classified as suspicious when the virus scanner for any reason is not able to handle them properly. Amongst others, the following can be causes for this:
  - The file attachment is larger than 1 MB and thus cannot be scanned completely.
  - The file attachment is encrypted.
  - The file attachment is an archive file exceeding the maximum allowed archive size.
- **Delete All Virus Attachments ...**  
Deletes all malicious file attachments like viruses.

Right-clicking a **Spoof**/ID header makes the following action available:

- **Delete Attachments From This Mail ...**  
Deletes all attachments from the selected mail object.

Right-clicking a selected file object makes the following actions available:

- **Get Attachment**  
Makes the cut attachment available for download. It is up to the respective administrator to download the file to his/her own harddisk, scan the file manually and thereafter possibly forward it to the original recipient.
- **Delete Attachment**  
Deletes the selected file attachment.

## 5.8 Grey Listing Tab

Contents of the Grey Listing tab are associated with Grey Listing set to **enabled** in the Mail Gateway settings (Section Grey Listing, page 253). The list summarises e-mail delivery attempts, which have reached the gateway.

The Grey Listing tab is subdivided into two areas, a Grey List and a White List.

### 5.8.1 Grey List

Data sets in the Grey List are arranged in sections disclosing the e-mails' arrival time. E-mails are classified into the following categories:

- **Newer than 1 hour**
- **Between 1 and 12 hours**
- **Older than 12 hours**

Objects in the first category **Newer than 1 hour** are subject to a greater movement. Sender-recipient pairs are removed from the grey list with the following successful delivery attempt. E-mails which do not experience a second delivery attempt, are successively moved to the lower categories.

The grey list can be used to:

- recognise peers exclusively delivering junk mail. When known, these hosts can be added to the **IP Blacklist** in the Block Filter configuration section (see Section Blacklists, **IP Blacklist**, page 255) thus further reducing unwanted e-mail traffic.
- recognise uncritical sender-recipient pairs whose e-mails could not be delivered due to a misconfigured sender's mail server not attempting a second delivery attempt. When known, these senders and/or hosts can be added to the **White List Peers** and/or **Senders** fields in the Grey Listing configuration section (see Section Grey Listing, **White List Peers**/Senders, page 254) thus excluding the specific servers from Grey Listing.

Available information is arranged in the following columns:

- **Sender**  
Shows the sender's e-mail address.
- **Receiver**  
Shows the recipient's e-mail address.
- **Peer IP**  
Shows the IP address of the sending mail server.
- **Peer Hostname**  
Shows the delivering mail server's hostname, if its name is DNS resolvable. Otherwise the field will contain the string **unknown**.
- **Count**  
This is the number of counted delivery attempts. Multiple unsuccessful delivery attempts might occur when the sending mail server retries delivery before Grey Listing Time expiration (see Grey Listing Time (Min)).
- **First Try**  
This is the time of the first delivery attempt.
- **Last Try**  
This is the time of the last delivery attempt.
- **All Tries**  
This is the sum of all delivery attempts. Multiple delivery tries may possibly occur, if a successional delivery attempt under-runs the **Grey Listing Time (Min)** (page 254).

Grey Listing entries **Older than 12 hours** are automatically deleted after 1 day.

## 5.8.2 White List

Contents of the White List are associated with parameter Auto White List (Senders) set to **yes** in the Mail Gateway settings (Section Grey Listing, page 253). The list contains all e-mail senders whose e-mails have been delivered successfully and which have been added to the temporary White List automatically.

Available information is arranged in the following columns:

- **Sender**  
Shows the sender's e-mail address.
- **Listed Since**  
Shows the date when the e-mail address has been added to the White List.

## 5.8.3 Context Menu Entries

Data sets in the White List are deleted automatically according to the interval, which is defined through parameter Remove from White List after (d) (page 254).


Manual deletion is possible through the following context menu entries available through right clicking any data set:


- **Remove**  
Deletes the selected entry from the list.
- **Clear List**  
Deletes all entries from the list.

## 5.9 Logs, Statistics, Events

### 5.9.1 Logs


#### Note:


For general information on the  **Logs** feature of phion netfence phion.a see **Log Viewer**, page 289.

Select  **Logs** on the phion.a toolbar and select the server your mail gateway service is installed on. Then double-click the mail gateway service name. Now you can access the logs of the mail gateway service.

### 5.9.2 Statistics

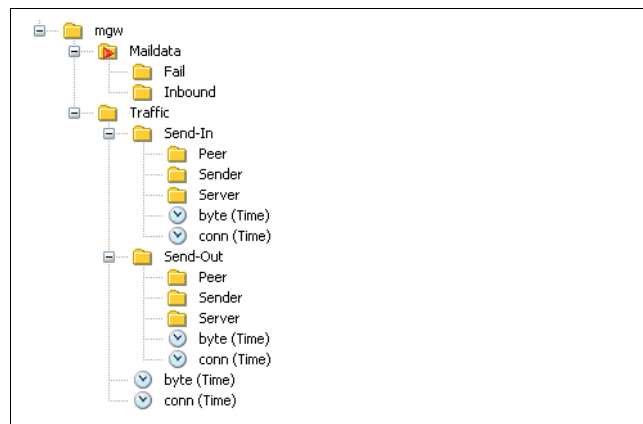
#### Note:

For general information on the  **Statistics** feature of phion netfence phion.a see **Statistics**, page 295.

Select  **Statistics** on the phion.a toolbar and select the server your mail gateway service is installed on.

Then double-click the mail gateway service name. Now you can choose between various types of statistics you can specify in Section Statistic Settings (page 256).

Fig. 6-13 Statistics tree



#### ➤ **Maildata**

These statistics visualise only bulk mail data without the SMTP protocol overhead.

There are three subtypes:

**Inbound** - successful inbound MTA delivery of a pair (sender, recipient)

**Outbound** - successful outbound MTA delivery of a pair (sender, recipient)

**Fail** - failed MTA delivery

#### ➤ **Traffic**

These statistics visualise total mail traffic with SMTP protocol overhead.

There are several subtypes:

**Receive-In** - Inbound SMTP receive traffic (SMTP Worker Processes)

**Receive-Out** - Outbound SMTP receive traffic (SMTP Worker Processes)

**Send-In** - Inbound MTA traffic

**Send-Out** - Outbound MTA traffic

**byte (Time)** and **conn (Time)** reflect total mail traffic without separation of peer/sender/server.


#### 5.9.2.1 Samples for Frequently Used Statistics

- How many mails have been sent out totally since ...?  
**Traffic** > **Send out** > **Conn (Time)** > Top list for time interval > select time interval you wish to be visualised
- How many mails have been received from outside totally since ... ?  
**Traffic** > **Receive out** > **Conn (Time)** > Top list for time interval > select time interval you wish to be visualised
- Who of my users has sent most mails?  
**Maildata** > **Outbound** > **Conn (Top Src)** > select instances from top list

### 5.9.3 Events

**Note:**

For general information on the events feature of phion.a see **Eventing**, page 305.

Select  **Events** on the phion.a toolbar. You may customize event notification by the mail gateway, as outlined in **Section** Event Settings (page 256). Triggered events are shown in the Events window.

## 6. E-mail Synchronisation after HA Handover

### 6.1 Automatic Synchronisation

For a detailed description about automatic synchronisation procedure see **High Availability**, page 375.

### 6.2 Manual Synchronisation

For a detailed description about manual synchronisation procedure see **High Availability**, page 375.



# DHCP

<b>1.</b>	<b>DHCP Enterprise</b>	
1.1	Overview .....	272
1.2	Working Principles & Process Structure .....	272
1.3	Configuration .....	273
1.3.1	Operational Setup .....	273
1.3.2	Address Pools .....	273
1.3.3	Known Clients .....	275
1.3.4	DHCP Option Templates .....	276
1.3.5	Parameter Templates .....	277
1.3.6	Classes .....	278
1.3.7	Dynamic DNS .....	278
1.3.8	GUI as Text .....	279
1.3.9	Text Based Configuration .....	279
1.4	Realtime Information .....	279
1.5	Example .....	280
<b>2.</b>	<b>"Regular" DHCP</b>	
2.1	Overview .....	282
2.2	Configuration .....	282
2.2.1	DHCP Server Settings .....	282
2.2.2	Global Settings .....	283
2.2.3	IP-Ranges .....	283
2.2.4	Special Clients .....	283
2.2.5	Options .....	283
2.3	Real Time Information .....	284
<b>3.</b>	<b>DHCP Relay Agent</b>	
3.1	DHCP Relay Settings .....	286
3.1.1	Cascading DHCP Relay Agent .....	287

# 1. DHCP Enterprise

## 1.1 Overview

The **D**ynamic **H**ost **C**onfiguration **P**rotocol is used for assigning IP addresses automatically.

The DHCP server has a given amount of so-called **leases**. These leases are IP addresses that are available for being "lent" to an interface. After a predefined amount of time, the client sends a request to the server whether it may keep the lease or not.

**Note:**

DHCP and the DHCP Relay Agent have been implemented according to the following RFCs:

- RFC 1497 (RFC 951)
- RFC 2131
- RFC 2132
- RFC 3046

The work flow consists of the following steps:

### Step 1 Discover

As soon as a client connects to the network to contact any reachable DHCP server (source IP: 0.0.0.0; destination IP: 255.255.255.255). This message includes the MAC address of the client. Thus the server(s) know where the request is coming from.

### Step 2 Offer

After receiving the discover message, the server(s) offers a lease to the client.

A lease consists of:

#### ➤ IP address

- The client gets an IP address out of a defined available IP range
- When the client's MAC address is defined within the class/know clients configuration this explicit IP address will be used

#### ➤ Options

These options define the subnetmask, the gateway, ...

### Step 3 Selection & Request

The client checks the received lease-offers and selects one.

**Note:**

The selection depends on the client configuration, but usually the lease received first is selected.

Now the client sends a request for the lease to the DHCP server that offered it.

### Step 4 Acknowledgement

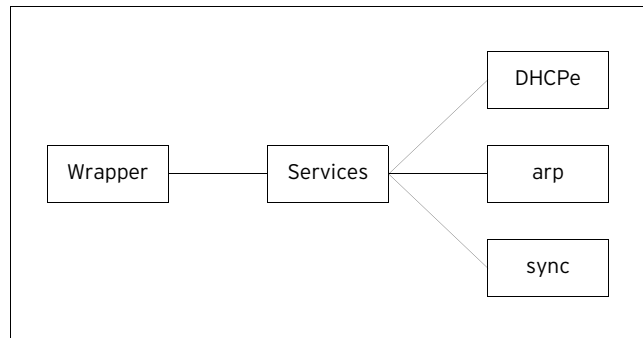
When the lease is still available the DHCP server sends an ACK to the client and the client activates the settings of the lease.

## 1.2 Working Principles & Process Structure

The process structure of the novel DHCPe server is presented in figure 7-1 Processes structure. In brief, five different processes are involved, which are:

- **Wrapper:** Responsible for finding available services
- **Services:** Takes care of looking for the DHCP server
- **DHCPe:** Represents the DHCP enterprise server
- **arp:** Takes care of sending arps every 10 seconds to all the clients accessible in the direct net
- **sync:** Responsible for the synchronisation among HA boxes

Fig. 7-1 Processes structure



All these processes use one unique log file named `server/serviceName` following the convention.

**Note:**

The DHCP Enterprise service does not replace the former phion DHCP-Server, although only one of them may run on the same box. New licenses are not required for the DHCP service to be fully recognised.



### 1.3 Configuration

Configuring DHCP Enterprise on a netfence gateway starts with introducing a corresponding DHCP service. Therefore select **Config** from the box menu and introduce the service by selecting **Create Service ...** from the context menu of **Assigned Services**.

**Note:**

Please see **Configuration Service - 4. Introducing a New Service**, page 97, for detailed information concerning the procedure and available options.

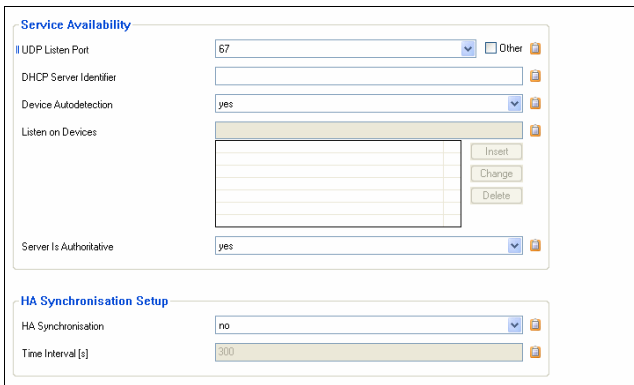
After the service has been created, the following two configuration entries are available in the config tree:

- ➔ **Dhcp Enterprise Configuration** - see below
- ➔ **Service Properties** - settings made during the introduction of the service

Enter the configuration dialogue via **Config > Box > Virtual Servers > <servername> > Assigned Services > <servicename> (dhcpe) > DHCP Enterprise Configuration**.

#### 1.3.1 Operational Setup

Fig. 7-2 DHCP Enterprise Configuration - Operational Setup



List 7-1 DHCP Enterprise Configuration - Operational Setup - section Service Availability

Parameter	Description
<b>UDP Listen Port</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. This parameter causes the DHCP server to listen for DHCP requests on the UDP port specified in port, rather than on default port 67.
<b>DHCP Server Identifier</b>	This parameter can be used to inform the client about the name of the server from which it is booting and should be the name that will be provided to the client.
<b>Device Autodetection</b>	Here the automatic detection of listening interfaces is activated/deactivated (default: <b>yes</b> ). Setting the parameter to no, activates parameter <b>Listen on Devices</b> (see below).
<b>Listen on Devices</b>	This parameter is only available, if the parameter <b>DHCP Server Identifier</b> is set to <b>no</b> . It allows specifying the listening interfaces explicitly.

List 7-1 DHCP Enterprise Configuration - Operational Setup - section Service Availability

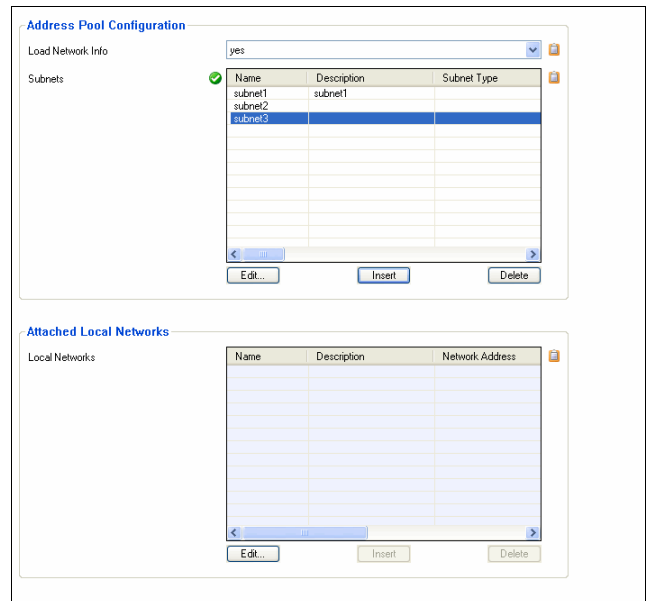
Parameter	Description
<b>Server Is Authoritative</b>	When the DHCP server receives a <b>DHCPREQUEST</b> message from a DHCP client requesting a specific IP address, the DHCP protocol requires that the server determines whether the IP address is valid for the network to which the client is attached or not. If the address is not valid, the DHCP server should respond with a <b>DHCPNAK</b> message, forcing the client to acquire a new IP address. To make this determination for IP addresses on a particular network segment, the DHCP server must have complete configuration information for that network segment. Unfortunately, it is not safe to assume that DHCP servers are configured with complete information. Therefore, the DHCP server normally assumes that it does not have complete information, and thus is not sufficiently authoritative to safely send <b>DHCPNAK</b> messages as required by the protocol.

List 7-2 DHCP Enterprise Configuration - Operational Setup - section HA Synchronisation Setup

Parameter	Description
<b>HA Synchronisation</b>	Setting this parameter to <b>yes</b> causes the periodical synchronisation of the DHCP database between the HA pair (default: <b>no</b> ).
<b>Time Interval [s]</b>	This parameter defines the period between synchronisation tasks (default: <b>300</b> )

#### 1.3.2 Address Pools

Fig. 7-3 DHCP Enterprise Configuration - Address Pools



List 7-3 DHCP Enterprise - Address Pool Configuration - section Address Pool Configuration

Parameter	Description
<b>Load Network Info</b>	This parameter activates/deactivates the automatic search for local networks (default: <b>yes</b> ).

List 7-4 DHCP Enterprise - Address Pool Configuration - section Subnets

Parameter	Description
<b>Description</b>	Here a describing text concerning the subnet can be entered.
<b>Shared Network Device</b>	This parameter defines whether the subnet is a shared one (default: <b>no</b> ). If an interface is to be shared (by setting to <b>yes</b> ) parameter <b>DHCP Enterprise - Address Pool Configuration - section Further Subnets</b> (see below) is activated.
<b>Shared Parameters</b>	Here the parameters for the shared network can be choosen.
<b>Shared DHCP Options</b>	Here the DHCP options for the shared network can be choosen.

List 7-4 DHCP Enterprise - Address Pool Configuration - section Subnets

Parameter	Description
<b>Subnet Type</b>	Defines the type of subnet. The following options are available: <b>local</b> (default) - activates parameter <b>Used Subnet</b> for selecting the required subnet <b>relayed / explicit</b> - activates parameters <b>Network Address</b> and <b>Netmask</b> for entering the required network.
<b>Used Subnet</b>	Here the required subnet has to be selected.
<b>Network Address</b>	Here the network address has to be entered.
<b>Netmask</b>	Here the network mask has to be entered.
<b>Server IP</b>	This parameter can be used to define the value that is sent for a given scope. The value specified must be an IP address for the DHCP server and must be reachable by all clients served by a particular scope. The usual case where the Server IP needs to be sent is when a physical interface has more than one IP address, and the one being sent by default isn't appropriate for some or all clients served by that interface. Another common case is when an alias is defined for the purpose of having a consistent IP address for the DHCP server, and it is desired that the clients use this IP address when contacting the server.
<b>Server Is Authoritative</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  When the DHCP server receives a <b>DHCPREQUEST</b> message from a DHCP client requesting a specific IP address, the DHCP protocol requires that the server determine whether the IP address is valid for the network to which the client is attached. If the address is not valid, the DHCP server should respond with a <b>DHCPNAK</b> message, forcing the client to acquire a new IP address. To make this determination for IP addresses on a particular network segment, the DHCP server must have complete configuration information for that network segment. Unfortunately, it is not safe to assume that DHCP servers are configured with complete information. Therefore, the DHCP server normally assumes that it does not have complete information, and thus is not sufficiently authoritative to safely send <b>DHCPNAK</b> messages as required by the protocol.
<b>Perform DDNS Updates</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  This parameter offers the following options: <ul style="list-style-type: none"> <li>➤ <b>true</b> - activates DNS parameter updates for subnets (parameter <b>DNS Zone</b> is activated)</li> <li>➤ <b>false</b> - deactivates DNS parameter updates for subnets</li> <li>➤ <b>not-set</b> (default) - enforces global DNS parameter to be used for subnets</li> </ul>
<b>DNS Zone</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.  If parameter <b>Perform DDNS Updates</b> is set to <b>true</b> , here the updating DNS zones (configured within <b>Dynamic DNS</b> , see 1.3.7 Dynamic DNS, page 278) are defined.
<b>Subnet Parameters</b>	Here the parameters for these subnets can be chosen. The available parameters are configured within <b>Parameter Templates</b> (see 1.3.5 Parameter Templates, page 277).
<b>Subnet DHCP Options</b>	Here the options for these subnets can be chosen. The available options are configured within <b>DHCP Option Templates</b> (see 1.3.4 DHCP Option Templates, page 276).
<b>Address Pools</b>	see list 7-6

List 7-5 DHCP Enterprise - Address Pool Configuration - section Multi Subnet Configuration

Parameter	Description
<b>Shared Network Device</b>	<b>Note:</b> This parameter set is only available in <b>Advanced View</b> mode.  Set this to <b>yes</b> if the determination of subnets should be used. This way it is possible to have multiple subnets on one device.

List 7-5 DHCP Enterprise - Address Pool Configuration - section Multi Subnet Configuration

Parameter	Description
<b>Shared Parameters</b>	Here the parameters for the shared network device can be chosen. The available parameters are configured within <b>Parameter Templates</b> (see 1.3.5 Parameter Templates, page 277)
<b>Shared DHCP Options</b>	Here the options for the shared network device can be chosen. The available options are configured within <b>DHCP Option Templates</b> (see 1.3.4 DHCP Option Templates, page 276)
<b>Further Subnets</b>	see list 7-7

List 7-6 DHCP Enterprise Configuration - SUBNETS tab - section Address Pools

Parameter	Description
<b>Pool description</b>	description of the pool
<b>Range DHCP Options</b>	defines DHCP options available for the range
<b>IP Begin</b>	start IP of the range
<b>IP End</b>	end IP of the range
<b>All Clients Policy</b> [default: none]	defines the policy that is to be used; <ul style="list-style-type: none"> <li>➤ <b>none</b> - no global policy is used; enforces usage of policy defined in parameters <b>Known Clients</b>, <b>Unknown Clients</b>, <b>Allowed Classes</b>, and <b>Denied Classes</b></li> <li>➤ <b>allow</b> - all pool-matching policies are set to allow (valid for all clients, that are known and unknown)</li> <li>➤ <b>deny</b> - all pool-matching policies are set to deny (valid for all clients, that are known and unknown)</li> </ul>
<b>entegra Clients Policy</b> [none]	defines the policy that is to be used; enforces usage of policy defined in parameters <b>Known Clients</b> and <b>Unknown Clients</b> (see below <b>none</b> - no entegra Clients Policy is used; ) <b>phion entegra-clients</b> - the phion-NAP-clients receive a IP address from the pool <b>guests</b> - phion-NAP-clients are excluded from this pool;
<b>Allowed Classes</b>	defines the classes that are allowed to get leases from this pool; see 1.3.6 Classes, page 278
<b>Denied Classes</b>	defines the classes that are NOT allowed to get leases from this pool; see 1.3.6 Classes, page 278
<b>Known Clients</b> [allow]	<b>allow</b> - known clients may obtain a lease from this pool <b>deny</b> - known clients may NOT obtain a lease from this pool <b>not-set</b> - deactivates the parameter
<b>Unknown Clients</b> [deny]	<b>allow</b> - unknown clients may obtain a lease from this pool <b>deny</b> - unknown clients may NOT obtain a lease from this pool <b>not-set</b> - deactivates the parameter
<b>BOOTP Clients Policy</b> [deny_dynamic]	Use the dynamic-bootp flag to tell the DHCP server to dynamically assign addresses to bootp clients or to not do so. <b>allow_dynamic</b> - dynamic BOOTP for IP addresses allowed <b>deny_dynamic</b> - dynamic BOOTP for IP addresses denied <b>not-set</b> - deactivates the parameter

List 7-7 DHCP Enterprise - Address Pool Configuration - section Further Subnets

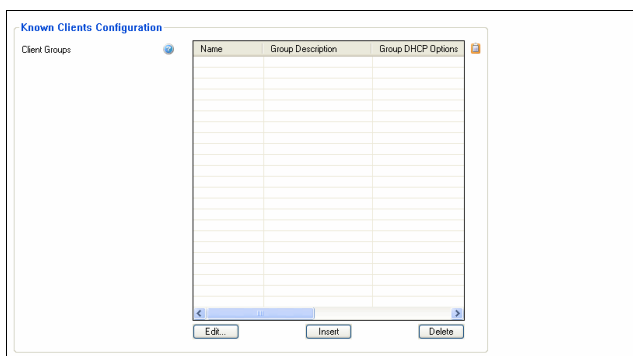
Parameter	Description
<b>Subnet Description</b>	This parameter is only available if parameter <b>Shared Network Device</b> (see above) is set to <b>yes</b> and allows determination of subnets using this interface. This way it is possible to have multiple subnets on ONE interface.
<b>Subnet Description</b>	Description of the subnet
<b>Subnet Type</b> [default: local]	Defines the type of subnet. The following options are available: <b>local</b> (default) - activates parameter <b>Used Subnet</b> for selecting the required subnet <b>relayed / explicit</b> - activates parameters <b>Network Address</b> and <b>Netmask</b> for entering the required network
<b>Used Subnet</b>	Here the required subnet has to be selected.
<b>Network Address</b>	Here the network address has to be entered.

**List 7-7** DHCP Enterprise - Address Pool Configuration - section Further Subnets

Parameter	Description
<b>Netmask</b> [8-bit]	Here the network mask has to be entered.
<b>Server IP</b>	This parameter can be used to define the value that is sent for a given scope. The value specified must be an IP address for the DHCP server, and must be reachable by all clients served by a particular scope. The usual case where the Server IP needs to be sent is when a physical interface has more than one IP address, and the one being sent by default isn't appropriate for some or all clients served by that interface. Another common case is when an alias is defined for the purpose of having a consistent IP address for the DHCP server, and it is desired that the clients use this IP address when contacting the server.
<b>Server Is Authoritative</b> [yes]	When the DHCP server receives a <b>DHCPREQUEST</b> message from a DHCP client requesting a specific IP address, the DHCP protocol requires that the server determines whether the IP address is valid for the network to which the client is attached. If the address is not valid, the DHCP server should respond with a <b>DHCPNAK</b> message, forcing the client to acquire a new IP address. To make this determination for IP addresses on a particular network segment, the DHCP server must have complete configuration information for that network segment. Unfortunately, it is not safe to assume that DHCP servers are configured with complete information. Therefore, the DHCP server normally assumes that it does not have complete information, and thus is not sufficiently authoritative to safely send <b>DHCPNAK</b> messages as required by the protocol.
<b>Perform DDNS Updates</b> [not-set]	This parameter offers the following options: <b>true</b> - activates DNS parameter updates for subnets (parameter <b>DNS Zone</b> is activated) <b>false</b> - deactivates DNS parameter updates for subnets <b>not-set</b> (default) - enforces global DNS parameter to be used for subnets
<b>Subnet Parameters</b>	Here the parameters for these subnets can be chosen. The available parameters are configured within <b>Parameter Templates</b> (see 1.3.5 Parameter Templates, page 277).
<b>Subnet DHCP Options</b>	Here the options for these subnets can be chosen. The available options are configured within <b>DHCP Option Templates</b> (see 1.3.4 DHCP Option Templates, page 276).

### 1.3.3 Known Clients

**Fig. 7-4** DHCP Enterprise Configuration - Known Clients



**List 7-8** DHCP Enterprise Configuration - Known Clients - section Group Based Assignment

Parameter	Description
<b>Group Description</b>	May hold a further description concerning the group.
<b>Group DHCP Options</b>	Defines the DHCP options that are available for this group.
<b>Group Parameters</b>	Defines the DHCP parameters that are available for this group.
<b>Automatic Hostname Assignment</b>	If this parameter is set to <b>true</b> (default: <b>false</b> ) then for every host declaration of this group of known clients, the name provided for host declaration will be supplied to the client as its hostname.

**List 7-8** DHCP Enterprise Configuration - Known Clients - section Group Based Assignment

Parameter	Description
<b>Known Clients</b>	see list 7-9

### Section *Client Group Members*

**List 7-9** DHCP Enterprise - Known Clients - Client Group Member - section Client Description

Parameter	Description
<b>Client Description</b>	description of the client

**List 7-10** DHCP Enterprise - Known Clients - Client Group Member - section Client Match & Address Assignment

Parameter	Description
<b>DHCP Client Identifier</b>	Host declarations are matched to actual DHCP or BOOTP clients by matching the dhcp-client-identifier option specified in the host declaration to the one supplied by the client, or, if the host declaration or the client does not provide a DHCP Client Identifier option, by matching the hardware parameter in the host declaration to the network hardware address supplied by the client. BOOTP clients do not normally provide a dhcp-client-identifier, so the hardware address must be used for all clients that may boot using the BOOTP protocol. Be aware that only DHCP Client Identifier option and hardware address can be used to match a host declaration. For example, it is not possible to match a host declaration to a host-name option. This is because the host-name option cannot be guaranteed to be unique for any given client, whereas both, hardware address and DHCP Client Identifier option, are at least theoretically guaranteed to be unique to a given client.
<b>MAC Address</b> [ff:ff:ff:ff:ff:ff]	defines the MAC address of the client required for identification
<b>MAC Type</b> [ethernet]	defines the type of network card requesting a lease (either <b>ethernet</b> or <b>tokenring</b> )
<b>Fixed IP Address</b>	defines, if required, a static IP address that is sent to the client

**List 7-11** DHCP Enterprise - Known Clients - Client Group Member - section Advanced Client Assignments

Parameter	Description
	<b>Note:</b> This parameter set is only available in <b>Advanced View</b> mode.
<b>Client DHCP Options</b>	defines DHCP options available for the client
<b>Client Parameters</b>	defines DHCP parameters available for the client
<b>Allowed Broadcast Reply</b> [not-set]	DHCP and BOOTP protocols both require DHCP and BOOTP clients to set the broadcast bit in the flags field of the BOOTP message header. Unfortunately, some DHCP and BOOTP clients do not do this, and therefore may not receive responses from the DHCP server. The DHCP server can be configured to always broadcast its responses to clients by setting this flag to <b>yes</b> for the relevant scope; relevant scopes would be inside a conditional statement, as a parameter for a class, or as a parameter for a host declaration. In order to avoid creating excessive broadcast traffic on your network, phion recommends to restrict the use of this option to as few clients as possible.

**List 7-11** DHCP Enterprise - Known Clients - Client Group Member - section Advanced Client Assignments

Parameter	Description
<b>Duplicates Policy</b> [allow]	Choose between one of the settings <i>allow</i> and <i>deny</i> in this place. Host declarations can match client messages based on the DHCP Client Identifier option or based on the client's network hardware type and MAC address. If the MAC address is used, the host declaration will match any client with that MAC address - even clients with different client identifiers. This doesn't normally happen, but is possible when one computer has more than one operating system installed on it - for example, Microsoft Windows and NetBSD or Linux.  This parameter tells the DHCP server that if a request is received from a client matching the MAC address of a host declaration or any other lease matching that MAC address should be discarded by the server, even if the UID is not the same. This is a violation of the DHCP protocol, but can prevent clients whose client identifiers change regularly from holding many leases at the same time.
<b>Client Hostname</b>	If a name is entered, the statement within a host declaration will override the use of the name in the host declaration.
<b>DDNS Hostname</b>	Defines the hostname that will be used in setting up the client's A and PTR records; if no DDNS hostname is specified the server will derive the hostname automatically, using an algorithm that varies for each of the different update methods.

### 1.3.4 DHCP Option Templates

**List 7-12** DHCP Enterprise - DHCP Option Templates - section Template Description

Parameter	Description
<b>Description</b>	May hold a describing text.

**List 7-13** DHCP Enterprise - DHCP Option Templates - section Basic Options

Parameter	Description
<b>Subnetmask [1]</b>	Here the required subnet mask has to be selected (default: not-set).
<b>Router [3]</b>	Here the default address(es) of the default gateway(s) are to be entered.
<b>DNS Servers [6]</b>	Here the IP address(es) of the DNS servers are to be entered.
<b>Domain Name [15]</b>	Here the domain name is to be entered.

**List 7-14** DHCP Enterprise - DHCP Option Templates - section entegra Policy Service Options

Parameter	Description
<b>Policy Service IPs/Names</b>	Here the IP addresses or DNS-resolvable names of the policy services are to be entered.

**List 7-15** DHCP Enterprise - DHCP Option Templates - section Extended Options

Parameter	Description
<b>Vendor [43]</b>	This parameter is used to exchange vendor-specific information. The definition of this information is vendor specific.
<b>Broadcast Address [28]</b>	Here the Broadcast Address can be entered.
<b>NIS Domain Name [40]</b>	Enter the domain of the <b>Network Information System</b> in this field.
<b>NIS Server [41]</b>	Here the IP address(es) of the NIS server(s) are entered.
<b>NTP Server [42]</b>	To enable synchronised times, here the IP address(es) of the NTP server(s) are entered.
<b>WINS Server [44]</b>	When using a WINS server, here the IP address(es) of the server(s) are entered.
<b>NBDD Server [45]</b>	When using a NBDD server, here the IP address(es) of the server(s) are entered.

**List 7-15** DHCP Enterprise - DHCP Option Templates - section Extended Options

Parameter	Description
<b>Netbios Node Type [46]</b>	<b>Note:</b> When using a Linux client this parameter is obsolete and has to left empty.  This entry allows NetBIOS to configure TCP/IP clients. The following values are available (with their indication): <b>not-set</b> (default) <b>b-node</b> broadcast; like clients use broadcast for name registration/resolution <b>p-node</b> point; like client registers itself at the netbios server (point-to-point) <b>m-node</b> multi; like client first uses b-node, if it fails p-node is used <b>Note:</b> However, b- and m-nodes should not be used with large networks because the broadcasts use lots of bandwidth. <b>h-node</b> hybrid; like m-node, but uses p-node first and then b-node (as a last resort)
<b>Netbios Scope Id [47]</b>	<b>Note:</b> When using a Linux client, this parameter is obsolete and must be empty.  When using NetBIOS Scope IDs (for example, for isolating NetBIOS traffic or for giving the same name to different computers), here this ID is to be entered. <b>Note:</b> The NetBIOS Scope ID is case-sensitive.
<b>LPR Server [9]</b>	When using this printing protocol for Unix systems, here the IP address of the printer has to be entered.
<b>Log Server [7]</b>	In case of a stand-alone log server, here the IP address of the server has to be entered.
<b>Time Server [4]</b>	In case of a time server according to RFC868, here the IP address of this server has to be entered.
<b>Time Offset [2]</b>	This field defines the client's time offset (in seconds) from UTC.
<b>IEN Name Server [5]</b>	In case of a IEN name server, here the IP address of this server has to be entered.
<b>Cookie Server [8]</b>	When using a stand-alone cookie server, here the IP address of this server has to be entered.
<b>Swap Server [16]</b>	When using a separate swap server, here the IP address of this server has to be entered.
<b>Local Subnets [27]</b>	In case of local subnets, they are selected in this field (default: <b>not-set</b> ).
<b>Impress Server [10]</b>	This field defines the IP address of an optional image impress server.
<b>Resource Location Server [11]</b>	This option specifies a list of RFC 887 Resource Location servers available to the client. Servers should be listed in order of preference.
<b>Perform Mask Discovery [29]</b>	<b>Note:</b> When using a Linux client, this parameter is not supported.  This field defines whether a subnet mask discovery is carried out or not. The following settings are available: <b>true</b> - Client uses ICMP for subnet mask discovery <b>false</b> - No subnet mask discovery is to be performed <b>not-set</b> (default) - deactivates the parameter
<b>Perform Router Discovery [31]</b>	<b>Note:</b> When using a Linux client, this parameter is not supported.  This field defines whether a router discovery is carried out or not. The following settings are available: <b>true</b> - Client performs ICMP router discovery (according to RFC1256) <b>false</b> - No router discovery is to be performed <b>not-set</b> (default) - deactivates the parameter
<b>Static Route Net [33]</b>	Use this option to specify a list of static routes that the client should install in its routing cache. If there are multiple routes to the same destination, you should list them in descending order of priority. The routes are made up of IP address pairs. The first address is the destination address; the second address is the router for the destination. The default route (0.0.0.0) is an illegal destination for a static route. Use the <b>Router [3]</b> parameter to specify the default route. The following options are available: <b>Static Route Net [33]</b> <b>Static Route GW [33]</b>



List 7-15 DHCP Enterprise - DHCP Option Templates - section Extended Options

Parameter	Description
<b>TFTP Server Name [66]</b>	This option is used for identifying a TFTP server when the "sname" field in the DHCP header has been used for DHCP options.
<b>Option150</b>	This parameter is to hand out IP address leases and specify the TFTP option 150 for VoIP phones.
<b>Boot File Name [67]</b>	This option is used for identifying a boot file when the "file" field in the DHCP header has been used for DHCP options.

### 1.3.5 Parameter Templates

List 7-16 DHCP Enterprise - Parameter Templates - section Template Description

Parameter	Description
<b>Description</b>	May hold a describing text.

List 7-17 DHCP Enterprise - Parameter Templates - section Lease Constraints

Parameter	Description
<b>Max Lease Time [s]</b>	Maximum length in seconds that will be assigned to a lease. The only exception to this is that Dynamic BOOTP lease lengths, which are not specified by the client, are not limited by this maximum.
<b>Def Lease Time [s]</b>	Default length in seconds that will be assigned to a lease.
<b>Min Lease Time [s]</b>	Minimum length in seconds that will be assigned to a lease.
<b>Reply Delay [s]</b>	Minimum number of seconds since a client began trying to acquire a new lease before the DHCP server will respond to its request. The number of seconds is based on what the client reports, and the maximum value that the client can report is 255 seconds. Generally, setting this to one will result in the DHCP server not responding to the client's first request but always responding to its second request. This parameter can be used to set up a secondary DHCP server which never offers an address to a client until the primary server has been given a chance to do so. If the primary server is down, the client will bind to the secondary server, but otherwise clients should always bind to the primary.  <b>Note:</b> This does not, by itself, permit a primary server and a secondary server to share a pool of dynamically-allocatable addresses.

List 7-18 DHCP Enterprise - Parameter Templates - section Dynamic DNS Parameters

Parameter	Description
<b>Do Fwd Updates</b>	This parameter instructs the DHCP server whether it should attempt to update a DHCP client's A record if the client acquires or renews a lease. This statement has no effect unless DNS updates are enabled and ddns-update is set to interim. If this statement is used to disable forward updates, the DHCP server will never attempt to update the client's A record, and will only ever attempt to update the client's PTR record if the client supplies an FQDN (Fully Qualified Domain Name) that should be placed in the PTR record using the fqdn option. If forward updates are enabled, the DHCP server will still honour the setting of the client-updates flag (default: <b>not-set</b> ).
<b>Optimised Updates</b>	If this parameter is false for a given client, the server will attempt a DNS update for that client each time the client renews its lease, rather than only attempting an update when it appears to be necessary. This will allow the DNS to heal from database inconsistencies more easily, but the cost is that the DHCP server must do many more DNS updates. If this parameter is true, the DHCP server will only update when the client information changes, the client gets a different lease, or the client's lease expires (default: <b>false</b> ).

List 7-18 DHCP Enterprise - Parameter Templates - section Dynamic DNS Parameters

Parameter	Description
<b>Update Static Leases</b>	This parameter, if set to <b>true</b> , causes the DHCP server to do DNS updates for clients even if those clients are being assigned their IP address using a fixed-address statement - that is, the client is being given a static assignment. This can only work with the interim DNS update scheme. It is not recommended because the DHCP server has no way to tell that the update has been done, and therefore will not delete the record when it is not in use. Also, the server must attempt the update each time the client renews its lease, which could have a significant performance impact in environments that place heavy demands on the DHCP server (default: <b>false</b> ).
<b>DDNS Domainname</b>	This parameter defines the domain name that will be appended to the client's hostname to form a FQDN (Fully Qualified Domain Name).
<b>Rev DDNS Domainname</b>	The name parameter defines the domain name that will be appended to the client's reversed IP address to produce a name for use in the client's PTR record. By default, this is "in-addr.arpa.", but the default can be overridden here.  The reversed IP address to which this domain name is appended is always the IP address of the client, in dotted quad notation, reversed - for example, if the IP address assigned to the client is 10.17.92.74, then the reversed IP address is 74.92.17.10. So a client with that IP address would, by default, be given a PTR record of 10.17.92.74.in-addr.arpa.
<b>Dynamic BOOTP Lease Time [s]</b>	This parameter is used for setting the length of leases dynamically assigned to BOOTP clients. At some sites, it may be possible to assume that a lease is no longer in use if its holder has not used BOOTP or DHCP to get its address within a certain time period. The period is specified in length as a number of seconds. If a client reboots using BOOTP during the timeout period, the lease duration is reset to length, so a BOOTP client that boots frequently enough will never lose its lease. Needless to say, this parameter should be adjusted with extreme caution.
<b>Boot File Server</b>	Used for specifying the host address of the server from which the initial boot file (specified in the filename statement) is to be loaded. Boot File Server should be a numeric IP address. If no Boot File Server parameter applies to a given client, the DHCP server's IP address is used.
<b>Boot File</b>	This parameter can be used to specify the name of the initial boot file which is to be loaded by a client. The filename should be a filename recognizable to whatever file transfer protocol the client can be expected to use to load the file.

List 7-19 DHCP Enterprise - Parameter Templates - section Miscellaneous Parameters

Parameter	Description
<b>Boot Unknown Clients</b>	<b>true / not-set</b> - clients without host declarations will be allowed to obtain IP addresses, as long as those addresses are not restricted by allow and deny statements within their pool declarations <b>false</b> - clients for whom there is no host declaration will not be allowed to obtain IP addresses
<b>RFC1048 Conformance</b>	Some BOOTP clients expect RFC1048-style responses, but do not follow RFC1048 when sending their requests. You can tell that a client is having this problem if it is not getting the options you have configured for it and if you see in the server log the message "(non-rfc1048)" printed with each BOOTREQUEST that is logged.  If you want to send RFC1048 options to such a client, you can set the always-reply-rfc1048 option in that client's host declaration, and the DHCP server will respond with an RFC-1048-style vendor options field. This flag can be set in any scope, and will affect all clients covered by that scope. <b>true</b> - response in RFC1048-style <b>false</b> - response NOT in RFC148-style <b>not-set</b> (default) - deactivates the parameter
<b>Hostname via Rev-DNS</b>	This parameter is used for telling DHCP whether or not to look up the domain name corresponding to the IP address of each address in the lease pool and use that address for the DHCP hostname option. <b>true</b> - lookup is done for all addresses in the current scope <b>false</b> - no lookups are done <b>not-set</b> (default) - deactivates the parameter

List 7-19 DHCP Enterprise - Parameter Templates - section Miscellaneous Parameters

Parameter	Description
<b>Ping Check</b>	If the DHCP server is considering dynamically allocating an IP address to a client, it first sends an ICMP Echo request (a ping) to the address being assigned. It waits for a second, and if no ICMP Echo response has been heard, it assigns the address. If a response is heard, the lease is abandoned, and the server does not respond to the client. This parameter introduces a default one-second delay in responding to DHCPDISCOVER messages, which can be a problem for some clients. The default delay of one second is configured using parameter <b>Ping Timeout [s]</b> (see below). The ping-check configuration parameter can be used to control checking - if its value is <b>false</b> or <b>not-set</b> (default), no ping check is done.
<b>Ping Timeout [s]</b>	If the DHCP server determined that it should send an ICMP echo request (a ping) because the ping-check statement is true, this parameter allows configuring how many seconds the DHCP server should wait for an ICMP Echo response. If no ICMP Echo response has been received before the timeout expires, it assigns the address. If a response is heard, the lease is abandoned, and the server does not respond to the client.

### 1.3.6 Classes

**Note:**

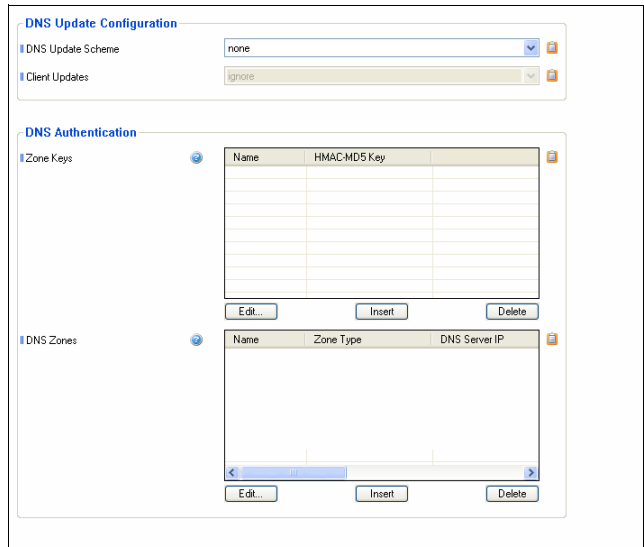
This parameter set is only available in **Advanced View** mode.

List 7-20 DHCP Enterprise - Classes - section Class Configuration

Parameter	Description
<b>Spawn Subclasses</b>	If there are spawn subclasses (default: <b>no</b> ) they have to be specified here.
<b>Spawn Parameter</b>	In case of spawn subclasses (default: <b>n</b> ) their parameter are configured via this parameter.
<b>Lease Limit</b>	This parameter defines the maximum number of parallel active leases.
<b>Match Parameter</b>	<b>Match Parameter</b> (default: <b>dhcp-user-class</b> ) <b>Match Type</b> (default: <b>exact</b> ) - defines the number matching values; that means <b>exact</b> indicates ONE client, <b>list</b> allows multiple client that have to be entered in parameter <b>Match Value List</b> . <b>Match Value</b> - defines the value that has to match (for example, MAC, store agent ID, ...) <b>Match Value List</b> <b>Note:</b> The way MAC addresses are entered depends on the used type of interface: <b>ethernet</b> requires a <b>1:</b> prior to the MAC address (for example <b>1:00:01:f3:34:44:2g</b> ) <b>tokenring</b> requires a <b>6:</b> prior to the MAC address (for example <b>6:00:01:f3:34:44:2g</b> )

### 1.3.7 Dynamic DNS

Fig. 7-5 DHCP Enterprise - Dynamic DNS



**Note:**

This parameter set is only available in **Advanced View** mode.

List 7-21 DHCP Enterprise - Dynamic DNS - section DNS Update Configuration

Parameter	Description
	<b>Note:</b> This parameter set is only available in <b>Advanced View</b> mode.
<b>DNS Update Scheme</b>	Define the <b>DNS Update Scheme</b> with this parameter. Two options are available: ➤ none (default) ➤ interim  The ddns-update-style statement is only meaningful in the outer scope - it is evaluated once after reading the <code>dhcpd.conf</code> file, rather than each time a client is assigned an IP address, so there is no way to use different DNS update styles for different clients.
<b>Client Updates</b>	The first point to understand about this style interim of DNS update is that the DHCP server does not necessarily always update both, the A and the PTR records. The FQDN (fully qualified domain name) option includes a flag which, when sent by the client, indicates that the client wishes to update its own A record. In that case, the server can be configured either to honour the client's intentions or ignore them. This is done with the statement <code>allow client-updates</code> ; or the statement <code>ignore client-updates</code> . By default, client updates are <b>ignored</b> .

List 7-22 DHCP Enterprise - Dynamic DNS - section DNS Authentication

Parameter	Description	
<b>Zone Keys</b>	Here the <b>HMAC-MD5 Key</b> for the dns zone has to be entered.	
<b>DNS Zones</b>	<b>Zone Type</b>	Choose between <b>Forward</b> (default), <b>Reverse</b> and <b>Both</b> .
	<b>DNS Server IP</b>	Enter the DNS Server IP here.
	<b>Forward Zone Name</b>	Holds the network of the forward lookup.
	<b>Reverse Lookup Net</b>	Holds the network of the reverse lookup.
	<b>Reverse Lookup Netmask</b>	Holds the netmask of the reverse lookup.
<b>Authentication Key</b>	Used for selecting a preconfigured (in parameter <b>Zone Keys</b> ) key, configured in Zone Keys.	



### 1.3.8 GUI as Text

**Note:**

This parameter set is only available in **Advanced View** mode.

List 7-23 DHCP Enterprise - GUI as Text

Parameter	Description
<b>Show GUI as Text</b>	Activating this parameter causes that the configuration file sent to the DHCP server is displayed (default: <b>no</b> ).
<b>GUI Corresponding Text</b>	Displays the configuration file of the DHCP server as read-only.

### 1.3.9 Text Based Configuration

**Note:**

This parameter set is only available in **Advanced View** mode.

List 7-24 DHCP Enterprise - Text Based Configuration

Parameter	Description
<b>Use Free Format</b>	Activating this parameter enables manual configuration of the DHCP server (default: <b>no</b> ). <b>Attention:</b> Setting this parameter to <b>yes</b> disables every settings made in the user interface. However, deactivating causes that the settings in the user interface are valid again.
<b>Free Format Text</b>	Here you can write the configuration file.

## 1.4 Realtime Information

The real time information for the configured DHCP server can be accessed via the box menu entry **DHCP**.

Fig. 7-6 Real Time Information - DHCP

IP-Address	State	Start	End	Hostname	Relay-ID	Hardware-Address	Hardware-Type
172.31.1.55	active	2005/11/05 17:46:45	2005/11/06 05:46:45	smart		00:02:55:fa:a0:b9	ethernet
172.31.1.48	active	2005/11/05 18:09:03	2005/11/06 06:09:03			00:10:13:04:44:29	ethernet
172.31.1.50	active	2005/11/05 18:09:10	2005/11/06 06:09:10			00:10:13:04:44:29	ethernet
172.31.1.46	active	2005/11/05 18:45:11	2005/11/06 06:45:11			00:10:13:04:44:2a	ethernet
172.31.1.47	active	2005/11/05 18:47:10	2005/11/06 06:47:10			00:10:13:04:44:2a	ethernet
172.31.1.45	active	2005/11/05 19:14:47	2005/11/06 07:14:47			00:10:13:04:44:2a	ethernet
10.0.70.10	active	2005/11/05 18:03:35	2005/11/06 06:03:35		eth2	00:10:13:04:44:29	ethernet
10.0.70.12	active	2005/11/05 18:03:43	2005/11/06 06:03:43		eth2	00:10:13:04:44:29	ethernet
10.0.70.11	active	2005/11/05 18:03:50	2005/11/06 06:03:50		eth2	00:10:13:04:44:2a	ethernet
10.0.70.13	active	2005/11/05 18:04:03	2005/11/06 06:04:03		eth2	00:10:13:04:44:2a	ethernet
172.31.1.54	active	2005/11/05 20:05:42	2005/11/06 08:05:42			00:10:13:04:44:2d	ethernet
172.31.1.21	active					00:10:48:00:2E:18	ethernet

RANGES			
Range Start	Range End	% Leased	Nr. of Leases
10.0.70.10	10.0.70.15	67	4
172.31.1.45	172.31.1.55	64	7
172.31.1.21	172.31.1.21	0	0

By using the **Delete** button (top left corner) it is possible to delete inactive and relayed leases manually.

**Attention:**

When deleting relayed leases, it may occur that a lease is assigned twice leading to duplicate IPs.

The refresh button (next to **Delete** button) is used for refreshing the display.

The following columns are used for displaying lease status (upper frame):

- **IP-Address** - displays the assigned IP address; additionally the status of the client is displayed by using the following icons:
  - indicating that client is up and running (ARPAble)
  - indicating that client is relayed (not ARPAble)
  - indicating that no client is listening on this IP
- **State** - displays the state of the lease.
- **Start** - displays time of lease assignment; used format: yyyy/mm/dd hh:mm:ss
- **End** - displays when the client has to renew its lease; used format: yyyy/mm/dd hh:mm:ss
- **Hostname** - if available, this column displays the configured hostname the client is assigned to
- **Relay-ID** - if available, this column provides the client's relaying interface
- **Hardware-Address** - displays the client's MAC address
- **Hardware-Type** - displays the client's interface type (**ethernet** or **token ring**)

The following columns are used for displaying **RANGE** status (lower frame):

- **Range Start** - displays the start IP address of the range; additionally, the lease consumption of the range is displayed by using corresponding icon (from ■ ■ ■ ■ ■ - low to high)
- **Range End** - displays the end IP address of the range
- **% Leased** - displays the current lease consumption in this range (in percent)
- **Nr. of Leases** - displays the exact number of leases currently in use in this range

**Note:**

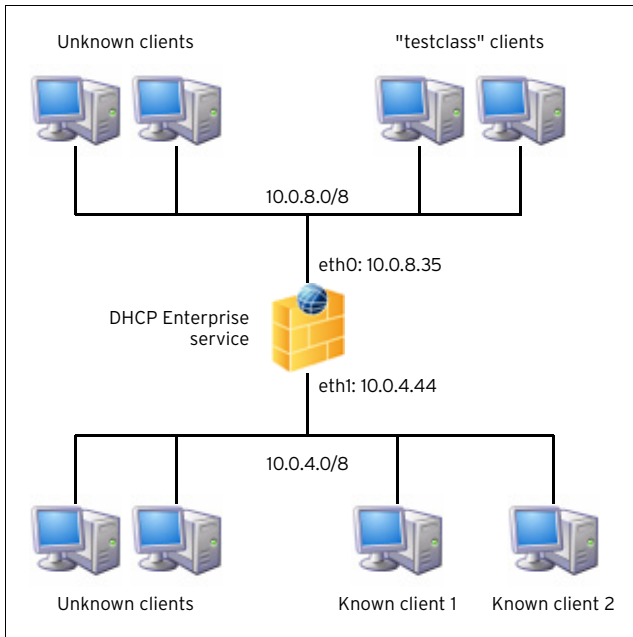
Take into consideration that known clients are displayed in the range status frame (indicated by identical start-/end IP address and value **0** in columns **% Leased** and **Nr. of Leases**). However, this does not indicate that the lease is currently assigned due to not-ARPAble relayed clients.

## 1.5 Example

Create DHCP for 2 networks with 3 different IP pools.

- **network 1** (10.0.8.0/8) - contains two address pools:
  - one pool for unknown clients
  - one pool for known clients (identified via their MAC addresses)
- **network 2** (10.0.4.0./8) - contains one address pool for unknown clients and two known clients

Fig. 7-7 Example environment



**Step 1** Create a DHCP Enterprise server using *FirstIP* 10.0.8.35 and *SecondIP* 10.0.4.44.

**Step 2** Create a DHCP Enterprise service using *First+Second-IP* for *Bind Type*.

**Step 3** Define MAC addresses for "testclass" clients. Change to *Advanced View* mode, enter *Classes* view and add a new class called **testclass**.

Set parameter *Match Type* to **MAC** and enter our ethernet MAC addresses 00:01:f3:34:44:2g and 00:01:f3:34:44:2e to parameter *Match Value List*.

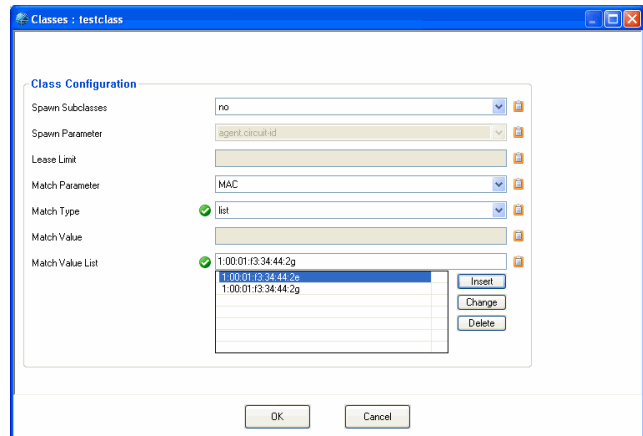
### Note:

The way MAC addresses are entered depends on the used type of interface:

**ethernet** requires a **1:** prior to the MAC address (for example 1:00:01:f3:34:44:2g)

**tokenring** requires a **6:** prior to the MAC address (for example 6:00:01:f3:34:44:2g)

Fig. 7-8 Example - Configuring CLASS Settings



### Step 4 Create subnet and pools for 10.0.8.0/8

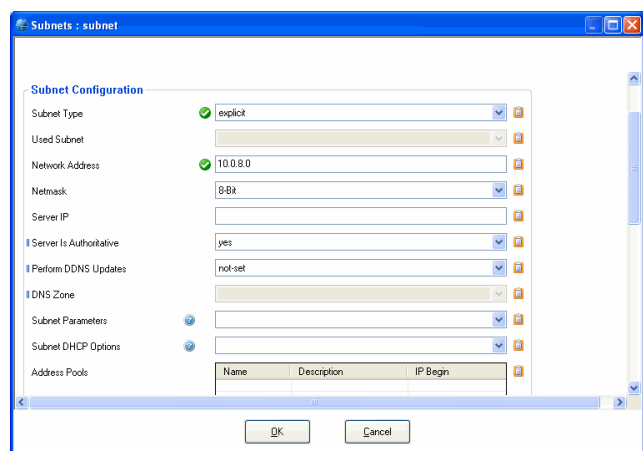
Enter *Address Pools* section and create a new subnet called **Subnet1**.

Configure the subnet according to the following table:

Table 7-1 Example - Configuration parameters for Subnet1

Parameter	Value
Subnet Type	explicit
Network Address	10.0.8.0
Netmask	8-bit

Fig. 7-9 Example - Configuring Subnet settings for Subnet1



Now we can create the 2 required address pools for Subnet1. Therefore, simply add new datasets to parameter *Address Pools* using the following settings:

Address Pool 1: **Unknown**.

Table 7-2 Example - Configuring Address Pool 1 for Subnet1

Parameter	Value	Description
IP Begin	10.0.8.10	Start and end IP address for our example environment is defined.
IP End	10.0.8.15	
Denied Classes	testclass	These parameter settings guarantee that only unknown clients may receive IP addresses from this pool.
Known Clients	deny	
Unknown Clients	allow	

Address Pool 2: **Classpool**.

Table 7-3 Example - Configuring Address Pool 2 for Subnet1

Parameter	Value	Description
IP Begin	10.0.8.20	Start and end IP address for our example environment is defined.
IP End	10.0.8.30	

**Table 7-3** Example - Configuring Address Pool 2 for Subnet1

Parameter	Value	Description
Allowed Classes	testclass	These parameter settings guarantee that only the allowed class may receive IP addresses from this pool.
Known Clients	not-set	
Unknown Clients		
BOOTP Clients Policy		

**Step 5 Create subnet and pool for 10.0.4.0/8**

Enter **SUBNETS** tab and create a new subnet called **Subnet2**.

Configure the subnet according to the following table:

**Table 7-4** Example - Configuration parameters for Subnet2

Parameter	Value
Subnet Type	explicit
Network Address	10.0.4.0
Netmask	8-bit

Now we can create the required address pool for Subnet2. Therefore, simply add new datasets to parameter **Address Pools** using the following settings:

Address Pool 1: **Unknown**.

**Table 7-5** Example - Configuring Address Pool 1 for Subnet2

Parameter	Value	Description
IP Begin	10.0.4.10	Start and end IP address for our example environment is defined.
IP End	10.0.4.15	
Known Clients	deny	These parameter settings guarantee that only unknown clients may receive IP addresses from this pool.
Unknown Clients	allow	

**Step 6 Configure Known Clients**

Enter tab **KNOWN CLIENTS** and add a new group called **Known1**.

Configure section **Known Clients** according the following table:

➤ Known Client **One**.

**Table 7-6** Example - Configuration parameters for Known Clients 1

Parameter	Value
MAC Address	00:01:f3:34:44:2g
Fixed IP Address	10.0.4.31 (optionally)

➤ Known Client **Two**.

**Table 7-7** Example - Configuration parameters for Known Clients 2

Parameter	Value
MAC Address	00:01:f3:34:44:2e
Fixed IP Address	10.0.4.32 (optionally)

**Step 7 Send Changes and Activate the configuration and have a running DHCP**

## 2. "Regular" DHCP

### 2.1 Overview

#### Attention:

From netfence 3.6 on "Regular DHCP" is not available when creating a new service. In multi-release environments formerly existing servers can be administered, though. Due to compatibility reasons, using DHCP Enterprise (see 1. DHCP Enterprise, page 272) is anyway highly recommended.

The **D**ynamic **H**ost **C**onfiguration **P**rotocol is used for assigning IP addresses automatically.

The DHCP server has a given amount of so-called **leases**. These leases are IP addresses that are available for being "lent" to an interface. After a predefined amount of time, the client sends a request to the server whether it may keep the lease.

#### Note:

DHCP and the DHCP Relay Agent was implemented according to the following RFCs:

- RFC 1497 (RFC 951)
- RFC 2131
- RFC 2132
- RFC 3046

The work flow consists of the following steps:

#### Step 1 Discover

As soon as a client connects to the network to contact any reachable DHCP server (source IP: 0.0.0.0; destination IP: 255.255.255.255). This message includes the MAC address of the client. Thus the server(s) know where the request is coming from.

#### Step 2 Offer

After receiving the discover message, the server(s) offer a lease to the client.

The lease consists of:

#### ➤ IP address

- The client gets an IP address out of a defined available IP range (see 2.2.3 IP-Ranges, page 283)
- When the clients MAC address is defined within the special client configuration (2.2.4 Special Clients, page 283) this explicit IP address will be used

#### ➤ Options

The options define the subnetmask, the gateway, ... (see 2.2.5 Options, page 283)

#### Step 3 Selection & Request

The client checks the received lease-offers and selects one.

#### Note:

The selection depends on the client configuration, but usually the lease received first is selected.

Now the client sends a request for the lease to the DHCP server that offered it.

#### Step 4 Acknowledgement

When the lease is still available the DHCP server sends an ACK to the client and the client activates the settings of the lease.

## 2.2 Configuration

As the regular DHCP service was obsolete in netfence 3.6, the regular DHCP service must already exist and have been migrated from a former netfence release.

The following two configuration entries exist in the configuration tree in **Config** > **Assigned Services**:

➤ **Dhcp Server Settings** - see 2.2.1 DHCP Server Settings, page 282

➤ **Service Configuration** - settings made during the introduction of the service

#### Note:

When configuring the Service itself (**Service Configuration**) take into consideration that only certain settings are allowed:

**Bind Type** **First-IP** or

**Second-IP** or

**Explicit** (only if just one explicit IP is specified)

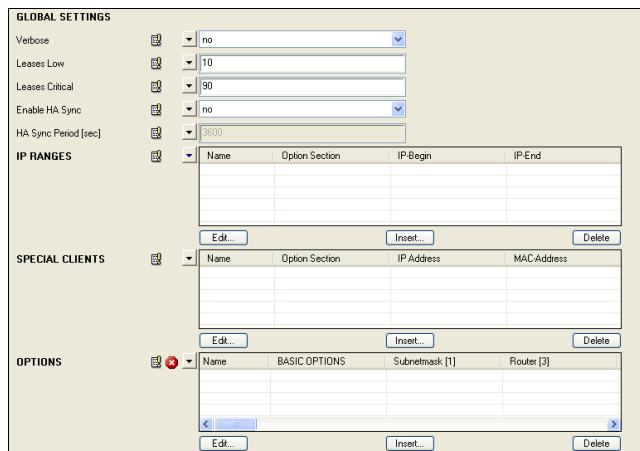
**First+Second-IP** (only First IP will be used)

#### Attention:

Currently the usage of only ONE subnet is supported. But you may define several IP ranges (see below) within this one subnet.

### 2.2.1 DHCP Server Settings

Fig. 7-10 DHCP Server Settings with pre-configured settings



The sections **IP-RANGES**, **SPECIAL-CLIENTS**, and **OPTIONS** are defined via datasets (consisting of multiple parameters). Therefore it is necessary to click **Insert ...** to get to the configuration dialogue for a new data set. However, if you want to modify an already existing data set, select the entry and click **Edit ...** instead.

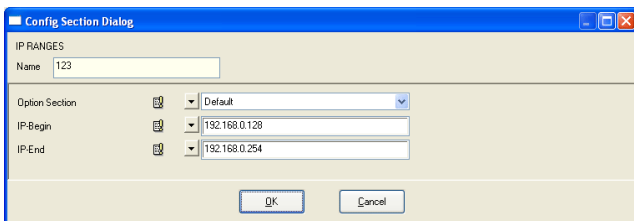
## 2.2.2 Global Settings

List 7-25 DHCP Server Settings - section GLOBAL SETTINGS

Parameter	Description
<b>Verbose</b>	Setting this parameter to <b>yes</b> causes that every action will be logged (☺ <b>Logs</b> > ⚙️ <servername> > ☹️ <servicename>; logs additionally to Administrator-relevant data, for example Error, Warning, Fatal, ..., also Info such as Requests, ACKs, ...)
<b>Leases Low / Leases Critical</b>	The events <b>Resource Limit Pending/Resource Limit Exceeded</b> [135/136] are triggered when the percentage of assigned leases (in %) reaches a critical value or exceeds this limit. <b>Note:</b> The bigger the available network the smaller the gap between low and critical level may be.
<b>Enable HA Sync</b>	Setting this parameter to <b>yes</b> causes the periodical synchronisation of the DHCP database between the HA pair.
<b>HA Sync Period [sec]</b>	This parameter defines the minimum period of time for starting the synchronisation (default: <b>3600</b> s). This period is valid as long the server is idle (no traffic is handled). When the server has traffic this minimum period of time may increase.

## 2.2.3 IP-Ranges

Fig. 7-11 Configuration - IP RANGES

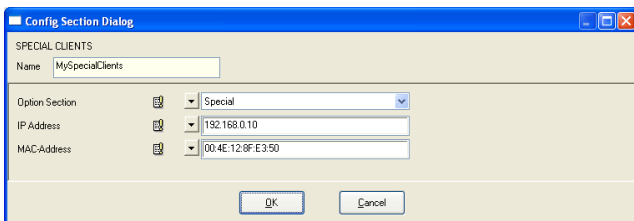


List 7-26 DHCP Server Settings - section Option Section and IP RANGES

Parameter	Description
<b>Option Section</b>	This field defines what kind of configured options (see 2.2.5 Options, page 283) should be used within this IP range.
<b>IP-Begin</b>	This field indicates the begin of the IP range including this IP address.
<b>IP-End</b>	This field indicates the end of the IP range including this IP address.

## 2.2.4 Special Clients

Fig. 7-12 Configuration - SPECIAL CLIENTS



List 7-27 DHCP Server Settings - section SPECIAL CLIENTS

Parameter	Description
<b>Option Section</b>	This field defines what kind of configured options (see 2.2.5 Options, page 283) should be used for this client.
<b>IP Address</b>	This field indicates the IP address that is sent to the client.
<b>MAC-Address</b>	Through this field the unique MAC address is defined that identifies the client.

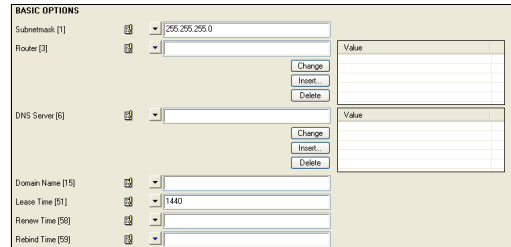
## 2.2.5 Options

**Note:**

The numeric values in square brackets indicate the option-numbering defined in RFC2132.

**BASIC OPTIONS:**

Fig. 7-13 Configuration - BASIC OPTIONS



List 7-28 DHCP Server Settings - section BASIC OPTIONS

Parameter	Description
<b>Subnetmask [1]</b>	Here the correct subnetmask has to be entered.
<b>Router [3]</b>	Here the IP address(es) of the default gateway(s) are to be entered.
<b>DNS Server [6]</b>	Here the IP address(es) of the DNS server(s) are to be entered.
<b>Domain Name [15]</b>	Here the domain name is to be entered.
<b>Lease Time [51]</b>	This field is used for defining the maximum period of time (in minutes) that an IP address may be leased.
<b>Renew Time [58]</b>	This field is used for defining the expired period of time after which the client sends a request (Unicast) to the server, it got the lease from, in order to extend its lease. The default value for this field is $0.5 \times \text{Lease Time}$ .
<b>Rebind Time [59]</b>	This field is used for defining the expired period of time after which the client sends a request (Broadcast) to ANY server to extend its lease. A reasonable value for this field is $0.875 \times \text{Lease Time}$ . <b>Note:</b> When configuring the parameters <b>Lease Time</b> , <b>Renew Time</b> and <b>Rebind Time</b> use the following rule of thumb to determine the values: <b>Lease Time &gt; Rebind Time &gt; Renew Time</b>

List 7-29 DHCP Server Settings - section EXTENDED OPTIONS

Parameter	Description
<b>Broadcast Address [28]</b>	Here the Broadcast Address can be entered.
<b>NIS Domain Name [40]</b>	Enter the domain of the Network Information System in this field.
<b>NIS Server [41]</b>	Here the IP address(es) of the NIS server(s) are entered.
<b>Host Name [12]</b>	Here the host name of the client can be entered.
<b>NTP Server [42]</b>	To enable synchronised times, here the IP address(es) of the NTP server(s) are entered.
<b>WINS Server [44]</b>	When using a WINS server, here the IP address(es) of the server(s) are entered.
<b>NBDD Server [45]</b>	When using a NBDD server, here the IP address(es) of the server(s) are entered.

List 7-29 DHCP Server Settings - section EXTENDED OPTIONS

Parameter	Description
<b>Netbios Node Type [46]</b>	<p><b>Note:</b> When using a Linux client, this parameter is obsolete and has to be left empty.</p> <p>This entry allows NetBIOS to configure TCP/IP clients. The following values are available (with their indication):</p> <p><b>1</b> b-node - broadcast; which means clients use broadcast for name registration/resolution</p> <p><b>2</b> p-node - point; which means client registers itself at the netbios server (point-to-point)</p> <p><b>4</b> m-node - multi; which means client first uses b-node, if it fails p-node is used.</p> <p><b>Note:</b> However, b- and m-nodes should not be used with large networks because the broadcasts use lots of bandwidth.</p> <p><b>8</b> h-node hybrid; which means like m-node, but uses p-node first and then b-node (as a last resort)</p>
<b>Netbios Scope Id [47]</b>	<p><b>Note:</b> When using a Linux client, this parameter is obsolete and has to be left empty.</p> <p>When using NetBIOS Scope IDs (like to isolate NetBIOS traffic or to give the same name to different computers), here this ID is to be entered.</p> <p><b>Note:</b> The <i>NetBIOS Scope ID</i> is case-sensitive.</p>
<b>LPR Server [9]</b>	When using this printing protocol for Unix systems, here the IP address of the printer has to be entered.
<b>Log Server [7]</b>	In case of a stand-alone log server, here the IP address of the server has to be entered.
<b>Time Server [4]</b>	In case of a time server according to RFC868, here the IP address of this server has to be entered.
<b>Time Offset [2]</b>	This field defines the client's time offset (in seconds) from UTC.
<b>IEN Name Server [5]</b>	In case of a IEN name server, here the IP address of this server has to be entered.
<b>Cookie Server [8]</b>	When using a stand-alone cookie server, here the IP address of this server has to be entered.
<b>Swap Server [16]</b>	When using a separate swap server, here the IP address of this server has to be entered.
<b>Local Subnets [27]</b>	In case of local subnets, they are entered in this field.
<b>Impress Server [10]</b>	This field defines the IP address of an optional Imagen Impress server.
<b>Resource Location Server [11]</b>	This field defines the IP address of an optional resource location server (according to RFC887).
<b>Perform Mask Discovery [29]</b>	<p><b>Note:</b> When using a Linux client, this parameter is not supported.</p> <p>This field defines whether a subnet mask discovery is carried out or not. The following settings are available:</p> <p><b>1</b> - Client uses ICMP for subnet mask discovery</p> <p><b>0</b> - No subnet mask discovery is to be performed</p>
<b>Perform Router Discovery [31]</b>	<p><b>Note:</b> When using a Linux client, this parameter is not supported.</p> <p>This field defines whether a router discovery is carried out or not. The following settings are available:</p> <p><b>1</b> - Client performs ICMP router discovery (according to RFC1256)</p> <p><b>0</b> - No router discovery is to be performed</p>
<b>Static Route [33]</b>	<p>This field is used for entering the static routes of the client.</p> <p><b>Note:</b> When using a Windows client, this parameter is not supported.</p>
<b>TFTP Server Name [66]</b>	Here a TFTP server may be defined.
<b>Boot File Name [67]</b>	This field allows entering a boot file name.

## 2.3 Real Time Information


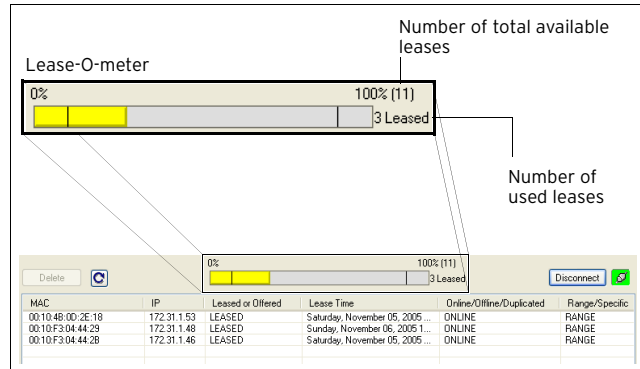
The real time information for the configured DHCP server can be accessed via the box menu entry  **DHCP**.

Fig. 7-14 Real Time Information - DHCP



By using the **Delete** button (top left corner) it is possible to delete active leases manually.

### Attention:

To avoid duplicate IPs after deleting a lease, the lease is not put back into the list of available IP addresses until the service is restarted.

The Refresh button (right to **Delete** button) is used for refreshing the display.

The so-called Lease-O-meter in the middle of the user interface indicates the level of lease usage.

### ➤ MAC

This column displays the client MAC address for each lease that is currently used.

### ➤ IP

This column displays corresponding client IP address.

### ➤ Leased or Offered

The state of a lease is displayed in this column. Possible values are **Leased** and **Offered**.

➤ **Leased** - indicates used IP addresses

➤ **Offered** - indicates leases that are currently offered but not yet taken

### ➤ Lease Time

Shows the amount time until the lease expires.

### ➤ Online/Offline/Duplicated

The DHCP sends ARP requests throughout the network. Depending on the response, the following states are possible:

➤ **Online** - the IP address answers the ARP request

➤ **Offline** - the IP address does not answer the ARP request

➤ **Duplicate** - multiple IP addresses answer the ARP request



➤ **Range/Specific**

This column shows what kind of IP address is used in this lease:

➤ **Range** - The IP address is defined through the **IP-Ranges** field (see 2.2.3 IP-Ranges, page 283)

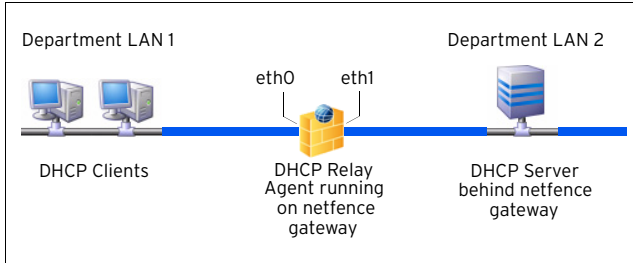
➤ **Specific** - The IP address is defined through the **Special Clients** field (see 2.2.4 Special Clients, page 283)

➤ **Option**

This column shows the name of the options used by this lease.



## 3. DHCP Relay Agent

Fig. 7-15 Example of use for a DHCP Relay Agent



A DHCP relay agent has to be used when DHCP clients and server are located in different networks both protected behind firewalls. DHCP relay agents communicate with unicast instead of broadcast so that the messages may pass the firewalls.

The DHCP relay agent does not handle IP addresses itself, but instead passes DHCP messages between the DHCP clients and their server.

Introduce a DHCP relay on a netfence gateway by selecting  **Config** from the box menu, navigating through the configuration tree until the  **Assigned Services** item is reached, and selecting **Create Service ...** from the context menu.





### Note:

Please see **Configuration Service - 4. Introducing a New Service**, page 97, for detailed information concerning procedure and available options for service creation.

### Note:

DHCP relay and DHCP server cannot live together on the same box. Make sure to configure these services on self-contained systems. This restriction is valid for DHCP servers that have been delivered until 2.4.x. DHCPe servers can live together with DHCP relay, as long as these services do not use the same interface.

By introducing a DHCP relay, the following configuration items are added to the configuration tree:

-   **Dhcp Relay Settings** - see 3.1 DHCP Relay Settings, page 286
-   **Service Properties** - settings made during the introduction of the service

## 3.1 DHCP Relay Settings

Fig. 7-16 DHCP Relay Settings

List 7-30 DHCP Relay Settings

Parameter	Description
<b>UDP Port</b>	This parameter defines the port the relay agent is listening on (default: <b>67</b> ).
<b>Relay Interfaces</b>	Define the network interfaces, which the DHCP relay agent utilises to connect the networks DHCP server and clients are situated in (eth0 and eth1 in the example given in figure 7-15). Choose the interfaces from the physical network interfaces available in the list. Virtual interfaces are not included in the list. If you require a virtual interface, select the <b>Other</b> checkbox and insert the interface manually. Click the <b>Insert ...</b> button after each interface's selection or manual specification to add the interface to the configuration. <b>Note:</b> When using Virtual LANs ( <b>Configuration Service - 2.2.5.3 Virtual LANs</b> , page 65), select the <b>Other</b> checkbox and enter the tagged VLAN interface (parameter <b>Hosting Interface</b> ).
<b>DHCP Server IPs</b>	In this place, specify the IP address(es) of the DHCP server(s) the DHCP relay is relaying for.
<b>Add Agent ID (AID)</b>	Set to yes ( <b>default</b> ), if you want the DHCP relay agent to add an <b>Agent ID (AID)</b> to the transmitted packets. An <b>AID</b> indicates that the data has been relayed.
<b>DHCP Packet Size [B]</b>	This parameter defines the maximum DHCP packet size in bytes (default: <b>1400</b> ).
<b>AID Relay Policy</b>	This parameter defines how to deal with DHCP packets already flagged by an AID. The following options are available: <b>Append</b> (default) - Attaches my agents's ID to the existing one leaving it intact. <b>Replace</b> - Replaces the existing AID with my agent's ID. <b>Forward</b> - Passes DHCP packets without any modification. <b>Discard</b> - Discards DHCP packets which are already flagged by an another agent's ID.
<b>Reply AID Mismatch Policy</b>	The relay agent scans packets it receives from the DHCP server for the server's IP address before forwarding them to the client. If it finds the IP address in the header, it forwards the packet to the client. If it cannot find it, the relay acts on the directive defined by the following parameter: <b>Discard</b> (default) - Discards the DHCP packet. <b>Forward</b> - Forwards the DHCP packet regardless. <b>Note:</b> The <b>Reply AID Mismatch Policy</b> parameter is of special importance when multiple relay agents serve the DHCP server.
<b>Packet Hop Count</b>	Limit the hop count (default: <b>10</b> ) with this parameter to avoid infinite packet loops.

### 3.1.1 Cascading DHCP Relay Agent

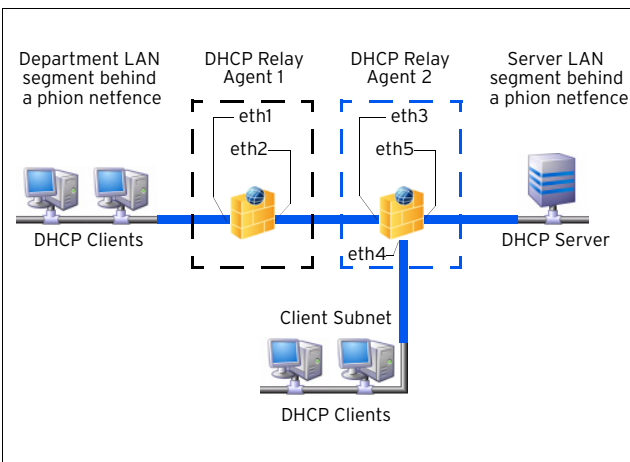
**Note:**

Actually, the DHCP Relay Agent is not designed for cascaded use. However, if there is demand to configure multiple relay agents in a cascaded environment, consider that you must not specify the server-side interface of the cascaded ("border") relay agent in the configuration, as this will lead to conflicts.

**Attention:**

Cascading DHCP relay agents are to be used only, if a client subnet is connected to the server-side DHCP Relay Agent.

**Fig. 7-17** Cascading DHCP Relay with interfaces to be configured



The configuration itself is done in the same way as the standard configuration depicted above, except for the definition of relay interfaces.

In the example (figure 7-17) two client subnets are connected to two DHCP Relay Agents 1 and 2. The interfaces listening to broadcast request from the clients have to be specified as relay interfaces in the configuration (eth1 and eth4). The server-side interface of Relay Agent 2 (eth5), which is connected to the DHCP Server must NOT be specified.



# Log Viewer

<b>1.</b>	<b>Overview</b>	
1.1	LogGUI .....	290
<b>2.</b>	<b>Functional Elements of the LogGUI</b>	
2.1	Selection Segment .....	291
2.2	Navigation Segment .....	291
2.3	View Segment .....	292
2.4	Types of Log Entries .....	292
2.5	Event Log Message Structure .....	292
2.6	Specialities .....	292
2.6.1	Clock Skew .....	292
2.6.2	Dirty Block .....	294
2.6.3	Digression: logwrapd .....	294

# 1. Overview

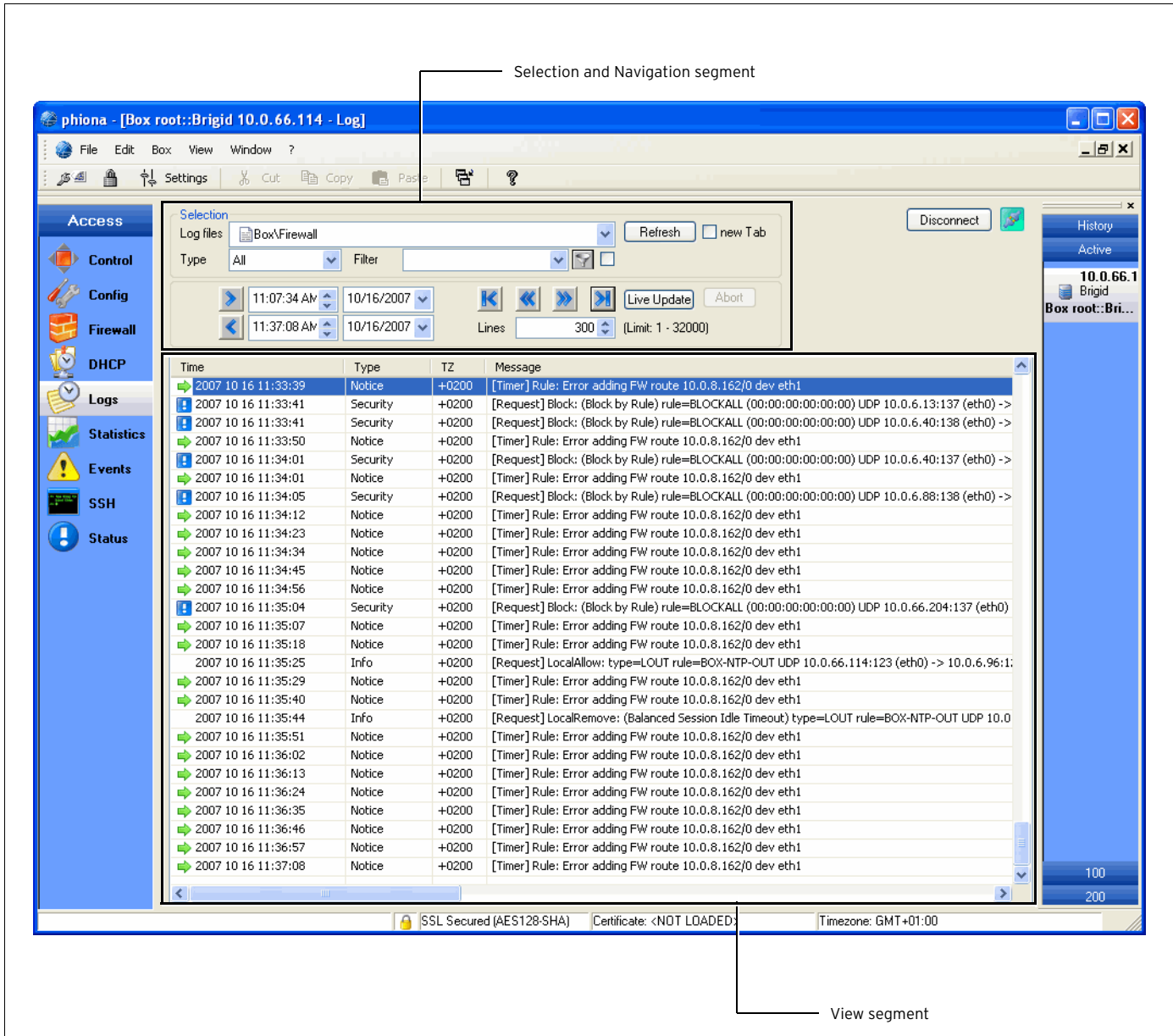
## 1.1 LogGUI

The phion LogGUI is an additional tool for receiving individual information for specific parts of a phion system.

The output is text-based and occurs systematically after an event has taken place. The output can be tailored individually to the specific needs and preferences of the administrator by use of the LogGUI.

To access the log viewer, click **Logs** in the box menu.

Fig. 8-1 LogGUI

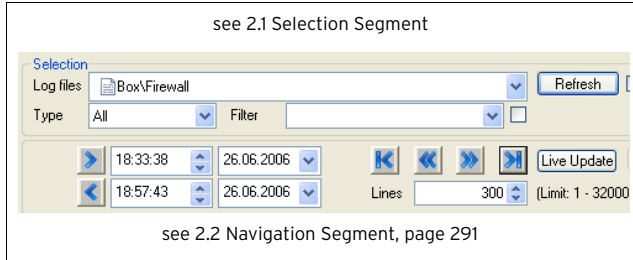




## 2. Functional Elements of the LogGUI

The LogGUI is divided into three segments, through which a selective presentation of a log protocol is made possible.

**Fig. 8-2** Navigation section of the LogGUI



### 2.1 Selection Segment

The directory displayed in the **Log-module** menu is divided into five logically separated types of log files which constitute the first level in the tree hierarchy.

The file tree consists of the log files in the directory `/var/phion/logs/`, which can also be reached in the box level.

- **Box**  
All the events on the box level can be found in the column Box. Various box specific daemons are included here. These types of log files are documented with the prefix `box_`.
- **Misc**  
The segment Misc deals with logs, that do not fall into a specific column. They are neither categorised as box services nor as server support or reports and do not have a prefix on the box level.
- **Reports**  
These types of logs - on the box level documented with the prefix `rep_` - include entries that are carried out in continuous intervals (cronjobs).
- **Fatal**  
All fatal errors that can occur on a phion netfence are - in addition to the original log file - collected in this section. The original log file is added in the fatal log message text as a prefix.
- **Services**  
This part deals with log file types that deal with server support. These types of log files are documented with the prefix `srv_`.

Within the Box branch the log files are grouped by operative themes, for example, **Auth** contains authentication log files.

For a detailed view of a specific log out of these categories select it by double-click.

In the selection segment it is possible to delete selected log entries. Therefore, select **Delete** Log in the context menu of the corresponding log entry. For deleting the log cache select **Clear Log Cache**. This way the database is build from ground up.

Additionally, the view of the section being presented can be restricted, by explicitly entering the log input type or by filtering a character string. The pull-down menu in the **Type** section is for choosing the type of log input.

The number of log entries to be presented is adjusted in the segment **Lines**.

You are also able to filter normal descriptive log entries of the type info and internal by selecting **All\_But\_Info**.

The form of the character string, which is to be filtered, can be entered in the **Filter** section. By doing so, the bordering hook is automatically enabled. This signifies that the filter is enabled and should be disabled to deactivate the filter.

For a simple and clearly arranged overview as well as an analysis of the individual log entries, the different entries in the logs are assigned to types. This is further explained under 2.3 View Segment, page 292.

The button **Refresh** updates the log tree in the selection segment.

Tickling checkbox **new Tab** creates a new tab for the new log view instead of replacing the "old" one.

### 2.2 Navigation Segment

The date fields enable you to enter the time and date for a particular segment of a log either directly, by use of the keyboard, or by using the pull-down menu to easily attain log entry items between larger time intervals.

When the desired log is marked, it is possible to thumb through the log items by using the navigation arrows:

**Table 8-1** Navigation arrows and their function

Icon	Description
	Browse back from the value entered for time and date
	Browse forward to the value entered for time and date
	Browse back from current entry
	Browse forward from current entry
	Browse from beginning of log
	Browse to end of log

The button **Live Update** enables an update of the view segment, if the log file concerned got any new entries. From case to case, long lasting presentation options or long processing filtering tasks can be terminated by using the **Abort** button.



## 2.3 View Segment

After a log has been selected and the navigation options (which can be time, date, type, and filter) have been set, the log entries are displayed in the view segment after having pressed one of the navigation arrows.

The view segment window is divided into three categories:

- **Time**  
This is the time when an event has taken place. The time indicator marks individual log entries.
- **Type**  
Shows the type of log entry
- **TZ**  
This column displays the UTC time zone offset compared to the local box time.
- **Message**  
Short description of the entry

## 2.4 Types of Log Entries

A certain symbol is given to every log entry depending on the type of the entry. **Info** and **Internal** describe normal events, which are not associated with a symbol. Table 8-2 summarises the individual types and their respective symbols.

Table 8-2 Log Entry types

Icon	Type	Description
	Warning	Uncritical event (for example login)
	Error	Event error (for example system calls, clock skew)
	Fatal	System critical events
	Notice	Normal system events (for example reading a configuration file)
	Security	Events relevant to security (for example authorisation, login)

Type **Panic**, which extremely rarely appears and is excluded in table 8-2, marks critical events compromising the system's functionality and stability.

The meaning of a symbol cannot be related to a single event. Instead it should be regarded in relation to the log type that has been marked.

## 2.5 Event Log Message Structure

At a glance Event logs look the same as any other log message. However, the message text holds very important information, and therefore requires a deeper look.

The following example contains a mail event log message:

Table 8-3 Event Log Message - Attributes

Date [yyyy mm dd]	Time [hh:mm:ss]	Type	TZ [+ hhmm]
2005 07 18	15:40:41	Info	+0200

Table 8-4 Event Log Message- ID and text

Message ID	Message Text
[1071065]	Insert Event from 127.0.0.1:12631 - (D)2 mgwext_mail 3 Mailgw-Rule 4506 Drop Recipient <e.example@phion.com> bart_111)

Event content (**bold** message text portion above) enclosed in brackets, ( and ) contains the following pipe /separated fields:

The log message text arranged as follows ...

```
(D|2|mgwext_mail|3|Mailgw-Rule|4506|Drop Recipient<e.example@phion.com>|bart_111)
```

... is built up of the following elements:

```
(Internal flag|Layer[1-3]|Layer description|Class ID [1-3]|Class description|Type (Event ID) |Layer Description|Full box name)
```

**Layer** and **Class** are hidden fields, which have originally been part of the event specification. However, the two parameters have no particular meaning, which could be used for filtering and extraction purposes by a security event management tool.

**Layer description** denotes the originator of the event on the netfence system. In the example above the event has been generated by a service named "mgwext\_mail".

**Class description** denotes a subcomponent of the originator, in the example above the event was triggered due to a mail gateway rule having handled a particular mail.

Suitable filtering criteria are **layer description**, **type identifier**, **class description**, and **full box name**.

## 2.6 Specialities

### 2.6.1 Clock Skew

Clock skews are events that describe an inconsistency in the timed recording of sequences. For example, this can occur when the system time has been changed, through which the incremental record of the time stamp is disturbed in the log.

Fig. 8-3 Log Sequence Number in Relation to System Time

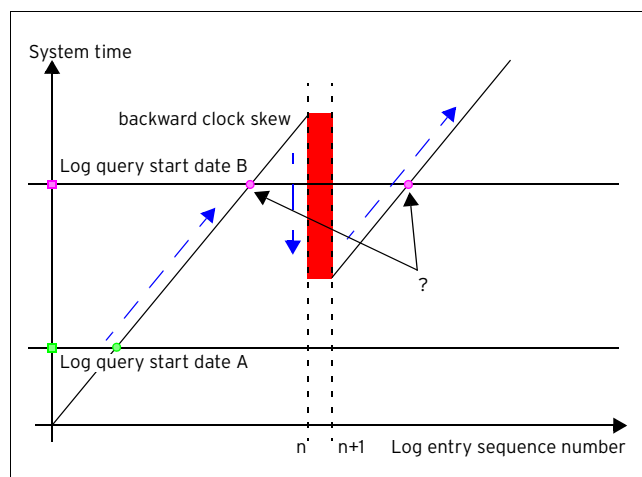


Figure 8-3 shows a clock skew event in the past. The leap in system time (indicated as red vertical bar) results in the recording of sequence pairs in the log file, which show the same time stamp.

For this reason if you start to browse the log from an inconsistent starting point (log query start date B, see the question mark in figure 8-3) it is ambiguous, which starting point is meant.

Hence a popup window will appear that lets you decide to chose the log query start date in order of the chronological occurrence of the clock skew entries in the corresponding log.

### 2.6.1.1 Analysing Clock Skew Entries in Log Files

This overview is meant to explain the cause of the most frequent clock skew entries produced by **dstats/dstatm**. Particular regard is paid to those messages generated in dirty situations.

**Dstats** and **dstatm** search for clock skews on every daily start-up of the service. The log file entries they produce will be related to the following processes:

- clock skew detection
- synchronisation of actively configured polling list and database
- reasons for service start-up abortion
- synchronisation between the local copy of the HA-database (which has been mirrored during the last HA-sync) and the current database of the HA-partner
- Furthermore, **dstats** searches for files, which are outdated due to a clock skew and should have been deleted according to the configuration file. If the checking routine fails, manual action has to be taken (see 4.2.2 Manual Correction for Time Preference, page 303).

Some of the errors described below might produce an additional log file entry like **"Comment / MAIN ADMIN action required!!!"** The reason for such a message will be that the main task is not running. Whenever you encounter it you might have to restart the task manually.

As well some of the malfunctions described in the following might additionally produce an entry in the **MC control > Stat Collect** tab. In case the value of these entries is **"INTERNAL ERROR"** please contact your sales partner or phion support.

### 2.6.1.2 Log File Entries related to Clock Skew Detection

Table 8-5 Log file entries related to clock skew detection

Log (Type/Message)	Corresponding content of BerkeleyDB-Header	Reason
"Info / MAIN no clock skew detection (initial)"	LastRun 0, LastStart 0	A clock skew cannot be detected because it is assumed that dstatm is either running for the first time or it has never run successfully.
"Error / *** Unresolvable clock skew detected ***"	LastRun <timestamp>, today <timestamp>	<i>HASync is active.</i> The current system time is either behind or more than two days ahead the time of the LastRun header field in the BerkeleyDB. A clock skew detection fails because of inconsistencies in time settings.  <i>HASync is not active.</i> The current system time is either behind or more than two days ahead the time of the LastRun header field in the BerkeleyDB. A clock skew detection fails because of inconsistencies in time settings.

### 2.6.1.3 Log File Entries related to Synchronisation of Polling List and Database

Table 8-6 Log file entries related to synchronisation of polling list and database

Log (Type/Message)	Reason
	Eventually the configuration cannot be read.
"Error / MAIN cannot sync box state with configuration: <specific error message>"	The configuration of the polling list cannot be synchronised with the database.
"Error / MAIN cannot save state db: <specific error message>"	The configuration of the polling list cannot be synchronised with the database.

### 2.6.1.4 Log File Entries related to Service Start-up Abortion

Table 8-7 Log file entries related to synchronisation of polling list and database

Log (Type/Message)	Reason
"Fatal / MAIN is disabled!"; "Comment / MAIN ADMIN action required!!!"	Main is in state DISABLED.
"Notice / MAIN trying to recover from <current_state> state"	Main is not in state CLEAN. If the field 'main task' has been set to STOPPED it will now be reset to IDLE. It will be assumed that the problem has been solved and normal operation can be continued.

### 2.6.1.5 Log File Entries related to Synchronisation between Ha-databases

#### Scenarios which will stop task MAIN:

These scenarios will produce an additional log file entry "Comment / MAIN ADMIN action required!!!". Checking the state of task MAIN is required.

Table 8-8 Log file entries related to synchronisation between HA-databases - Scenarios which will stop task MAIN

Log (Type/Message)	Reason
"Error / MAIN sync state dirty!"	HASync is active but the sync state-file is DIRTY.

**Table 8-8** Log file entries related to synchronisation between HA-databases - Scenarios which will stop task MAIN

Log (Type/Message)	Reason
"Warning / MAIN ha entry: activity state changed to disabled"	HASync is not active but the database entry for the HA-partner has been not set to DISABLED.
"Info / MAIN ha state db not available, assuming initial"	HASync is active but the database of the HA-partner is not available. It is assumed that the HA-partner has never been active and thus has no "state", which it could have negotiated during the HASync. The database of the HA-partner will contain the comment entry "no state present, assuming initial".
"Error / MAIN cannot load HA state db: <specific error message>"	HASync is active but the database of the HA-partner is though available not readable.
"Error / MAIN HA state db out of date"	HASync is active and the database of the HA-partner is available. There are time inconsistencies in the LastStart header fields of the BerkeleyDBs though, which means the LastStart header field in the own BerkeleyDB is younger than the one in the HA-partner's DB. Furthermore the DB header field LastRun does not reflect the current day.  The database of the HA-partner is obsolete. A data inconsistency is most likely. As an automated troubleshooting is not possible in this case, a manual check has to be undertaken. Possible scenario: The active HA-partner has crashed during HA-synchronisation. The following log entry could be expected in this case (see next entry below):
"Info / MAIN HA state db out of date? Assuming block and restart scenario"	HASync is active but the ActivityState of the HA-Partner is DISABLED.
"Warning / MAIN HA sync enabled although HA box is disabled"	HASync is active but the ActivityState of the HA-Partner is DISABLED.
"Fatal / AIN HA takeover in inconsistent state!"	HaSync is active but the HA-partner is not in state CLEAN.
"Warning / MAIN ha entry: activity state changed to disabled"	HaSync is not active but the HA-partner state is not DISABLED.
"Error / MAIN session state unknown, going to stop!", "Error / MainLoop - main task UNKNOWN"	The state of MAIN could not be determined during start-up.
"Error / MAIN cannot sync poll state, going to stop!", "Error / MainLoop - main task poll_pending"	Synchronisation of configured polling list and database is not possible (compare to 2.6.1.3 Log File Entries related to Synchronisation of Polling List and Database).
"Error / MAIN internal error <error_num>", "Error / MainLoop - main task poll_pending"	A system related error has occurred during polling (for example missing system resources)

### Scenarios which will not stop the task MAIN

The errors described below will not stop task MAIN because there will be no indication that data on the (local) MAIN has been damaged. Take into consideration that on the other hand data on the HA-partner could be in an inconsistent mode.

In case the synchronisation is not successful, the current try is given up and the MAIN task is reset to 'sync\_await'. When the maximum allowed number of retries is exceeded, the main status changes to 'await\_daybreak'. The database will not be synchronised with the HA-partner. Manual action will be necessary to solve the problem.

**Table 8-9** Log file entries related to synchronisation between HA-databases - Scenarios which will not stop task MAIN

Log (Type/Message)	Reason
"Error / MAIN local compression cooking done with error %d, going to stop!", "Error / MainLoop - main task cook_pending"	Cooking of statistics files could not be completed.
"Error / MAIN cannot write HA sync file", "Error / MainLoop - main task sync_pending"	The HA sync file could not be written. Check for a previously created HA sync file which possibly could not be overwritten. Check for HDD errors. Restart dstatm.
"Error / MAIN HA sync done with error <error_num>", "Comment / MAIN could not start sync process"	The sync-process cannot be started.
"Error / MAIN HA sync unsuccessful (try <retry_count>)"	The HA synchronisation has failed. Prior error messages have to be analysed to solve this problem.

## 2.6.2 Dirty Block

It is possible that corrupt entries are taken to a log. "Corrupt" in this case means that the log entry does not conform with the expected log entry format. These entries are called **dirty blocks**.

There are different circumstances which can lead to dirty block entries. Examples could be unsuitable timestamp formats due to a wrong version of the **network time protocol daemon** (ntpd) or the recording of binary data, where a timestamp is completely missing. Such entries are indicated and shown as dirty blocks in the view segment area.

## 2.6.3 Digression: logwrapd

The directories relevant for recording events can be found in `/var/phion/logs/` and `/var/phion/logcache/` on the box level. In addition, there are directories for every segment (Range), named after the client number.

The files found in the directory `/var/phion/logcache/` with the extension LAF (**Log Access File**), are structure authorities that are produced in a cycle and continually updated. They are used to raise log file interrogation performance.

The box daemon logwrapd is responsible for handling logs and LAF structures as well as log cycling, detection of clock skews, and dirty blocks.

### Attention:

Logs and LAF-structures in the above mentioned directories are not to be renamed, erased or manipulated.

# Statistics

<b>1.</b>	<b>Overview</b>	
1.1	Box Statistics .....	296
1.2	Server Statistics .....	297
<b>2.</b>	<b>Operation of the Statistics Module</b>	
2.1	Time Statistics .....	297
2.1.1	Control Field .....	297
2.1.2	Graphs .....	298
2.2	Top Statistics .....	299
2.2.1	Control Field .....	299
2.2.2	Graphs .....	299
<b>3.</b>	<b>Configuration</b>	
3.1	Service Configuration .....	300
<b>4.</b>	<b>Advanced Topics</b>	
4.1	Cooking of Statistics .....	302
4.2	Dealing with a Box in the "Future" .....	302
4.2.1	Self-healing for Quantitative Preference .....	303
4.2.2	Manual Correction for Time Preference .....	303
4.2.3	Further Issues .....	304


# 1. Overview

The phion statistics module raises a multitude of statistical data reflecting box and server processes, such as disk utilisation, processor load, and traffic generation.

The following services are responsible for handling of statistics data:

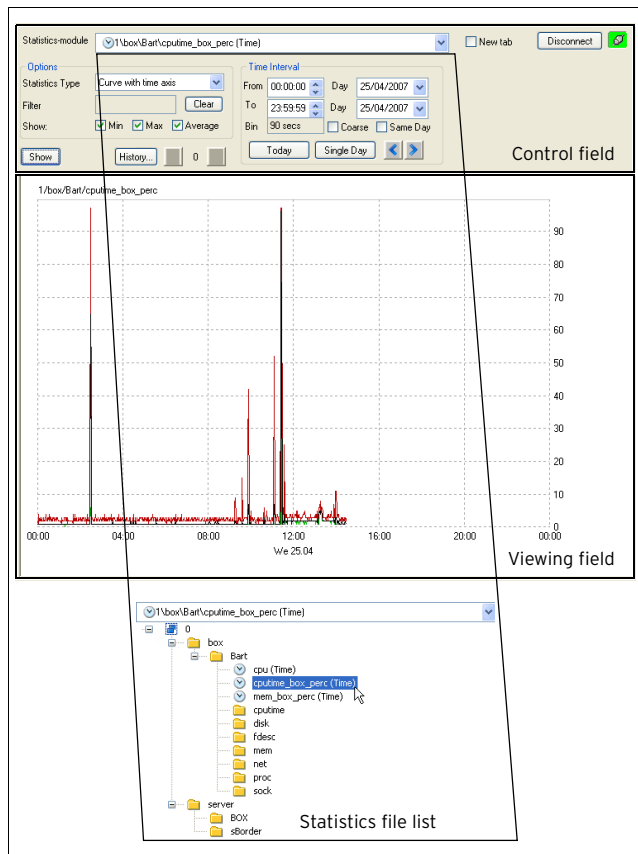
**Table 9-1** Services responsible for statistics files handling

Service	Responsibility
<b>cstatd</b>	Collection of statistics files.
<b>qstatd</b>	Handling of statistics queries, like display of statistics files contents in the statistics viewer.
<b>dstats (statcook daemon)</b>	Validation and "cooking" (which means compression) of statistics files. Utility run by cron as daily job. Recognises corrupted statistics files and prevents their collection by cstatd and dstatm. Available on both, self-managed systems and management centres.
<b>dstatm</b>	MC specific service. Collection of statistics files from MC-administered boxes ( <b>phion management centre - 9. MC Statistics, page 436</b> ).
<b>qstatm</b>	MC specific service. Handling of statistics queries, display of statistics files contents in the statistics viewer on the management centre ( <b>phion management centre - 9. MC Statistics, page 436</b> ).

To access the Statistics viewer, click  **Statistics** in the box menu of the graphical administration tool phion.a.

**Note:**  
Collection of statistics by **cstatd** is not included in all licenses. If statistics records are unavailable, check your license's coverage.

**Fig. 9-1** Statistics user interface



As shown in figure 9-1, the statistics window user interface is divided into two areas, a Control and a Viewing field.

In the Control field, statistics file and various display options may be selected for display in the Viewing field. Double-click a folder to expand the statistics file list. Double-click a statistics file to select it for display.

**Note:**  
Always click the **Show** button after having defined viewing options in order to display the statistics file analysis.

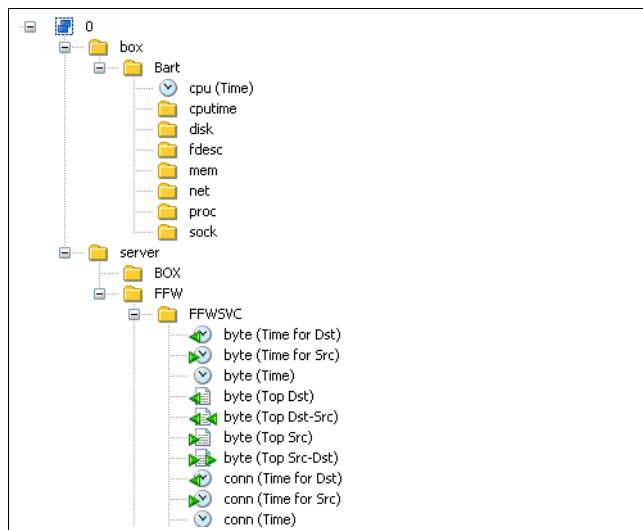
To delete statistics files, select a folder in the Statistics file list, then right-click and then select **Delete Statistics** from the context menu.

Generally, data originates from two sources:

- System resources
- Operative service data

The statistical raw data is registered according to time, connection, or a combination of both. Statistical data containing time information is defined as **time data** (which means timed statistics), whereas connection based data is defined as **top data** or **top statistic**.

**Fig. 9-2** Tree structure of the Statistics module



## 1.1 Box Statistics

The different box resources recorded are:

- **cpu (Time)**  
The CPU load x 100 is displayed in the graphic. The CPU load is an equivalent and has no unit. For example, on a single processor machine CPU load 1 states that a given process utilises the whole processor. The equivalent on a dual processor machine is CPU load 0.5, which means a given process utilises half of the available CPUs.
- **cpulime**  
The amount of CPU time needed for running or completed processes is displayed. The unit is a millisecond per second.



- **disk**  
Status of available disk space (filling degree) of the single partitions, available as byte and as percentage statistic.
- **fdesc**  
Number of file descriptors per phion box or server process
- **mem**  
Main memory capacity in bytes per phion box or server process
- **net**  
Net transfer statistic (in/out) per network interface in bytes, packets and the number of errors of the configured network interface.
- **proc**  
Number of current box and server processes
- **sock**  
Number of open sockets per box or server process

## 1.2 Server Statistics

Server statistics are recorded as transfer capacity (byte statistic), the number of connections handled (conn statistic) and number of open connections (open-conn statistic). Which of these statistic types are actually recorded depends on the specific service type. Also, the detailed structure of the service statistic tree depends on the type of service.

The statistic types in detail:

- **byte (Time for Dst)**  
Time statistic by means of bytes transferred for a certain destination address
- **byte (Time for Src)**

- Time statistic by means bytes transferred for a certain source address
- **byte (Time)**  
Time statistic by means of bytes transferred
- **byte (Top Dst)**  
Top statistic by means of bytes transferred for a certain destination address
- **byte (Top Src-Dst / Dst-Src)**  
Top statistic by means of bytes transferred for a certain pair of source and destination address
- **byte (Top Src)**  
Top statistic by means of bytes transferred for a certain source address
- **conn (Time for Dst)**  
Time statistic of the number of connections to a specific destination
- **conn (Time for Src)**  
Time statistic of the number of connections from a specific source
- **conn (Time)**  
Time statistic of the number of connections
- **conn (Top for Dst)**  
Top statistic of the number of connections to a specific destination
- **conn (Top for Src)**  
Top statistic of the number of connections from a specific source
- **conn (Top for Src-Dst / Dst-Src)**  
Top statistic of number of connections for a specific pair of source and destination addresses
- **open-conn (Time)**  
Number of open connections

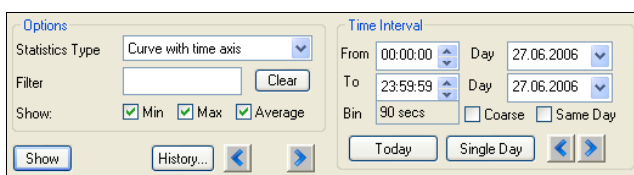
## 2. Operation of the Statistics Module

### 2.1 Time Statistics

#### 2.1.1 Control Field

The following values may be adjusted in the Control field related to viewing of statistics files of type **Time**:



Fig. 9-3 Control field for type Curve with time axis





List 9-1 Control field for type Curve with time axis - section Options

Parameter	Description
<b>Statistics Type</b>	Defines the display mode of the graph. Available selection are: ➤ <b>Curve with time axis</b> ➤ <b>Bars with time axis</b>
<b>Filter</b>	Depending on the statistics type either a source or a destination address has to be specified. The format of these addresses depends on the phion service type and is equivalent to the corresponding <b>Top</b> statistic.
<b>Clear button</b>	Clicking this button clears the <b>Filter</b> field.
<b>Show</b>	Checkboxes to the right of the <b>Show</b> label define display of minimum, maximum and/or average values. <b>Min</b> (minimum) - When selected, a <b>green</b> curve for the lowest value within the selected time interval is displayed. <b>Max</b> (maximum) - When selected, a <b>red</b> curve for the the highest value within the selected time interval is displayed. <b>Average</b> - When selected, a <b>black</b> curve for the calculated average value within the selected time interval is displayed.



List 9-1 Control field for type Curve with time axis - section Options

Parameter	Description
Show button	Clicking this button generates the statistics analysis. To open the report in a new tab instead of overwriting currently displayed content, select the <b>New tab</b> checkbox prior to clicking the <b>Show</b> button.
History	Clicking this button opens the <b>Statistics History</b> window, which lists all analyses that have been executed during the current phion.a session. Double-click a report in the list to open it anew. Alternatively, browse through all available reports by clicking the  and  arrows to the right of the history button.

List 9-2 Control field for type Curve with time axis - section Time Interval - Curves

Parameter	Description
	(for Statistics Type: Curve with time axis)
From	Start time for the analysis on a specific day.
To	End time for the analysis on a specific day.
Day	Start and end date of the analysis.
Bin / Coarse	The <b>Bin</b> value represents the density of the graph. Select the <b>Coarse</b> checkbox to reduce density and to smoothen the curve. Lower graph density is suitable for survey of long observation periods.
Today	Sets the analysis period to the current date.
Same Day	Sets the analysis period to the selected start date.
Single Day	Sets the analysis period to the selected start date.
 	Shifts the analysing period to an earlier or later time interval following the configured settings in the <b>From</b> , <b>To</b> and <b>Day</b> fields.

List 9-3 Control field for type Curve with time axis - section Time Interval - Bars

Parameter	Description
	(for Statistics Type: Bars with time axis)
Year / Month / Day	Checkbox selection and insertion of appropriate date values into the fields below, sets the analysing period to the corresponding interval.
Today	Sets the analysis period to the current date.
 	Shifts the analysing period to an earlier or later time interval following the configured settings in the <b>From</b> , <b>To</b> and <b>Day</b> fields.

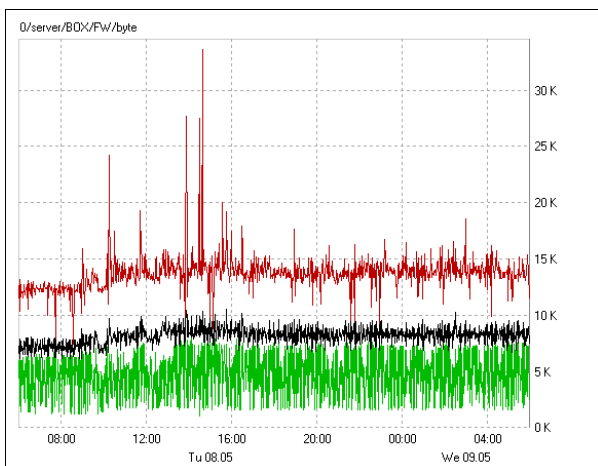
## 2.1.2 Graphs

Time statistics analyses can be displayed as curves or bars with a time axis.

### Curve with time axis

To display statistics files a curves, select **Curve with time axis** from the **Statistics Type** list and click the **Show** button.

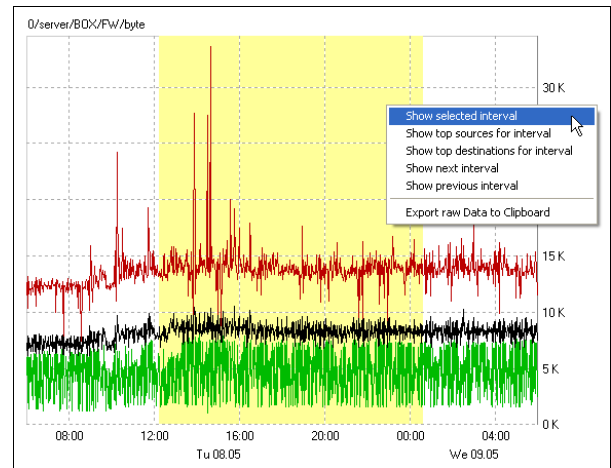
Fig. 9-4 Curve type



With appropriate selection (see **Min**, **Max**, **Average** checkboxes), three curves for minimum (green), maximum (red), and average (black) values will be displayed.

To detail a part of the analysis, left-click the starting point of the new interval, drag the cursor through the window and release the mouse-button at the interval's end point.

Fig. 9-5 Time Interval selection

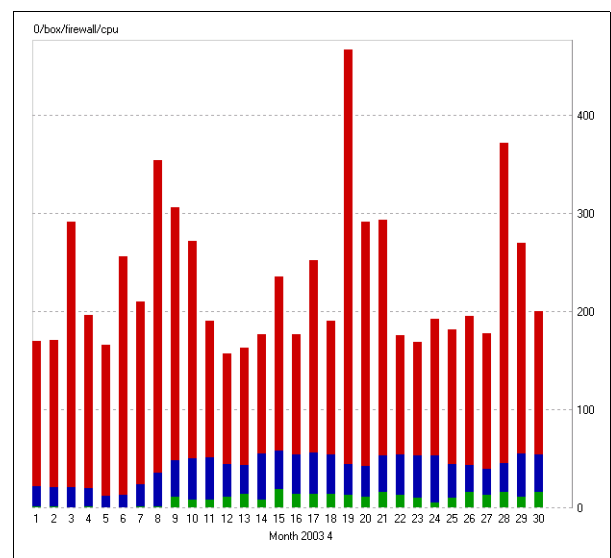


Right-click the selected area to open the related context menu and click **Show selected interval** to display the new time interval in detail.

In the newly opened view, right-click anywhere, then click **Show next interval** in the context menu to display the statistics details following the previously shown time interval. Note that clicking this option influences the time values in the **Time Interval** section within the Control field (see above).

### Bars with time axis

Fig. 9-6 Bar type



Bars with accumulated statistical data may be generated by day, month, or year. Again, with appropriate selection and availability of data (see **Min**, **Max**, **Average** checkboxes), bars will be divided into three parts for indication of minimum (green), maximum (red), and average (blue) values.

## 2.2 Top Statistics

Top statistics are always displayed as bars in the statistics module.

Top statistics show values (bytes or number of connections) and the corresponding connection information (source and/or destination address) in a sorted manner.

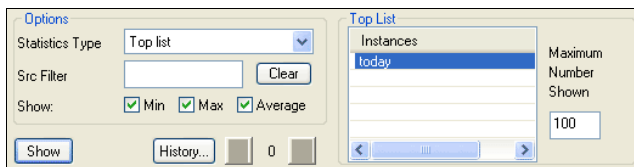
### 2.2.1 Control Field

Options for top file types can be set in this field.

The observation period is subdivided into the actual day (today), date of past day, week, and month. The existence of week and month instances depends on the configuration of the statistics daemon by means of the phion.a configuration module.

After an option has been changed, the **Show** button must always be clicked on in order to activate the setting options.

Fig. 9-7 Control field



#### Section **Options**

- **Statistics type**  
For the top file types, there is only the **Top list** statistic type
- **Src Filter**  
In this box, character strings can be entered, according to which IP address, port and protocol are to be filtered. Wildcards ? and \* can be used.
- **Clear**  
Button for re-setting the Src filter
- **Show**  
There is no minimum, maximum of average for top statistics.
- **Show** button  
The options that have been set are activated by a left mouse click
- **History**  
Via this button a dialogue is opened containing the last statistics displays and their settings.  
By clicking on the arrows (◀, ▶) previously set options are displayed.

#### Section **Top List**

- **instances**  
Options window for observation period. An individual instance can be selected by means of the left mouse button (day, month, or year). Several instances can be selected with STRG + left mouse button or with shift +

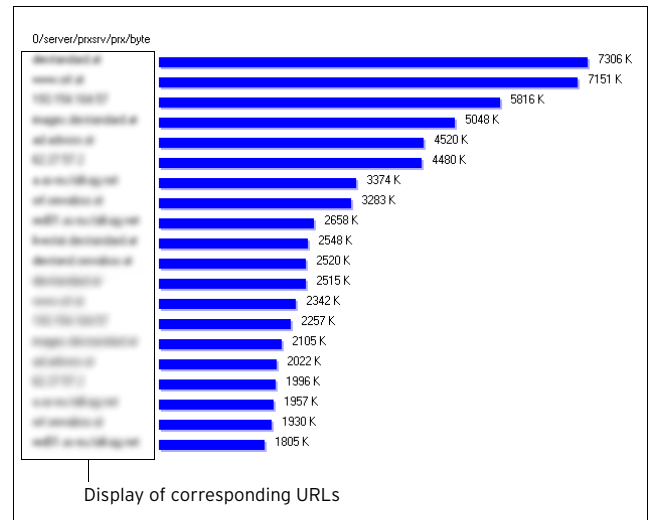
left mouse button. An individual instance can be selected by means of the left mouse button (day, month, or year). Several instances can be selected with STRG + left mouse button or with shift + left mouse button.

#### ➤ **Maximum Number shown**

Input box for determining the number of bars that are to be displayed

### 2.2.2 Graphs

Fig. 9-8 Example for Top list statistics



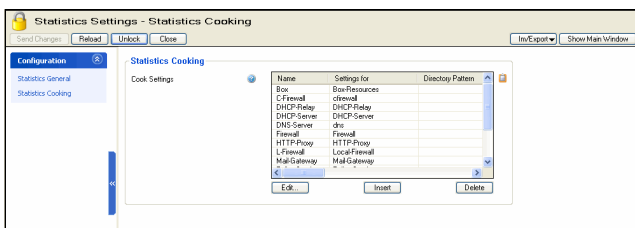
## 3. Configuration

The range of statistics files that may be viewed in the Statistics viewer depends on settings for:

- **Statistics generation by each service (Configuration Service** - List 3-91 Service Configuration - Statistics - section Statistics Settings, page 97). Default settings provide that all services generate statistics.
- **Configuration of the Statistics daemon** (see 3.1 Service Configuration).

### 3.1 Service Configuration

Fig. 9-9 Configuration dialogue - Statistics - Statistics Cooking







The statistics package represents an integral part of the phion box infrastructure and consists of two box services (`cstatd` and `qstatd`) as well as an utility program (`dstats`), which is regularly invoked by cron.

The utility `dstats` coarsens time resolution of accumulated statistical data according to configurable rules, and if specified eventually removes statistics files when they are no longer needed. In this latter regard it is related to the log file management utility `logstor`.

#### Note:

Both utilities need to be invoked. Default settings provide that both utilities are run as daily cronjobs by the cron daemon.

To open the **Statistics Daemon Configuration**, in the box menu click  **Config**, and then double-click  **Statistics** (accessible through  **Box** >  **Infrastructure Services**).

The following configuration options are available:

#### Statistics General view

List 9-4 Infrastructure Services - Statistics General - section Global Settings

Parameter	Description
<b>Corrupted Data Action</b>	<p>This option defines the action <code>dstats</code> executes when it recognises a corrupted DB file. The following options are available:</p> <ul style="list-style-type: none"> <li>➤ <b>Delete</b> - deletes the corresponding DB file (default).</li> <li>➤ <b>Archive</b> - moves the DB file to a lost+found directory</li> </ul> <p><b>Note:</b> Recognising a corrupted data file always triggers the event <b>Corrupted Data File</b> [150].</p> <p><b>Attention:</b> Regardless of the configured action a corrupted data file, which prevents <code>cstatd</code> from actually collecting statistics is always removed. Beside the event <b>Corrupted Data File</b> [150] the following log file entries are written: Fatal "Watchdog: SIGSEGV detected" Fatal "CSTAT: DoCleanup" Fatal "Remove corrupt stat file: /var/phion/stat/_filename_" Fatal "CSTAT: DoCleanup finished"</p>

List 9-4 Infrastructure Services - Statistics General - section Global Settings

Parameter	Description
<b>Disc Write</b>	<p>This option defines the statistics data types that should be recorded and written to the harddisk. The following options are available:</p> <ul style="list-style-type: none"> <li>➤ <b>On</b> (default) - Box and Server statistics are written to disk</li> <li>➤ <b>Off</b> - No statistics are written to disk</li> <li>➤ <b>Box_only</b> - Only box statistics are written to disk</li> <li>➤ <b>Server_only</b> - Only server statistics are written to disk</li> </ul>
<b>Skip Null Stats</b>	<p>This parameter steers the behaviour of <code>cstat</code> concerning 0 byte or 0 connection statistics. When set to <b>yes</b> (default: <b>no</b>) empty statistics files will be omitted when writing to the harddisk.</p>
<b>Query Process Priority</b>	<p>In case of high CPU load during statistical queries this parameter allows decreasing process priority (range <b>0</b> (highest) - <b>19</b> (lowest); default: <b>8</b>).</p>

#### Statistics Cooking view

List 9-5 Box Services - Statistics Cooking - section Statistic Cooking - section Cook Settings

Parameter	Description
	<p>In this section it may be defined how <code>dstats</code> should handle specific data types.</p>
<b>Settings for</b>	<p>In this field, select the software module to whose statistics data the settings below should apply. In the list, all software modules with appropriate default configuration are available that generate statistics data. Optionally, <b>Pattern-Match</b> may be selected to define a file pattern that should apply for cooking of statistics data. Selecting <b>Pattern-Match</b> enables the <b>Directory Pattern</b> field below, which expects insertion of an applicable file pattern.</p>
<b>Directory Pattern</b>	<p><b>Pattern-Match</b> settings apply to statistics files available in sub-folders of <code>/var/phion/stat</code>. Patterns may be specified by either inserting full folder names or by using wildcards (? and *), in which the question mark wildcard (?) stands for a single character and the asterisk wildcard (*) stands for an arbitrary number of characters.</p> <p><b>Attention:</b> Generally, there is no need to make use of directory patterns when specifying cooking settings, as the default settings suffice most needs. If you do use directory patterns, make sure that they do not interfere with the module settings configuration. For a specific data type always use EITHER module OR directory pattern settings. <code>dstats</code> works through the configured instances successively, and will omit directory patterns that apply to directories it has already processed. Additionally, for clearly arranged management, place directory patterns at the end of the configuration file.</p> <p><b>Example pattern:</b> To include all statistics files starting with 'conn' generated by the VPN services running on servers <b>s1</b> and <b>s2</b>, insert the following pattern structure: <b>Actual file structure:</b> <code>/var/phion/stat/0/server/s1/vpn/conn&lt;xxx&gt;</code> <code>/var/phion/stat/0/server/s2/vpn/conn&lt;xxx&gt;</code> <b>Directory pattern:</b> <code>*/server/s*/vpn/conn*</code> <b>Attention:</b> Avoid too openly defined patterns spanning multiple folders, such as <code>*/server/*/*</code>. If you do use patterns spanning multiple folders, be aware of their implication and always position them at the list bottom.</p>

List 9-6 Statistic Cooking- section Type: Time

Parameter	Description
	<p><b>Note:</b> Options in this section apply to <b>Time</b> statistics only (like <b>byte (Time for Dst)</b>, <b>conn (Time for Src)</b>, ...).</p>

List 9-6 Statistic Cooking- section Type: Time

Parameter	Description
<b>Resolution 1h after (Days)</b>	Number of days, after which the granularity of statistics data of type time should be increased to one hour. Data more recent than the inserted number of days will not be affected.
<b>Resolution 1d after (Days)</b>	Number of days, after which the granularity of statistics data of type time should be increased to one day. <b>Note:</b> The period between cooking from hour to day granularity has to be 2 days minimum. If set to 1 day it will result in a summary offset for hourly granularity of 0 days per instance. This will lead to an error message in the <code>dstat</code> log file similar to the following: <b>Cannot create, file byte.hour_tot&lt;cookInstStartTS&gt; exists already.</b>
<b>Delete Data after (Days)</b>	Number of days, after which statistics data of type time should be deleted.

List 9-7 Statistic Cooking - section Type: Top

Parameter	Description
	<b>Note:</b> Options in this section apply to <b>Top</b> statistics only (for example <code>byte (Top Dst)</code> , <code>conn (Top Src)</code> , ...).
<b>Condense Data after (Days)</b>	Number of days, after which statistics data of type top should be merged into larger temporal bins. Data more recent than the inserted number of days will not be affected.
<b>Delete Data after (Days)</b>	Number of days, after which statistics data of type top should be deleted.
<b>Resolution</b>	Available resolutions are <b>weekly</b> and <b>monthly</b> . Settings trigger data rearrangement so as to be representative of an entire week or a month. <b>Attention:</b> It is recommendable only to change this parameter as long as the system is not productive. Thoughtless modifying may cause imprecise visualisation in the statistics viewer due to incomplete cook instances.

**Statistic Transfer view**

List 9-8 Statistic Transfer - Transfer Settings

Parameter	Description
	<b>Note:</b> This section is only available if the box is MC-administered. Configuration is required in context with collection of statistics files by the <b>MC-StatCollect</b> service ( <code>dstatm</code> ) running on the management centre. For a description of configuration options, see <b>phion management centre</b> - 9.4 Transfer Settings, page 440.

**Calculation of cooking and deletion offsets:**

Local compression cooking and deletion are configured separately for **Time** and **Top** statistics by providing the earliest point in time when an action (cooking or deletion) should be performed. These points in time are specified incrementally as number of days in the past.

*Example:*

On October 15, an offset of **5** means, that file instances from an earlier date than October 9 through October 9 should be processed. File instances from October 10 through October 14 (which indicates an offset of 5 days) and additionally October 15 should remain uncooked.

Time statistics may be cooked in a 2-level approach: In the first level cooking granularity is increased to 1 hour, in the second to a full day. The second level can only be enabled if the first is enabled, too. It is intended for providing the data for long-term trends, for example data for disk utilisation. The number of days that will be stored within a single cook instance is calculated out of the specified offsets.

For Top statistics only a one-level approach is available, because the additionally attainable factor of compression is primarily data-dependent and cannot be estimated reliably. Cooking granularity may be either weekly or monthly.

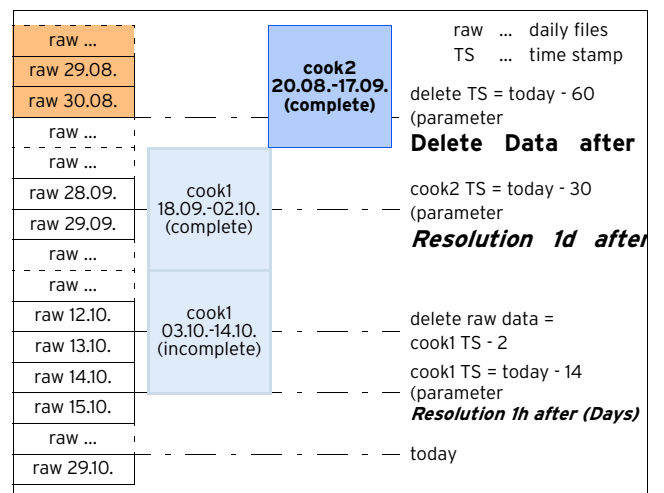
Deletion of obsolete file instances is as well controlled by offset specification.

**Note:**  
These offsets determine when statistics data is obsolete and that they are used for calculation of cooking parameters.

On the other hand cooking offsets imply the offset when raw data files become obsolete and can be deleted. See figure 9-10 to understand the relationship between configuration parameters.

The length of a cooking instance can be calculated using the equation  $[(\text{cook1 TS} - \text{cook2 TS}) - 1] * 2$ .

Fig. 9-10 Event chain of a cooking instance



## 4. Advanced Topics

### 4.1 Cooking of Statistics

The following chapter explains a feature that can only be understood with some deeper insight into the statistics module.

Figure 9-11 shows firewall connection time statistics, reaching from March 08 to March 16, with minimum and maximum values enabled. As we can see there are no minimum and maximum values available for March 08 to 10. Querying the same time statistics starting with March 09 (figure 9-12) results in minimum and maximum values on March 09 and 10. This is not an error in the statistics module, but can rather be explained by examining the data instances used to satisfy a request. Furthermore, this scenario may only occur for transfer rates (bytes or connections per time unit).

Fig. 9-11 Timed connection statistics starting at 08.03.

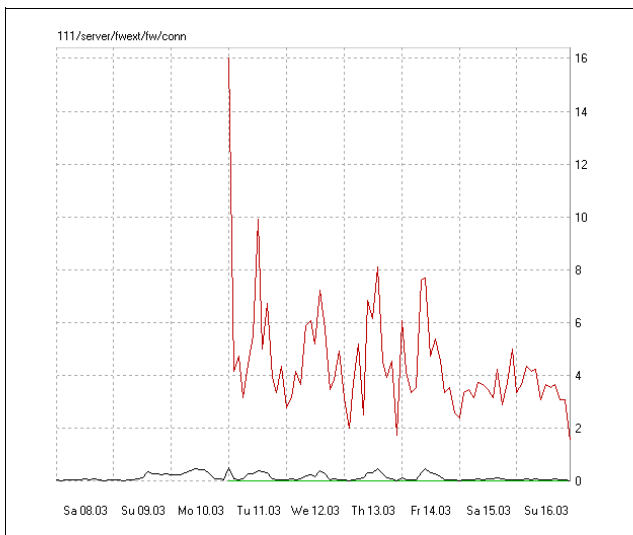
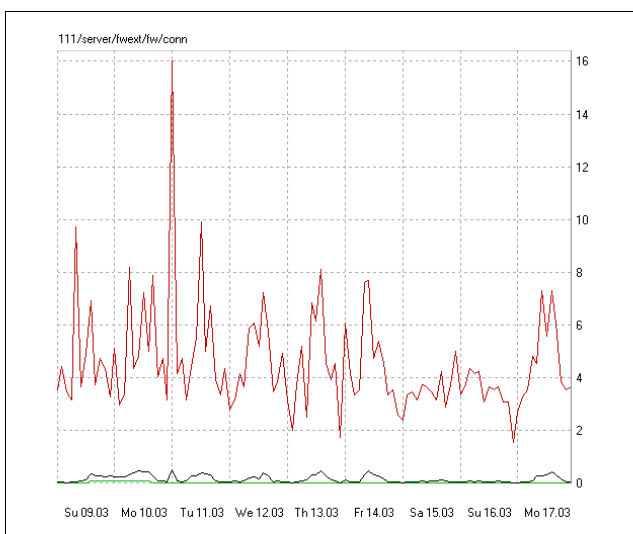


Fig. 9-12 Timed connection statistics starting at 09.03.



Statistical data is stored in separate file instances. The collected data with the highest time resolution is stored in daily files containing one day per file (*raw* data). After some time the data may be compressed to a time resolution of one hour and stored in files that contain multiple days (*cooked* data). The number of days stored in a compressed (*cooked*) instance depends on the specific configuration settings. It is important to state that such a cooked instance does not contain minimum and maximum values, because here they are of no significance.

For the given firewall service, the full time resolution is only available for March 09 and earlier. Before this date, time statistics are compressed. This is the reason for the above mentioned divergence. The query in figure 9-11 uses the cooked data for March 8 to 10 and covers the analysis of the remaining days with raw data. Minimum and maximum values are available with the first raw data instance used, which is March 11. The statistics module can execute the query in figure 9-12 with raw data files only, and thus presents minimum and maximum values over the whole time interval.

### 4.2 Dealing with a Box in the "Future"

#### How to solve problems related to time drift on boxes

Incorrect time settings on a box will amongst others result in falsified statistics data. This falsification is even of more concern if the box is MC-administered.

Time settings on MC-administered boxes and on the MC itself have to run in a synchronised mode to allow for correct operation of several functions described below. Usually, NTP is used to guarantee this. A deviation in time settings can occur if the administrator changes date and time manually or if the BIOS clock drifts while NTP is not available.

Box time going behind the actual time or behind MC time is a minor problem, because in this case the system's self-healing process will provide readjustment soon after having reset box time settings manually to the correct values (see below, 4.2.1).

Consequences of box time going ahead of the actual time or ahead of MC time are more time-consuming to repair. The bigger the drift, the higher the effort has to be. Depending on whether you expect the statistics data to be correct on a quantity basis or correct on time entries, the following solutions are possible:



## 4.2.1 Self-healing for Quantitative Preference

**cstatd** checks at a day's change over if current files have to be switched, hereby using the file's date header. Files currently in active use will be transferred into a historical file with corresponding date ending if their header date lies in the past.

Assuming box time settings are behind, the statistics files will be transferred to a historical file on the next day and "self-healing" will be completed. The statistics files will lack some time entries.

Assuming box time settings are ahead, you have corrected these time settings manually. **cstatd** comes upon a file containing a future date and will in an analogous manner leave it at this date, then continue using it for statistics writing until the header date is equal with the actual date. When the file is then switched, it will contain data with diverging time entries from more than one day. "Self-healing" is completed and a new day file is written.

**Note:**

Even on MC-administered boxes there is not necessarily the need for further manual corrections concerning the reorganisation of statistics files. After having adjusted the time settings on the box you may wait for the next **dstats** process. This will detect **toSend** files with a future time stamp in `/var/phion/dstats/` which have not yet been delivered to the MC (which means that no **masterAccept** file is available). The **dstats** process will remove these files and create them freshly.

## 4.2.2 Manual Correction for Time Preference

When diverging time entries in statistics and logging files should be avoided, the following steps have to be undertaken for readjustment.

### 4.2.2.1 Required Actions on the Box

**Step 1 Statistics**

- Block `cstat`.
- Delete all sub-folders and files in `/var/phion/stat/`.
- Delete all files with future timestamp in `/var/phion/dstats/`.
- Set the correct time on the box.
- Restart the phion subsystem to assure that all sub processes resume the correct time settings.

**Step 2 Log cache**

- Block `logd`.
- Delete sub-folders and files in `/var/phion/logcache/`.
- Set the correct time.

**Step 3 Logs**

- If possible delete sub-folders and files in `/var/phion/logs/`.
- If deleting is not possible move the contents from `/var/phion/logs/` to another directory.
- If no action is taken, querying the statistics files with the `phion.a` GUI will further on result in incorrectly displayed timeline events. Moreover the cache files will continue to contain duplicate entries, even after the time settings have been adjusted.

**Note:**

If the box was running for one day with wrong time settings you should check directory `/var/phion/dstats`.

**Attention:**

On MC-administered boxes do not delete statistics with time stamps smaller or equal to the highest `masterAccept` time stamp. These statistics have already been collected by the MC, and they will there be overwritten with completely new files if these have a smaller time stamp.

### 4.2.2.2 In Addition to the Actions on the Box do the Following on the MC

**Step 4 Main statistics**

- Block `dstatm`
- Delete files with a wrong time stamp in sub-folders of `/var/phion/mainstat/`
- Delete `toSend`-files with a wrong time stamp in `/var/phion/dstats/`
- If present delete the folder `/var/phion/dstats/tmp/`
- Set the correct time.

### 4.2.3 Further Issues

Especially on MC-administered boxes time drift might cause some other problems as well. Below you will find a brief summary of known issues and an instruction how to correct them.

#### 4.2.3.1 Licenses

Wrong time settings may lead to incorrect license handling. Licenses may not yet be valid though they should be, or they lose their validity too early. Licenses of MC-administered boxes cannot be validated correctly against the MC if the time difference between these two systems is too large. The grace period of Floating Licenses might get exceeded.

Restarting the `rangeconf` service on the MC or the control service on the administered box is another source of error on incorrectly adjusted systems. The restart will involve a license validation and if this fails box licenses might get deactivated immediately.

- Move the file `/opt/phion/preserve/licstamp` on the administered box to another place.

**Attention:**

The services will be stopped by this action.

- Set the correct time.
- Restart the `rangeconf` service on the MC.
- Restart the control service on the box.

#### 4.2.3.2 Time Restrictions defined by Firewall Rule Sets

With wrong time settings the restrictions will take effect untimely.

- Adjusting the box time is the only required action to solve this problem.

#### 4.2.3.3 Dynamic Firewall Rules

With wrong time settings the defined firewall rules will be activated and respectively deactivated untimely.

- Adjusting the box time is the only required action to solve this problem.

#### 4.2.3.4 Access Cache

With wrong time settings the date and time entries in the Access Cache will be incorrect.

- Adjusting the box time will solve this problem.
- In addition to this adjustment flush the Access cache with the command `acpfctrl cache flush all`.

#### 4.2.3.5 Cron Jobs

With wrong time settings Cron Jobs will be executed untimely.

- Adjusting the box time is the only required action to solve this problem.

#### 4.2.3.6 Mail Gateway

Wrong time settings will lead to a divergence between the retrieving and the delivery time of e-mails.

- Adjusting the box time is the only required action to solve this problem.
- If there are still many e-mails in the queue, which you wish to be stamped with the correct date and time, you may optionally delete the databases `spool.db` and `history.db` in the directory `/phion0/spool/<server_servicename>`. They will then be created freshly.

# Eventing

<b>1.</b>	<b>Overview</b>	
1.1	General .....	306
<b>2.</b>	<b>Event Configuration</b>	
2.1	General .....	306
2.1.1	Events Tab .....	306
2.1.2	Severity Tab .....	307
2.1.3	Notification Tab .....	308
2.1.4	Server Action Tab - Execute Program .....	309
2.1.5	Basic Tab .....	311
2.2	Event Monitoring .....	311
2.2.1	General .....	311
2.2.2	Confirm Events .....	313
2.2.3	Delete Events .....	313
2.2.4	Alarm Types / Disable Alarm .....	313
2.2.5	Filter Settings .....	314
2.2.6	Event Monitor - Live Mode .....	314

# 1. Overview

## 1.1 General

The event module displays current information about the netfence gateway.

Whenever an event is generated, the counting device for this event will be increased. If this counter reaches its (configurable) limit the system will go into alarm condition.

Via the so-called **Notification** type you are able to define actions that are carried out if a certain event is triggered (like mails, program executions, SNMP traps; see 2.1.3 Notification Tab, page 308).





### Attention:

The event monitor should be used as a tool to get a quick overview of the system(s). In order to maintain the event monitor's usability it is recommended to delete older entries. The statistics and the log module are created to recall the past.

# 2. Event Configuration


## 2.1 General

The Event Configuration window allows for viewing of events that are generated on netfence systems and customising of event handling.

To open the Event Configuration window, double-click  **Eventing** (accessible through  **Config** >  **Box** >  **Infrastructure Services**).

Event processing is determined by customisable settings that can be configured in the following tabs:

- **Basic tab**  
Use this tab to define general parameters for event propagation and default settings for alarm notifications (see 2.1.5 Basic Tab, page 311).
- **Notification tab**  
Use this tab to customise existing or define additional notification types (see 2.1.3 Notification Tab, page 308).
- **Severity tab**  
Use this tab to view severity categorisations and optionally to modify notification types associated with them (see 2.1.2 Severity Tab, page 307).
- **Events tab**  
Use the Events tab to view a listing of all available event types and optionally to customise event handling, Severity ID and Notification ID settings for each specific event (see 2.1.1 Events Tab, page 306).

Events are visualised in the **Event Monitor**. Access it by clicking the  **Events** icon in the box menu (see 2.2 Event Monitoring, page 311). On a single box, the event monitor lists all events that have been generated on the box itself. On a management centre (that has been accessed using the **MC-Address** in the phion.a login screen), the event monitor lists events that have been generated by the MC-Services and events from the boxes the MC administers, if these events have been configured to be propagated to the MC.

Event propagation to an MC and notification settings are configurable in multiple places.

The configured settings are processed in the following sequence:

### Event propagation to an MC

- The parameter setting **Send Event to MC** in the Basic tab (see page 311) defines if boxes shall generally propagate their events to the management centre or not. The checkbox is selected by default. If cleared, events are never propagated. The setting in the Basic tab overrules the settings defined in the other configuration areas.
- The parameter setting **Propagate to MC** in the Severity tab (see page 308) defines general propagation of events that are assigned with a specific Severity ID. This setting may be overruled by customised settings for specific events in the Events tab. When the checkbox is cleared in the Severity tab, it is automatically cleared as well from all events that are associated with the corresponding severity category.
- The parameter setting **Propagate to MC checkbox** in the Events tab (see page 307) overrules the setting specified in the Severity tab.

### Generation of notifications

In the Severity tab a notification type is associated with each Severity ID. This assignment may be overruled by defining event specific notification settings in the Events tab.

## 2.1.1 Events Tab

The **Events** tab contains a listing of all events that may be generated on self-managed netfence gateways and management centres. For a complete list of all available events see **System Information** - 5. List of Default Events, page 516.

The listing is divided into the following columns:

**Table 10-1** Overview of events in the Events tab

Column	Description
<b>ID</b>	This is the Event-ID.
<b>Description</b>	This event description is written to the event monitor GUI and to logging facilities. The event description is sometimes extended by additional information in case the event may be triggered by multiple processes.
<b>Severity ID</b>	This is the severity level that has been assigned to the event.
<b>Severity</b>	This is the severity description. Severity categories range from informational events to security events.
<b>Notification ID</b>	This is the effective notification setting applying to the event.
<b>Notification</b>	This is the notification description.
<b>Pers.</b>	This is the effective persistency setting of the event. This setting is only of interest on MC-administered boxes (see Persistent checkbox, page 307).
<b>Prop.</b>	This is the effective setting for propagation of the event to an MC. This setting is only of interest on MC-administered boxes (see 2.1 General, page 306).
<b>Drop</b>	This is the effective setting for dropping of the event (see <b>Drop Event checkbox</b> , page 307).

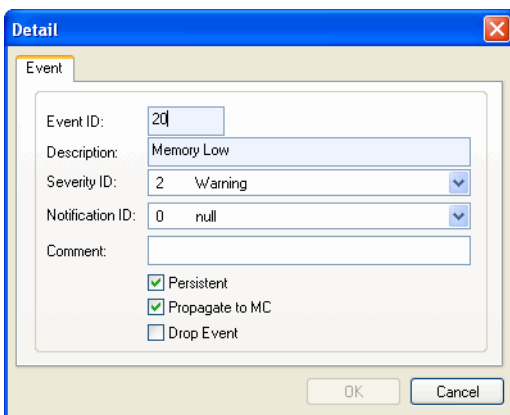
The following functional elements are placed at the bottom of the listing:

- **Lookup** field  
Insert the object ID of the element you are looking for here to find it quickly.
- **Change ...** button  
Double-click or select a list entry and click the **Change ...** button to open the object for editing.

### 2.1.1.1 Change an Event Entry

To change the properties of an event, lock the configuration dialogue, select the event, then open it by double-clicking. This makes available the **Detail** window.

**Fig. 10-1** Event detail window



The following event details may be configured:

**List 10-1** Events tab - Event details

Parameter	Description
<b>Event ID</b>	This is the unique Event-ID (read-only).
<b>Description</b>	This event description is written to the event monitor GUI and to logging facilities (read-only).
<b>Severity ID</b>	This is the severity level of the event. Severity levels reach from informational to security event generation. They determine the notification type that should be triggered when the event occurs. Note that the Notification ID setting below may override the notification assignment within the severity settings. For information on severity settings see 2.1.2 Severity Tab, page 307.

**List 10-1** Events tab - Event details

Parameter	Description
<b>Notification ID</b>	This is the notification setting applying to the event. The Notification ID determines alarm actions that should be initiated when the event occurs (like e-mail generation, pop-up of alarm messages, ...). For information on notification settings see 2.1.3 Notification Tab, page 308. Setting to " <b>0 null</b> " means that notification settings shall be inherited from the configuration defined in the Severity tab (see 2.1.2 Severity Tab, page 307).
<b>Comment</b>	Optionally insert a customised event description into this field.
<b>Persistent checkbox</b>	This parameter is only of interest on MC-administered boxes. When selected (default) the event is only propagated to the MC once, even if occurring frequently. Before it can be propagated anew, it has to be deleted on the MC. This measure may be taken to prevent excessive event propagation.
<b>Propagate to MC checkbox</b>	This parameter is only of interest on MC-administered boxes. When selected (default) generated box events are propagated to the MC. <b>Note:</b> This setting overrides the equivalent setting in the Severity tab (see page 308). Refer to 2.1 General, page 306 to understand the processing logic.
<b>Drop Event checkbox</b>	Events that have been appointed for dropping (checkbox selected) are neither inserted into the local DB nor are they propagated to an MC.

- Click **Send Changes** and **Activate** to activate your changes.

### 2.1.1.2 Font Styles used in the Event Tab

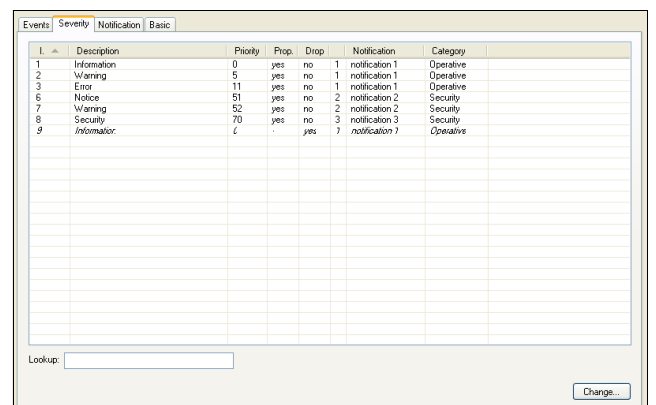
The following ID font styles apply for event depiction:

**Table 10-2** Font styles characterising event settings

Font style	Description
angle and weight regular	Settings for this event have not been customised. They are inherited from settings defined in the Severity tab.
angle regular/weight bold	The Notification ID for this event has been customised and thus overriding the ID defined in the Severity tab. This event has been appointed for dropping in the Severity tab but the setting has been revoked in the Event tab.
angle italic/weight regular	This event has been appointed for dropping through customisation of Severity ID settings in the Severity tab.
angle italic/weight bold	The event has been appointed for dropping in the Event tab thus overriding the inherited setting configured in the Severity tab.

## 2.1.2 Severity Tab

**Fig. 10-2** Severity tab



List 10-2 Severity tab - Column view

Column	Description
<b>ID</b>	<p>Displays the severity ID. The following severity IDs with corresponding default descriptions are in use:</p> <ul style="list-style-type: none"> <li>➤ <b>Operative Events</b> <ul style="list-style-type: none"> <li>ID 1 - Information</li> <li>ID 2 - Warning</li> <li>ID 3 - Error</li> </ul> </li> <li>➤ <b>Security Events</b> <ul style="list-style-type: none"> <li>ID 4 - Notice</li> <li>ID 5 - Warning</li> <li>ID 6 - Security</li> </ul> </li> </ul> <p><b>Note:</b> An event's severity ID is responsible for the colour visualisation coming to effect in the status map of the box (<b>Getting Started</b> - 3.2.1 Start Screen, page 18) and, if the box is MC-administered and events are propagated to it, in the status map of the MC Control Centre (<b>phion management centre</b> - 5.2 Status Map Tab, page 397). The events generate the following colour depiction:</p> <ul style="list-style-type: none"> <li>➤ IDs 1 (Information) and 4 (Notice) &gt; <b>green</b></li> <li>➤ IDs 2 and 5 (Warning) &gt; <b>yellow</b></li> <li>➤ IDs 3 (Error) and 6 (Security) &gt; <b>red</b></li> </ul>
<b>Description</b>	This severity description is written to the event monitor GUI and to logging facilities.
<b>Prop.</b>	This is the setting for propagation of the event to an MC. This setting is only of interest on MC-administered boxes. It may be overruled by customising settings in the Events tab (see 2.1.1 Events Tab, page 306).
<b>Drop</b>	This is the setting for dropping of the event (see <b>Drop event</b> below). It may be overruled by customising settings in the Events tab (see 2.1.1 Events Tab, page 306).
<b>Notification ID</b>	This is the notification setting applying to all events assigned with the given Severity ID. The notification setting may be overruled by customising settings in the Events tab (see 2.1.1 Events Tab, page 306).
<b>Notification</b>	This is the notification description.
<b>Category</b>	This is the category the event is assigned to. Categories are <b>Operative</b> and <b>Security</b> events.

### 2.1.2.1 Modification of the Severity

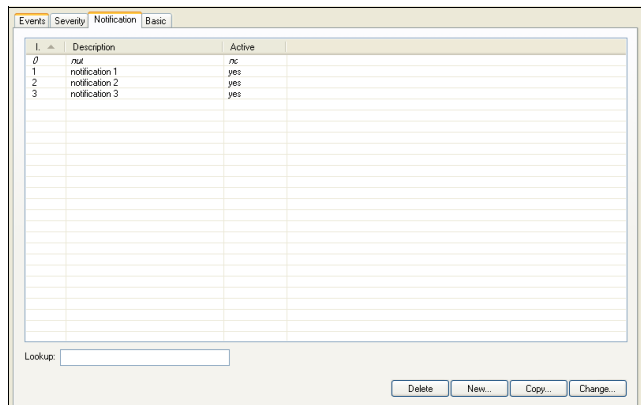
By double-clicking a severity entry the dialogue for editing is opened:

List 10-3 Severity tab - Severity details

Parameter	Description
<b>Severity ID</b>	This is the unique Severity-ID (read-only).
<b>Description</b>	This is the customisable severity description.
<b>Notification ID</b>	This is the notification setting applying to all events assigned with the given Severity ID. The Notification ID determines alarm actions that should be initiated when the event occurs (like e-mail generation, pop-up of alarm messages, ...). For information on notification settings see 2.1.3 Notification Tab, page 308. The notification setting may be overruled by customising settings in the Events tab (see 2.1.1 Events Tab, page 306).
<b>Propagate to MC</b>	This parameter is only of interest on MC-administered boxes. When selected (default) generated box events are propagated to the MC. Note that this setting may be overridden by the equivalent setting in the Events tab. Refer to 2.1 General, page 306 to understand the processing logic.
<b>Drop event</b>	<p>Events that have been appointed for dropping (checkbox selected) are neither inserted into the local DB nor are they propagated to an MC.</p> <p><b>Note:</b> This setting may be overridden by the equivalent setting in the Events tab.</p>

## 2.1.3 Notification Tab

Fig. 10-3 Notification tab



ID	Description	Active
0	<i>new</i>	no
1	notification 1	yes
2	notification 2	yes
3	notification 3	yes

### Attention:

An entry displayed in *italic* indicates that the notification is inactive and an alarm condition will never be reached.

The following buttons are available:

- **Delete**  
Deletes the selected entry
- **New**  
Creates a new entry
- **Copy**  
Duplicates the selected entry
- **Change ...**  
Changes the selected entry

Using the buttons **New**, **Change ...** or simply by double-clicking on an entry opens the Detail dialogue.

### Global settings

#### Note:

Be aware of the Notification ID. If the background is light yellow it indicates that the notification is in use either by an event or severity.

If you have to delete notification or change its notification ID, delete notification settings at respective events and severities that use this notification (referential integrity).

Until this is done, the Notification ID can be changed/deleted.

List 10-4 Notification tab - Column view

Column	Description
<b>Notification ID</b>	Adding and/or copying: this value has to be unique.
<b>Description</b>	Description of the notification
<b>Event must be confirmed</b>	If this checkbox is selected, the event is in alarm status until the user confirms it.



### 2.1.3.1 Server Action Tab - Mail

By ticking the checkbox **Enable** and selecting the server action **Mail** (**Type** menu), events that are using this notification ID create a mail that is, for example, sent to the corresponding administrator.

Fig. 10-4 Server Action tab - Type Mail

**Note:**

If the basic tab (see 2.1.5 Basic Tab, page 311) is already configured, the set default values will be pre-entered.

The sender ID has to be entered into the field **From**. It is recommended to use the box name and its domain to have a clearly identifiable ID.

The field **To** holds the mail address where the event mail is sent to.

In the **Mail Server** field the IP address or resolvable name of the affected mail server has to be entered.

If the global settings **Event must be confirmed** (see Global settings) is selected, the checkbox **Repeat every** is available. Activating this option unlocks the section below, where the specific repeat time interval is to be entered. Therefore, simply enter the wanted time interval (numeric type) and select the time unit (seconds). The event will repeat propagating mails until the user confirms the event in the event monitor.

### 2.1.4 Server Action Tab - Execute Program

By ticking the checkbox **Enable** and selecting the server action **Execute Program** (**Type** menu), events that are using this notification ID start a specific program.

Fig. 10-5 Server Action tab - Type Execute Program

Enter the path and the filename of the executable in the field **Parameter**. This can be any executable file on the netfence gateway.

**Note:**

Enter the path name like `/tmp/executable`.

If the global settings **Event must be confirmed** (see Global settings, page 308) is selected, the checkbox **Repeat every** is available. Activating this option unlocks the section below, where the specific repeat time interval is to be entered. Therefore, simply enter the wanted time interval (numeric type) and select the time unit (seconds). The event will repeat executing the program until the user confirms the event in the event monitor.

### 2.1.4.1 Server Action Tab - SNMP

By ticking the checkbox **Enable** and selecting the server action **SNMP** (**Type** menu), events that are using this notification ID propagate a SNMP trap to an external security event monitoring system.

**Note:**

It is recommended to create an explicit rule for SNMP traps in the local-out rule set (**UDP**, Port **162**) of your netfence gateway and/or management centre.

Fig. 10-6 Server Action tab - Type SNMP

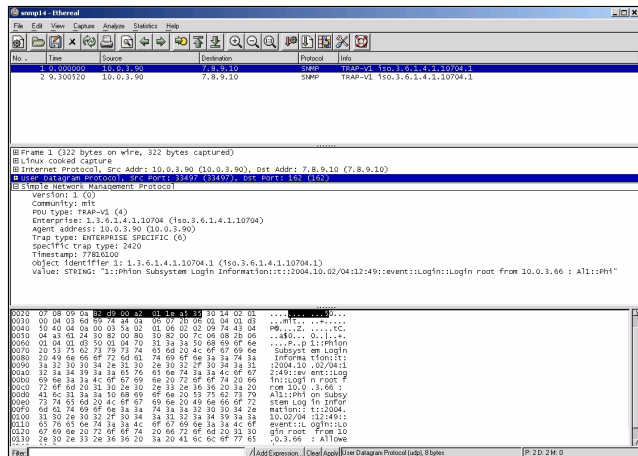
**Note:**

If the basic tab (see 2.1.5 Basic Tab, page 311) is already configured, the set default values will be pre-entered.

List 10-5 Server Action tab - Type SNMP

Column	Description
<b>Destination</b>	IP address of the external monitoring system.
<b>Spec Type</b>	Via this field the sent specific Trap PDU type is configurable according to the needs of the monitoring system. Alternatively, the unique event ID can be used for purpose (see below). <b>Note:</b> If network management software like <b>Tivoli NetView6000</b> or <b>HP Open View</b> is ought to receive SNMP traps, set this parameter to <b>1</b> .
<b>Use Event ID</b> checkbox	Ticking this checkbox causes the usage of the corresponding event ID as specific trap type. <b>Note:</b> If network management software like <b>Tivoli NetView6000</b> or <b>HP Open View</b> is ought to receive SNMP traps, do NOT activate this checkbox.
<b>Enterprise</b>	This line displays the registered phion company OID (1.3.6.1.4.1.10704).
<b>Community</b>	This field is used for entering the SNMP community where the netfence gateway is located in according to your community concept.

Fig. 10-7 Example for a SNMP trap



The section **Simple Network Management Protocol** depicted in figure 10-7 provides the following information:

Table 10-3 SNMP Parameters

Line	Value	Description
Version	1 (0)	used SNMP version
Community	mit	community as configured above
PDU Type	TRAP-V1(4)	used Trap PDU version
Enterprise	1.3.6.1.4.1.10704 (iso.3.6.1.4.1.10704)	phion's registered company OID
Agent address	10.0.3.90 (10.0.3.90)	address of transmitting system
Trap type	ENTERPRISE SPECIFIC (6)	used Trap type
Specific trap type	2420	in this case the event ID is available; if the checkbox <b>Use Event ID</b> is not selected, here the configuration of parameter <b>Spec Type</b> is displayed
Timestamp	77816100	systems uptime in seconds
Object identifier	1.3.6.1.4.1.10704.1 (iso.3.6.1.4.1.10704.1)	displays phion's enterprise OID and the sub-identifier (last digit, in this example 1). The MIB can be obtained from phion.
Value	1::Phion Subsystem Login Information::: 2004.10.02/04:12:49::event::Login root from 10.0.3.66 ...	here the human-readable event text is displayed; the submitted data is divided by double colon (::) and listed as follows: ID::Description::Type Description:: System date and time::Layer Description::Class Description::Data

If the global settings **Event must be confirmed** (see Global settings, page 308) is selected, the checkbox **Repeat every** is available. Activating this option unlocks the section below, where the specific repeat time interval is to be entered. Therefore, simply enter the wanted time interval (numeric type) and select the time unit (seconds). The event will repeat propagating SNMP traps until the user confirms the event in the event monitor. Take into consideration that the notification is sent only after confirming the event (using **Send - Reset Alarm**; see 2.2.1.1 Context Menu, page 312).

### 2.1.4.2 Client Action Tab

**Note:**

Client actions concern actions in phion.a (what happens at event monitoring).

To set actions, first select the **Enable** checkbox.

Choose between two possibilities:

➤ **Audio Alert**

plays an audio sound when an event with this notification occurs.

The sound specified must fit into available physical memory and has to be playable by an installed waveform-audio device driver.

It searches the following directories for sound files: current directory (where phion.a is located), windows directory, windows system directory, directories listed in the PATH environment variable, and the list of directories mapped in a network.

For example, the audio file **chord.wav** is in the same folder as phion.a.exe, type **chord.wav** in the input field **Parameter** or enter an absolute path (like **c:\temp\chord.wav** (enter path for Windows systems)).

➤ **Popup**

opens a pop-up window displaying the notification message, as soon as an event configured with this notification type occurs.

### 2.1.4.3 Thresholds (to Activate Notification) Tab

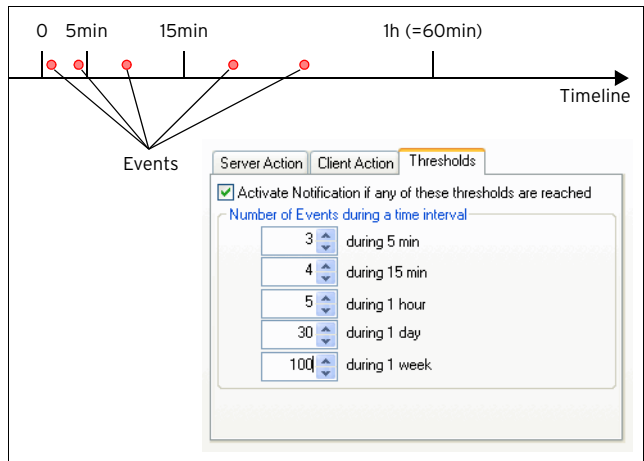
To limit the amount of events that are generated, there is a possibility to determine the time when an event entry should be generated.

**Note:**

When checkbox **Activate Notification if any of these thresholds are reached** is not selected, notification is **NOT** activated.

Example: an event occurs 5 times as follows:

Fig. 10-8 Example for occurring event and settings for Threshold tab



The example shown in figure 10-8 results in the following notifications:

**Table 10-4** SNMP notifications

After ... minutes	Event count	Activate notification at counter	Activate notification
5	2	3	no
15	3	4	no
60	5	5	yes

Assuming the settings above means that a wrong password is entered 5 times within 1 hour. This will generate one event entry because of the configuration **5 during 1 hour**.

Possible errors:

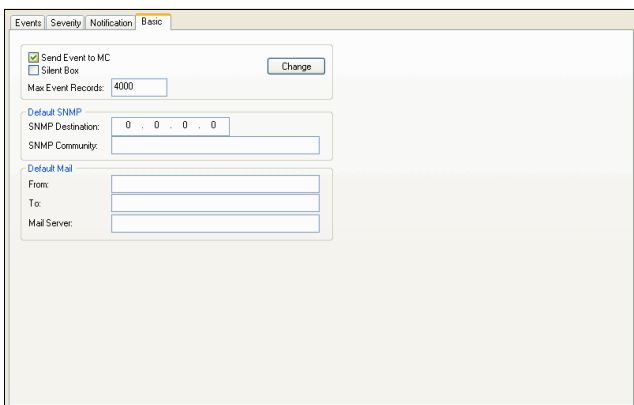
To use actions (server action or client action) select the **Enable** checkbox.

Check the tab **Thresholds** for correct entries (increasing values) and the checkbox **Activate Notification if any of these thresholds are reached**.

### 2.1.5 Basic Tab

Use this tab to define general parameters for event propagation and default settings for alarm notifications.

**Fig. 10-9** Basic tab



**List 10-6** SNMP Notifications

Parameter	Description
<b>Send Event to MC</b>	When selected (default), MC-administered boxes forward their events to the central eventing service (mevent) on the management centre. Event forwarding also applies to events that are generated on the management centre itself. <b>Attention:</b> This setting defines if boxes shall generally propagate their events to the MC. If cleared, events are never propagated. The setting in the Basic tab overrides the settings defined in the other configuration areas (Severity tab, see 2.1.2 Severity Tab, page 307 and Events tab, see 2.1.1 Events Tab, page 306).
<b>Silent Box</b>	Select this checkbox to disable event alarms and collect events only.
<b>Max Event Records</b>	This is the maximum number of event entries that shall be displayed in the Event Monitoring GUI (default <b>4000</b> ). Note that if this maximum has been reached new events will not be recorded in the Monitoring GUI. It is recommended to delete events on a regular basis and to refer to the Logs and Statistics Monitoring areas to recall the past.

**List 10-7** SNMP Notifications - section Default SNMP

Parameter	Description
<b>SNMP Destination</b>	IP address of the external monitoring system.

**List 10-7** SNMP Notifications - section Default SNMP

Parameter	Description
<b>SNMP Community</b>	This field is used for entering the community where the netfence gateway is located in according to your community concept.

**List 10-8** SNMP Notifications - section Default Mail

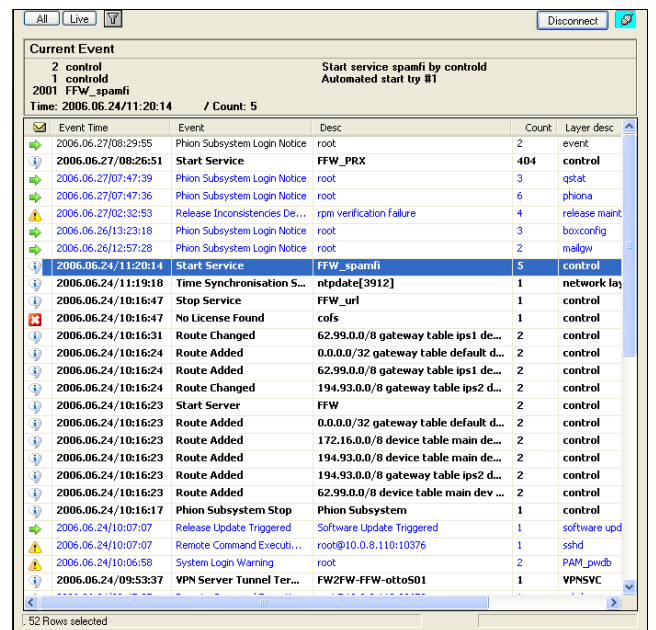
Parameter	Description
<b>From</b>	Sender ID. It is recommended to use the box name and its domain to have a clearly identifiable ID.
<b>To</b>	Holds the mail address where the event mail is sent to.
<b>Mail Server</b>	IP address or resolvable name of the affected mail server. <b>Attention:</b> After modifying the parameters be sure to click button <b>Change</b> in order to set the changes active.

## 2.2 Event Monitoring

### 2.2.1 General

To open the event monitor, click **Events** in the box menu of the graphical administration tool phion.a.

**Fig. 10-10** Event monitor



In the upper left of the dialogue are three buttons:

- **All**  
Update all current events.
- **Live**  
Listens continuously for new events. This also enables popup windows and sound; see 2.2.6 Event Monitor - Live Mode, page 314.
- (filter)  
Adapt a filter mechanism to all current events (see 2.2.5 Filter Settings, page 314).

**Note:** Notification messages are only enabled in live mode.

**Note:** Hence to have the event monitor in normal mode can be seen as a display of the current event system status.

**Severity status column**

This column contains the following icons (sorted ascending according to their priority):

- ⓘ Information
- ⚠ Warning
- ❌ Error
- ➡ Notice
- 🔒 Security

Different font colours and highlightings are used to indicate event importance:

- black normal text      Uncritical or already confirmed event
- blue normal text      New, not yet read event
- black bold text      Alarm event; Pay attention
- black italic      Alarm event temporarily disabled

**2.2.1.1 Context Menu**

To confirm an event, open the context menu by selecting the event and press the right mouse button. This opens the context menu shown in figure 10-11.

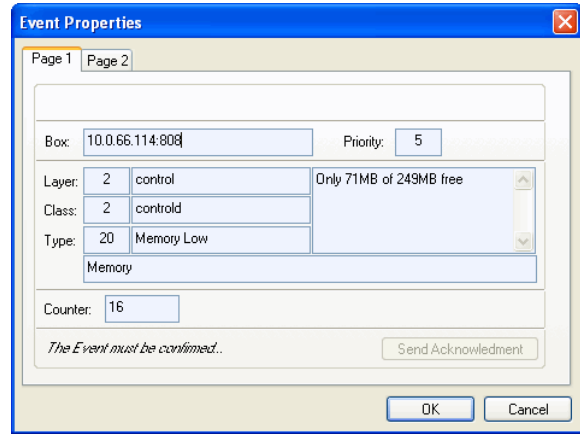
Fig. 10-11 Context menu



- **Send - Acknowledgment**  
Use this function to acknowledge events asking for confirmation. Acknowledging an event will terminate the alarm function, if the corresponding event has been configured with generation of warning notifications (playing of sound or generation of e-mail messages).
- **Send - Reset Alarm**  
This function has the same impact as event acknowledgement. In addition, it removes the warning icon ⚠ from the task bar.
- **Send - Mark as Read**  
This function is only available for uncritical events not asking for confirmation. It has the same impact as simply marking an event in the list for three seconds. Marking an event as read adds access information to the event properties "Page 2 tab" (figure 10-12, page 312).
- **Temporary Disable ...**  
Disables alarm conditions temporarily. Disabled events are displayed in *italic*.

- **Delete Event**  
Erases an event. It is recommended to delete older entries to keep a "compact" event monitor.
- **Properties ...**  
Displays details of a selected event

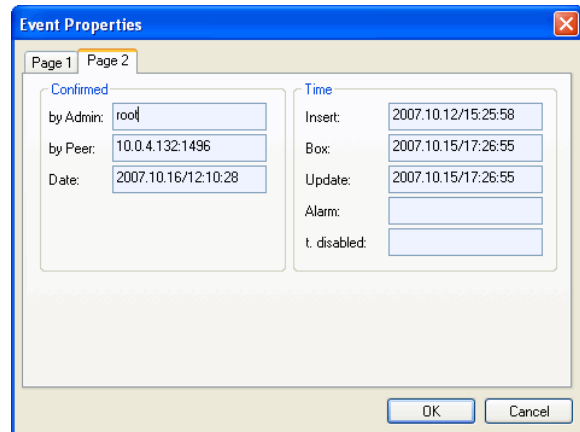
Fig. 10-12 Page 1 of the Properties dialogue



List 10-9 Event Properties - Page 1 tab

Parameter	Description
<b>Box</b>	IP address of the box that created the event
<b>Layer</b>	There are three layers. Layer 1 is boot-layer, layer 2 is box-layer and layer 3 is server/service-layer.
<b>Class</b>	Three types of classes can appear here. Class 1 is operative, Class 2 is resources and Class 3 is security.
<b>Type</b>	Event ID

Fig. 10-13 Page 2 of the Properties dialogue



List 10-10 Event Properties - Page 2 tab - section Confirmed

Parameter	Description
<b>Confirmed</b>	- <b>by Admin</b> - Who has confirmed the event? - <b>by Peer</b> - IP address of the management workstation - <b>Date</b> - Date and time when the event has been marked as read, that means confirmed.

List 10-11 Event Properties - Page 2 tab - section Time

Parameter	Description
<b>Insert</b>	Date and time when the event was inserted in the database
<b>Box</b>	Internal system information related to the insert time (please ignore this value).
<b>Update</b>	Date and time of status changes of this event (mark, read, acknowledge, ...)
<b>Alarm</b>	Date and time when the alarm had been sent
<b>t. disabled</b>	Date and time when the alarm was disabled temporarily


- **Columns ...**  
Shows/hides different table columns

Additionally, the context menu contains already well known selections like **Export List to Clipboard**, **Export Selected to Clipboard**, **Print List**, ...

### 2.2.1.2 Examples

- **Event in Alarm Condition, Event must be Confirmed**  
If an event is in alarm condition and the user has to confirm (not done yet), server action (box) will be enabled (send mail or others and repeat every n minutes).  
This box action will be repeated (if set in config), if the user confirms this event explicit (**Send - Acknowledgement**); user ID action at this event will be saved.
- **Event in Alarm Condition, Event must NOT be Confirmed**  
If an event is in alarm condition, a notification is displayed (a pop-up window) and the alarm is not stopped:  
No more notifications will come in the future; to enable notifications stop alarm.  
User action at this event will be saved.

## 2.2.2 Confirm Events

There are two types of event confirmation (this can be set in the  **Config** section of phion.a):

Normal events do not require confirmation.

Mark regarding alarm and wait 3 seconds; font will then change from **bold** or **blue** to black.

The second possibility is by selecting **Send - Mark as Read** from the context menu (right-mouse-button menu).

Alarms must be confirmed:

Mark the corresponding alarm, right-click and select **Send - Acknowledgement**.

**Note:**

The default mode of the of event monitor is static, i.e events are not updated continuously. After having made changes (for example, acknowledgements, alarm deletions, ...), click the **All** button to update the event list.

## 2.2.3 Delete Events


Deleting events is no particular difficult task when the phion netfence is administered by a management centre. To guarantee consistence of the eventing on both systems, the following procedure takes place:

- Step 1**    **Box: Event is considered to be deleted**
- Step 2**    **Box: Sends delete sequence to the MC**
- Step 3**    **MC: Deletes event from database**
- Step 4**    **MC: Sends acknowledgement to box**
- Step 5**    **Box: Deletes event from database**


**Note:**

If this procedure fails due to connection problems, the event entry will NOT be deleted. Refresh the view by clicking the **All** button to verify whether the event has been deleted or not.

## 2.2.4 Alarm Types / Disable Alarm

If an alarm occurs, a yellow alert sign () is displayed in the taskbar.

To see alert details, move the mouse over the icon. A left-mouse click opens the event monitor.

Alarm notifications can be configured in the  **Config** section of phion.a.

The following alarm types are available:

- **Playing of sound**  
If the configured sound file is not available, a couple of bars from Beethoven (Elise) is played.
- **Warning pop-up window**  
A window displaying the warning message pops up.

An alarm can be disabled as follows:

- **Temporary Disable**  
Mark the event in the list and open the context menu through clicking the right mouse button. Then select the entry **Temporary Disable**. Enter the wanted time interval for which the alarm should be turned off.  
To use **Temporary Disable**, mark the alarm and click right to enter the context menu. Now you may enter the amount of time, in which alarm shall be disabled.  
After entering the time and clicking **OK**, the event will be displayed **italic**.


**Attention:**

Temporarily disabled events will not use the alarm communication (pop-up window, sound) to the user for this time (if alarm options are set).

**Note:**

If an event has to be confirmed and is in alarm condition, deleting alarm will also delete request for acknowledgement.  
If an alarm is stopped, repeating server actions (mail, executable on box, ...) will stop also.

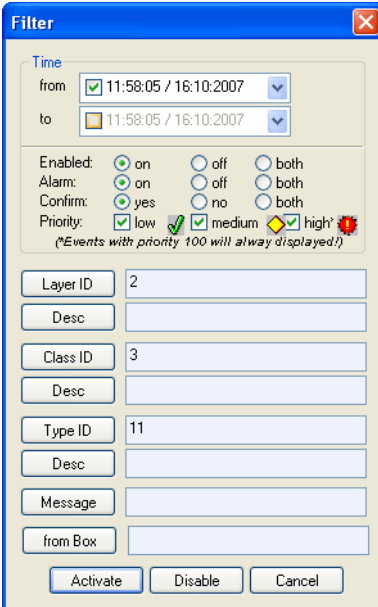
## 2.2.5 Filter Settings

To narrow down the view in the listing, filter options can be applied. To open the **Filter** dialogue, click the filter button .

The aim is only to display the following event types:

- Events with Layer ID 2
- Events with Class ID 3
- Events with Event ID 11
- Time restrictions shall not apply.

Fig. 10-14 Filter dialogue with values according to the example

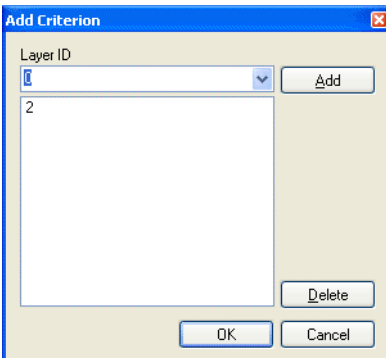


The Filter dialogue box contains the following fields and options:

- Time:** from 11:58:05 / 16:10:2007, to 11:58:05 / 16:10:2007
- Enabled:**  on,  off,  both
- Alarm:**  on,  off,  both
- Confirm:**  yes,  no,  both
- Priority:**  low,  medium,  high (Events with priority 100 will always be displayed!)
- Layer ID:** 2
- Desc:** (empty)
- Class ID:** 3
- Desc:** (empty)
- Type ID:** 11
- Desc:** (empty)
- Message:** (empty)
- from Box:** (empty)
- Buttons: Activate, Disable, Cancel

To enter values click on (for example) the **Layer ID** button to open the **Add Criterion** dialogue.

Fig. 10-15 Add Criterion dialogue



The Add Criterion dialogue box contains the following fields and options:

- Layer ID:** 2
- Buttons: Add, Delete, OK, Cancel

Enter the corresponding value into the pull-down field (for example, field **Layer ID**) and click **Add**. Clicking on **OK** closes the **Add Criterion** dialogue and sets the value in the corresponding field of the **Filter** dialogue.

## 2.2.6 Event Monitor - Live Mode

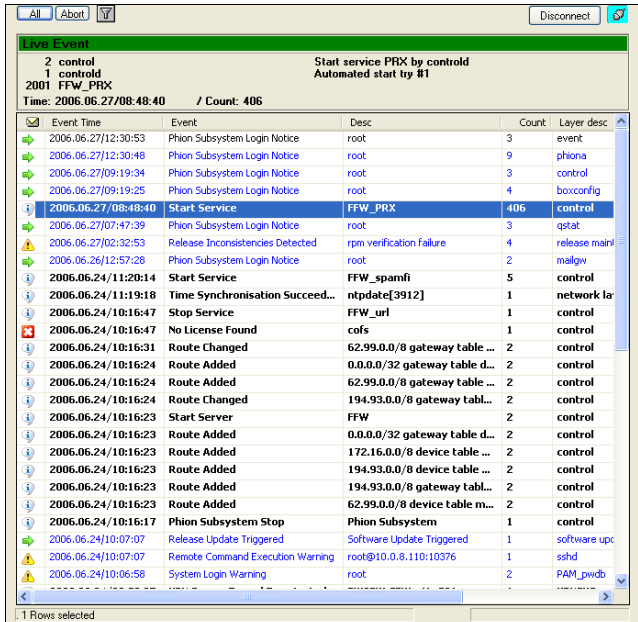
The live mode displays all newly created events, contrary to normal mode that does not display new events.

In live mode alarm messages like pop-up windows and sound (if it is configured) are also enabled.

To enable live mode click the **Live** button. This will change the top label "Current Event" to "Live Event" with green background.

A status bar in the lower right corner will also indicate this status. When an event occurs in the live mode, the background will blink green and red for a few seconds. The newly occurred event is indicated with a flag symbol (🚩).

Fig. 10-16 Event monitor in live mode



The Event Monitor in live mode displays a list of events with the following columns: Event Time, Event, Desc, Count, and Layer desc. The top of the window shows "Live Event" and "Start service PRX by control" with a green background. The status bar at the bottom indicates "1 Rows selected".

Event Time	Event	Desc	Count	Layer desc
2006.05.27/12:30:53	Phion Subsystem Login Notice	root	3	event
2006.06.27/12:30:48	Phion Subsystem Login Notice	root	9	phion
2006.06.27/09:19:34	Phion Subsystem Login Notice	root	3	control
2006.06.27/09:19:25	Phion Subsystem Login Notice	root	4	boxconfig
2006.06.27/08:48:40	Start Service	FFW_PRX	406	control
2006.06.27/07:47:39	Phion Subsystem Login Notice	root	3	qstat
2006.06.27/02:32:53	Release Inconsistencies Detected	rpm verification failure	4	release main
2006.06.26/12:57:28	Phion Subsystem Login Notice	root	2	malgw
2006.06.24/11:20:14	Start Service	FFW_spamfi	5	control
2006.06.24/11:19:18	Time Synchronisation Succeed...	ntpdate[3912]	1	network la
2006.06.24/10:16:47	Stop Service	FFW_url	1	control
2006.06.24/10:16:47	No License Found	cofs	1	control
2006.06.24/10:16:31	Route Changed	62.99.0.0/8 gateway table ...	2	control
2006.06.24/10:16:24	Route Added	0.0.0.0/32 gateway table d...	2	control
2006.06.24/10:16:24	Route Added	62.99.0.0/8 gateway table ...	2	control
2006.06.24/10:16:24	Route Changed	194.93.0.0/8 gateway tabl...	2	control
2006.06.24/10:16:23	Start Server	FFW	2	control
2006.06.24/10:16:23	Route Added	0.0.0.0/32 gateway table d...	2	control
2006.06.24/10:16:23	Route Added	172.16.0.0/8 device table ...	2	control
2006.06.24/10:16:23	Route Added	194.93.0.0/8 device table ...	2	control
2006.06.24/10:16:23	Route Added	194.93.0.0/8 gateway tabl...	2	control
2006.06.24/10:16:23	Route Added	62.99.0.0/8 device table m...	2	control
2006.06.24/10:16:17	Phion Subsystem Stop	Phion Subsystem	1	control
2006.06.24/10:07:07	Release Update Triggered	Software Update Triggered	1	software upc
2006.06.24/10:07:07	Remote Command Execution Warning	root@10.0.8.110:10376	1	sshd
2006.06.24/10:06:58	System Login Warning	root	2	PAM_pwdb



# DNS

<b>1.</b>	<b>Overview</b>	
1.1	Literature .....	316
<b>2.</b>	<b>Installation</b>	
2.1	Create Service .....	316
<b>3.</b>	<b>Configuration</b>	
3.1	Service Properties .....	317
3.2	DNS Server Configuration .....	317
3.3	Zone Independent DNS Server Settings .....	317
3.4	Zone Configuration .....	318
3.4.1	Predefined Zones .....	318
3.4.2	Add a New Zone .....	318
3.4.3	Edit/Add a New Start of Authority .....	319
3.4.4	Edit/Add a New Name Server .....	320
3.4.5	Add a New Host .....	320
3.4.6	Add a New Mail-Exchanger .....	321
3.4.7	Add a New Domain .....	321
3.4.8	Add New Others .....	322
3.4.9	Reverse Lookup Zones .....	322

# 1. Overview

This chapter describes how to install and configure a phion DNS server.

## 1.1 Literature






The following reading is recommendable to get familiar with DNS and BIND:

- **DNS and BIND**, 4th Edition  
written by Paul Albitz and Cricket Liu, published by O'Reilly & Associates  
ISBN 1-56592-512-2
- **SuSE Linux 7.3 Netzwerk**, 2. Auflage 2001  
published by SuSE GmbH (included in SuSE Linux 7.3 Professional Package)
- **DNS-HOWTO**  
[en.tldp.org/HOWTO/DNS-HOWTO.html](http://en.tldp.org/HOWTO/DNS-HOWTO.html)

# 2. Installation

A box server already has to exist, before a DNS service can be created.

## 2.1 Create Service

To create a DNS service, select **Create Service** from the context menu of  **Config** >  **Box** >  **Virtual Servers** >  **<servername>** >  **Assigned Services** and assign **DNS** as software module.

Click the **Activate** button to activate the changes. The newly installed DNS service is now ready for configuration.

**Attention:**

DNS service installation collides with a running Forwarding/Caching DNS (bdns) (**see Run Forwarding / Caching DNS, page 55**). The DNS service must run exclusively. Do NOT install both services.

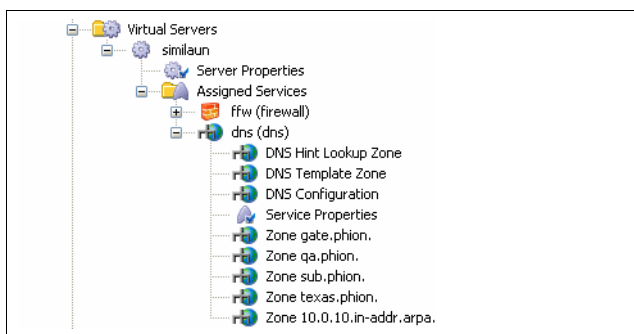
### 3. Configuration

#### 3.1 Service Properties

To access the service configuration area, double-click **Service Properties**. For service configuration details, refer to **Configuration Service - 4. Introducing a New Service**, page 97.

#### 3.2 DNS Server Configuration

Fig. 11-1 File structure of the DNS service



The following configuration nodes are available in the DNS service:

- **Hint Zone**  
The Hint Zone contains information on the initial set of root servers (see 3.4.1 Predefined Zones, page 318).
- **Template Zone**  
The Template Zone may be used to build templates for creation of new zones (see 3.4.1 Predefined Zones, page 318 for detail information).
- **DNS Config**  
Double-clicking **DNS Configuration** directs to the **Forward Lookup** configuration area. Sub items of Forward Lookup are the already existing zones, including the Hint Zone and the Template Zone.  
To create a new zone, right-click **Forward Lookup** and select **Add New Zone ...**. The newly created zone will initially inherit all settings made in the Template Zone. The inherited settings can freely be modified and supplemented with further settings. For a more detailed description of possible configuration options see 3.4.2 Add a New Zone, page 318.

**Note:**  
The DNS configuration area can be accessed by double-clicking any of these configuration nodes. The triggered node determines the initial view in the **DNS Configuration** area. Note that the sub-items **'** and **'\_template'** are identical in all cases, though.

**Note:**  
Before starting major configurations it is best to lock the complete branch of the configuration tree below **Assigned Services** > **<servicename> (dns)**.

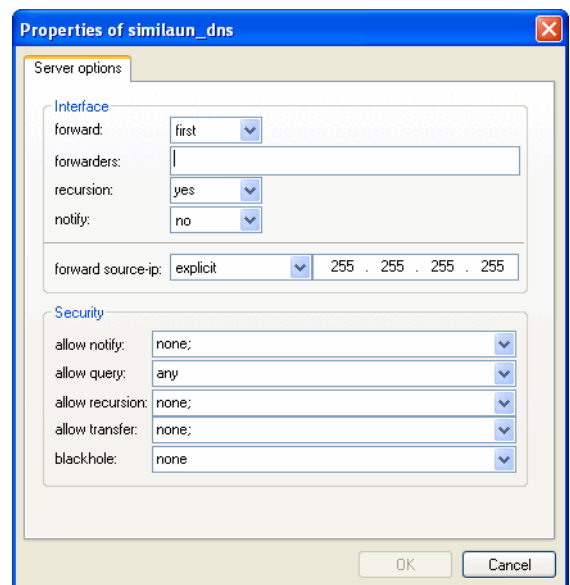
#### 3.3 Zone Independent DNS Server Settings

Fig. 11-2 DNS configuration area

Name	Type	Data
.	Master	
._template	Master	
gate.phion.	Master	
qa.phion.	Master	
sub.phion.	Master	
texas.phion.	Master	

To configure zone independent DNS server settings, double-click **DNS Configuration**, then right-click the server name in the DNS Configuration area (DNSSrv in the example). After that select **Properties ...** from the context menu (figure 11-2).

Fig. 11-3 DNS server properties



List 11-1 DNS Server - Properties configuration - section Interface

Parameter	Description
	The interface section lets you configure the forwarding behaviour of the DNS service.
<b>forward</b>	This menu offers the following settings: <b>&lt;blank&gt;</b> - The default settings of BIND are used. <b>first</b> - The server forwards the DNS query first. Only in case no entry is found the local database is queried. <b>only</b> - The server forwards all DNS queries.
<b>forwarders</b>	Enter the DNS servers here to which DNS queries are forwarded. Separate multiple entries with a semicolon and space (like 10.0.0.53; 10.0.0.67).
<b>recursion</b>	Define the allowance of recursive queries. The following options are available: <b>yes</b> - The server allows recursive queries. <b>no</b> - The server does not allow recursive queries. <b>&lt;blank&gt;</b> - The default settings of BIND are used.
<b>notify</b>	Define whether the DNS server should actively notify its slaves about settings' updates.

List 11-1 DNS Server - Properties configuration - section Interface

Parameter	Description
<b>forward source-ip</b>	This field offers various selections which IP address the DNS server should use for contacting other DNS servers. <b>server-first</b> - The DNS service uses the first server IP for connecting. <b>server-second</b> - The DNS service uses the second server IP for connecting. <b>explicit</b> - The DNS service uses an explicit IP address for connecting. This IP address must be configured as a server IP. <b>&lt;blank&gt;</b> - The default settings of BIND are used.

List 11-2 DNS Server - Properties configuration - section Security

Parameter	Description
	The security section holds security options for the DNS service. In each pull-down field one of the following values can be filled in: <b>none</b> <b>any</b> (one or more IP addresses) These entries can optionally be complemented with further IP addresses. <b>Note:</b> Separate multiple entries of IP addresses or address ranges (phion notation has to be used ( <b>Getting Started</b> - 5. phion Notation, page 25)) with a semicolon and space (like 10.0.0.53; 10.0.0.67; 192.168.0.10; 10.17.0.0/16).
<b>allow notify</b>	Lists the hosts that are allowed to notify the DNS server about zone changes.
<b>allow query</b>	Lists the hosts that are allowed to query the DNS server. By default all hosts are allowed to query the DNS server.
<b>allow recursion</b>	Specifies which hosts are allowed to make recursive queries on this server.
<b>allow transfer</b>	Lists the hosts that are allowed to fetch the DNS database from the DNS server.
<b>blackhole</b>	Specifies a list of addresses that the server will not accept queries from or use to resolve a query.

## 3.4 Zone Configuration

### 3.4.1 Predefined Zones

As described before the phion.a DNS GUI contains two predefined zones:

#### 🔗 **\_template**

This zone contains the general template, which is used as model for all newly created zones. The procedure for creating and modifying template settings is identical to the procedure for creating and editing settings in another zone. Note that only template settings which have already existed before creating the zone will be inherited. Double-click on the entry (**\_template**) to create or modify settings for SOA, Primary Server, Nameserver, ... Right-click into the main window to create new hosts, mail-exchangers, ... Every setting made here will be clearly arranged in a separate row within the main window and can be selected for further modification or deletion.

#### 🔗 **'.'**

The initial set of root-servers is defined using a **hint zone**. When the server starts up it uses the hint zone file to find a root name server and get the most recent list of root name servers. The 'zone "."' is short for this

root zone and means any zone for which there is no locally defined zone (slave or master) or cached answer.

#### **Attention:**

Do NOT modify the root server settings unless you exactly know what you are doing.

### 3.4.2 Add a New Zone

To introduce a new zone right-click on your DNS server and select **Lock Server** from the context menu. Optionally you may lock the DNS Server in the Config Tree already. The configuration may now be modified.

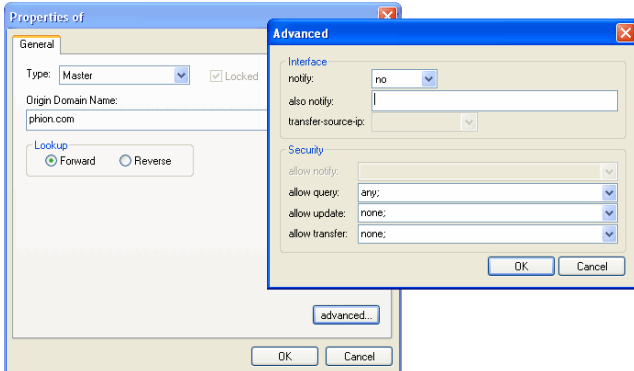
Select **Add New Zone** from the context menu and configure the following options:

List 11-3 DNS Server - Zone configuration - section General

Parameter	Description
<b>Type</b>	Set the needed zone type here
<b>Master</b>	Every domain configuration change takes place on the master. From here the information is propagated to the secondary servers. A master zone requires at least a Start of Authority (SOA) record and a Name Server (NS) record. Be sure to examine the security settings of the master zone, since a corrupt master zone can cause a lot of problems.
<b>Slave</b>	A slave zone is a replica of a master zone. The masters list specifies one or more IP addresses that the slave contacts to update its copy of the zone. DNS slave zones do not require much configuration; just enter the IP addresses of the master server (or servers) and examine the security settings. Be sure to set a transfer-source-IP, otherwise the slave zone will not be accepted by the DNS server.
<b>Forward</b>	A forward zone is used to direct all queries in it to other servers. The specification of options in such a zone will override any global options declared in the options statement. A forward zone does not need a transfer-source-IP. Be sure to check the security settings.
<b>Hint</b>	The initial set of root name servers is specified using a hint zone. When the server starts up, it uses the root hints to find a root name server and get the most recent list of root name servers. The netfence DNS server already has pre-configured a hint zone (Zone "."), so normally there is no need to introduce another hint zone.
<b>Note:</b>	Depending on the selected types the necessary settings may be slightly different. Such settings are marked with <b>(optional)</b> in the following.
<b>Origin Domain Name</b>	Enter the domain name you wish to create here (for example, phion.com).
<b>Lookup</b>	This section is used for defining whether the zone should <b>Forward</b> or <b>Reverse</b> lookup. DNS forward lookup provides IP addresses for known host names, while reverse lookup provides host names for known IP addresses. The netfence DNS server is able to provide DNS reverse lookup only for 8-bit networks (like 213.47.10.0/8).
<b>Masters (optional)</b>	This field is available when type <b>Slave</b> is selected. Enter the master IP addresses here.
<b>Forwards (optional)</b>	This field is available when type <b>Forward</b> is selected. Enter the forward IP addresses here.

By clicking the **advanced ...** button a new window appears containing additional settings:

**Fig. 11-4** DNS properties with open advanced window



**Note:**  
Refer to the BIND documentation for detailed information about the **advanced** options.

**List 11-4** DNS Server - Zone configuration - Advanced Settings - section Interface

Parameter	Description
<b>notify</b>	Allows the administrator to select whether the DNS server should notify slave DNS servers about zone changes. Possible values for selection are <b>yes/no/explicit</b> . If <b>explicit</b> is selected enter the explicit IP in the <b>also notify</b> field below.
<b>also notify</b>	Here you may enter a list of hosts that should be notified about zone changes although these machines are not registered slaves of the DNS server. <b>Note:</b> Separate multiple entries with a semicolon and space (like 10.0.0.53; 10.0.0.67; 192.168.0.10).
<b>transfer-source-ip</b>	This field is only available for type <b>Slave</b> . It defines the IP address the slave has to use when contacting its master DNS server. The following options are available: <b>service-default</b> <b>server-first</b> <b>server-second</b> <b>explicit</b> <b>Note:</b> Slave zones must have <b>transfer-source-ip</b> to work.

**List 11-5** DNS Server - Zone configuration - Advanced Settings - section Security

Parameter	Description
	offers detailed security options for the DNS service. Each pull-down field can take one of the following values: ➤ <b>none</b> ➤ <b>any</b>
<b>allow notify</b>	This field is only available for type <b>Slave</b> . It defines if the <b>Slave</b> accepts notifications about updates from its master.
<b>allow query</b>	Lists the hosts that are allowed to query the DNS server. By default all hosts are allowed to query the DNS server.
<b>allow update</b>	Lists the hosts that are allowed to update the database of the DNS server.
<b>allow transfer</b>	Lists the hosts that are allowed to fetch the DNS database from the DNS server.

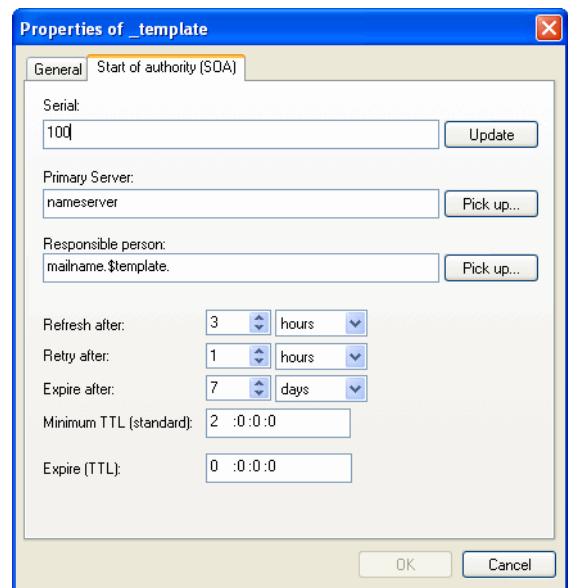
### 3.4.3 Edit/Add a New Start of Authority

At creation time of the phion DNS Server a standard template is created which is automatically inherited by newly generated zones. This standard template may freely be deleted or modified. In case you have deleted it, and have thereafter created a new zone, proceed as follows to comprehend the following instructions:

Select the newly created domain lacking a **Start of Authority (SOA)** record in the tree view, right-click into the main window and choose **Add a New Start of Authority (SOA) ...** from the context menu.

If the SOA record already exists, double-click on one of the existing entries with type **NS** or **SOA** and select the properties tab **Start of Authority (SOA)**.

**Fig. 11-5** Configuring a new SOA



**List 11-6** DNS Server - SOA configuration

Parameter	Description
<b>Serial</b>	Enter a serial number here. <b>Note:</b> Clicking <b>Update</b> will increase the serial number by one. The serial number of the master has to be higher than the serial number saved on the slave, otherwise the slave will stop fetching information updates from its master.
<b>Primary Sever</b>	Select the primary name server of the domain here. <b>Note:</b> By clicking <b>Pickup</b> already created entries can be selected.
<b>Responsible person</b>	Use this field to define a person responsible for this host/zone. The syntax that has to be used is <code>username.domain</code> (for example <code>ernestexample.test.org</code> ) <b>Note:</b> By clicking <b>Pickup</b> already created entries can be selected.
<b>Refresh after</b>	This interval tells the slave how often it has to check whether its data is up to date.
<b>Retry after</b>	When the slave fails to reach the master server after the refresh period ( <b>Refresh after</b> ), then it starts trying again after this set time interval.
<b>Expire after</b>	When the slave fails to contact the master server for the expire period, the slave expires its data. Expiring means that the slave stops giving out answers about the data because the data is too old to be useful.
<b>Minimum TTL (standard)</b>	This value sets the <b>Time To Live</b> of cached database entries of this zone. <b>Note:</b> The format for TTL is days:hours:minutes:seconds.

List 11-6 DNS Server - SOA configuration

Parameter	Description
<b>Expire (TTL)</b>	This value sets the <b>Time To Live</b> of cached database entries of this zone until it is considered as expired. <b>Note:</b> The format for TTL is days:hours:minutes:seconds.

### 3.4.4 Edit/Add a New Name Server

To introduce a new NS (**N**ame **S**erver), press the right mouse button in the right part of the window and select **New Name Server (NS) ...** from the context menu.

If a nameserver has already been created open an already existing entry with type **SOA** or **NS** and choose the tab **Nameserver (NS)**.

**Note:**

A new nameserver can only be entered if the SOA has already been generated.

Fig. 11-6 Configuring a new name server

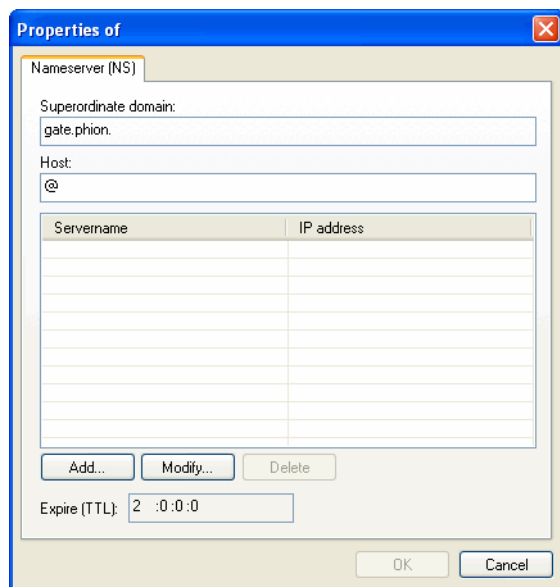
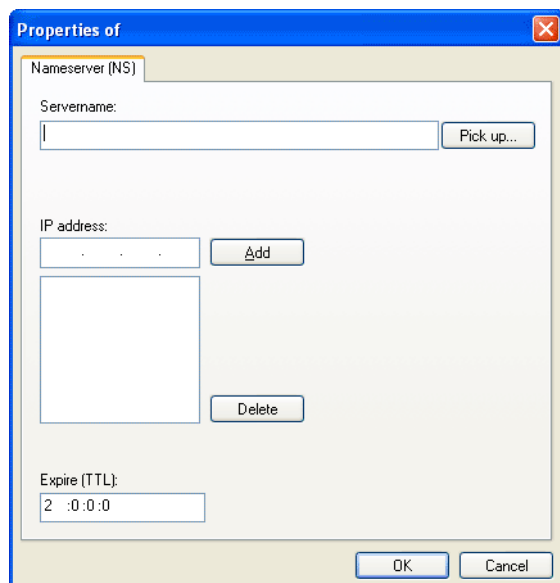


Fig. 11-7 Adding a nameserver



List 11-7 DNS Server - Name Server configuration

Parameter	Description
<b>Superordinate domain</b>	This is a read-only field. It displays the name of the domain the nameserver will be responsible for.
<b>Add .../Modify .../Delete</b> buttons	Clicking the button <b>Add ...</b> , opens a new window allowing you to add name servers.
<b>Servername</b>	This is the name of the name server.
<b>IP Address</b>	This is the IP address of the name server.
<b>Expire (TTL)</b>	This is the globally defined length of life, future name server records are expected to have. <b>Note:</b> The format for the Time to Live (TTL) is days:hours:minutes:seconds.

### 3.4.5 Add a New Host

To introduce a new host, press the right mouse button in the main window and select **New Host ...** from the context menu.

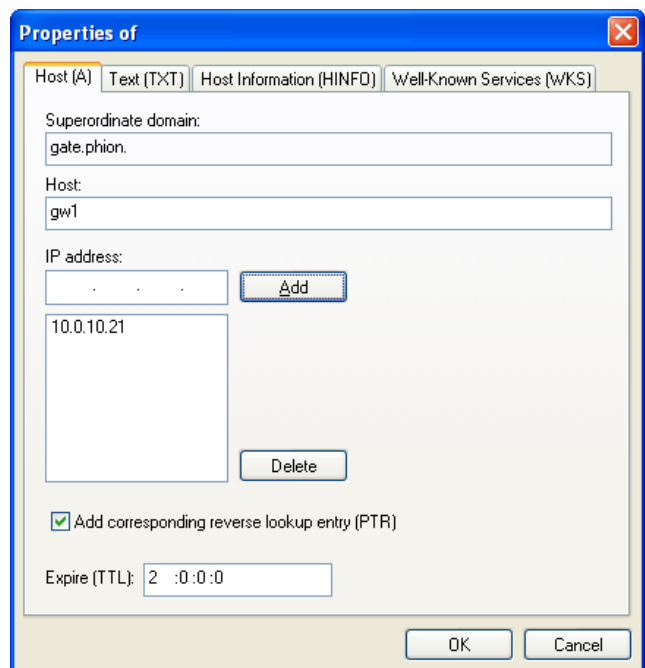
Entries made in the individual tabs will be saved in separate rows of type **A**, **TXT**, **HINFO** and **WKS** within the main configuration window.

Select the checkbox **Add corresponding reverse lookup entry (PTR)** to automatically create a pointer record when creating the A-Record.

**Note:**

In order to function, the reverse zone already has to exist (see 3.4.9 Reverse Lookup Zones, page 322).

Fig. 11-8 Configuring a New Host



List 11-8 DNS Server - Adding a New Host - Host (A) tab

Parameter	Description
<b>Superordinate domain</b>	This is a read-only field. It displays the name of the domain where the new host is created in. <b>Note:</b> This field is also displayed in all other tabs of this window.
<b>Host</b>	Enter the name of the host here. <b>Note:</b> In all other tabs of this window this field is also displayed but read-only.



**List 11-8** DNS Server - Adding a New Host - Host (A) tab

Parameter	Description
<b>IP address</b>	To enter a new host IP address click <b>Add</b> . To delete an existing address click <b>Delete</b> .
<b>Expire (TTL)</b>	The format for this field is days:hours:minutes:seconds.

**List 11-9** DNS Server - Adding a New Host - Host Information (HINFO) tab

Parameter	Description
	The fields of this tab ( <b>Hardware Type</b> and <b>Operating System</b> ) can be used to provide information on used hardware and operating system platform a host is running.

**List 11-10** DNS Server - Adding a New Host - Text (TXT) tab

Parameter	Description
<b>Text</b>	In this field any text can be entered, for example, for describing the system to simplify maintenance of the DNS database.
<b>Expire (TTL)</b>	The format for this field is days:hours:minutes:seconds.

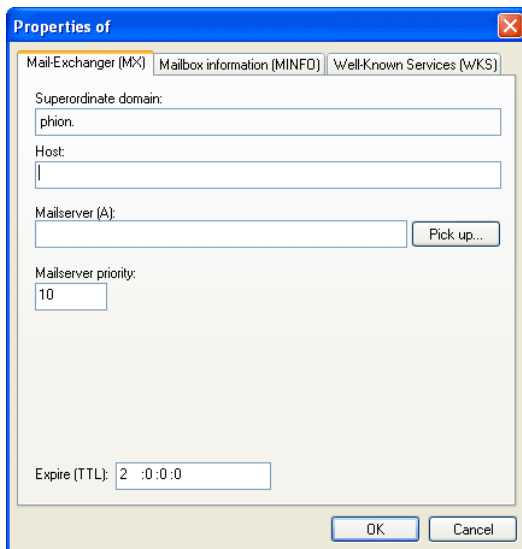
**List 11-11** DNS Server - Adding a New Host - Well-Known Services (WKS) tab

Parameter	Description
	Enter the IP address and the used protocol in the appropriate fields. The services need to be entered in plain text and separated with blanks (like telnet ssh smtp ftp).

### 3.4.6 Add a New Mail-Exchanger

To introduce a new mail exchanger, press the right mouse button in the main window and select **New Mail-Exchanger ...** from the context menu.

**Fig. 11-9** Configuring a new mail exchanger



**List 11-12** DNS Server - Adding a New Mail-Exchanger - Mail-Exchanger (MX) tab

Parameter	Description
<b>Superordinate domain</b>	This is a read-only field. It displays the name of the domain the mail-exchanger handles mail-traffic for. <b>Note:</b> This field is also displayed in all other tabs of this window.
<b>Host</b>	Depending on the needs the following values are entered here: @ - mail-exchanger is responsible for @domain.com any_text - mail-exchanger is responsible for @any_text.domain.com <b>Note:</b> In all other tabs of this window this field is also displayed but read-only.

**List 11-12** DNS Server - Adding a New Mail-Exchanger - Mail-Exchanger (MX) tab

Parameter	Description
<b>Mailserver (A)</b>	Here the name of the mailserver has to be entered. <b>Note:</b> By clicking <b>Pickup</b> already created entries can be selected.
<b>Mailserver priority</b>	Use this field to set the mailserver priority.
<b>Expire (TTL)</b>	The format for this field is days:hours:minutes:seconds.

**List 11-13** DNS Server - Adding a New Mail-Exchanger - Mailbox information (MINFO) tab

Parameter	Description
<b>Mailbox (MB)</b>	Here the name of the mailbox has to be entered. <b>Note:</b> By clicking <b>Pickup</b> already created entries can be selected.
<b>Error mailbox (MB)</b>	Here the name of the error mailbox has to be entered. <b>Note:</b> By clicking <b>Pickup</b> already created entries can be selected.
<b>Expire (TTL)</b>	The format for this field is days:hours:minutes:seconds.

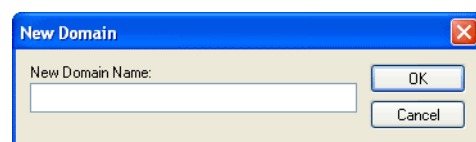
**List 11-14** DNS Server - Adding a New Mail-Exchanger - Well-Known Services (WKS) tab

Parameter	Description
	Enter the IP address and the used protocol in the appropriate fields. The services need to be entered in plain text and separated with blanks (for example telnet ssh smtp ftp).

### 3.4.7 Add a New Domain

To introduce a new sub-domain, click right in the main window and then select **New Domain** from the context menu.

**Fig. 11-10** Configuring a new sub-domain



Enter a name for the new sub-domain. After clicking **OK** the new sub-domain appears in the DNS tree. Within the new sub-domain you are able to perform the same operations as described above.

**Note:**

Completely set up new sub-domains before executing **Send Changes > Activate**. Unconfigured sub-domains will be deleted.

### 3.4.8 Add New Others

There are several other objects you can add to your DNS configuration.

**Note:**

Consult the BIND documentation to learn about the appropriate parameters and functions of these objects.

**Note:** These objects can be introduced by right-clicking in the right part of the DNS config window and selecting **New Others**.

The following objects can be added to the DNS configuration:

**Table 11-1** Supplementary DNS configuration objects overview

Object	Description
A	New host
AAAA	IPv6 address
AFSDB	AFSDB records specify the hosts that provide a style of distributed service advertised under this domain name. A subtype value (analogous to the <i>preference</i> value in the MX record) indicates which style of distributed service is provided with the given name. Subtype 1 indicates that the named host is an AFS® database server for the AFS cell of the given domain name. Subtype 2 indicates that the named host provides intra-cell name service for the DCE cell named by the given domain name.
CNAME	CNAME specifies an alias or nickname for the official or canonical name. An alias should be the only record associated with the alias; all other resource records should be associated with the canonical name and not with the alias. Any resource records that include a zone name as their value (for example, NS or MX) must list the canonical name, not the alias. This resource record is especially useful when changing machine names.
HINFO	HINFO records contain host-specific data. They list the hardware and operating system that are running on the listed host. If you want to include a space in the machine name, you must quote the name. Host information is not specific to any address class, so ANY may be used for the address class. There should be one HINFO record for each host. For security reasons, many sites do not include the HINFO record, and no applications depend on this record.
ISDN	Representation of ISDN addresses.
MB	MB lists the machine where a user wants to receive mail. The "name" field is the user's login; the machine field denotes the machine to which mail is to be delivered. Mail box names should be unique to the zone.
MG	The mail group record (MG) lists members of a mail group.
MINFO	MINFO creates a mail group for a mailing list. This resource record is usually associated with a mail group, but it can be used with a mailbox record. The "name" specifies the name of the mailbox. The "requests" field is where mail such, as requests to be added to a mail group, should be sent. The "maintainer" is a mailbox that should receive error messages. This is particularly appropriate for mailing lists when errors in members' names should be reported to a person different to the sender.
MR	MR records lists aliases for a user. The "name" field lists the alias for the name listed in the fourth field, which should have a corresponding MB record.
MX	MX records specify a list of hosts that are configured to receive mail sent to this domain name. Every host that receives mail should have an MX record, since if one is not found at the time the mail is delivered, an MX value will be imputed with a cost of 0 and a destination of the host itself.
NS	NS lists a name server responsible for a given zone. The first "name" field lists the zone that is serviced by the listed name server. There should be one NS record for each name server of the zone, and every zone should have at least two name servers, preferably on separate networks.
PTR	PTR allows special names to point to some other location in the domain. The following example of a PTR record is used in setting up reverse pointers for the special in addr.arpa domain. This line is from the example mynet.rev file. In this record, the "name" field is the network number of the host in reverse order. You only need to specify enough octets to make the name unique.

**Table 11-1** Supplementary DNS configuration objects overview

Object	Description
RP	RP identifies the name (or group name) of the responsible person(s) for a host. This information is useful in troubleshooting problems over the network.
RT	Route-through binding for hosts that do not have their own direct wide area network addresses (experimental).
SVR	Information on well known network services (replaces WKS).
TXT	A TXT record contains free-form textual data. The syntax of the text depends on the domain in which it appears; several systems use TXT records to encode user databases and other administrative data.
WKS	WKS records describe the well-known services supported by a particular protocol at a specified address. The list of services and port numbers comes from the list of services specified in /etc/services. There should be only one WKS record per protocol and address. Because the WKS record is not widely used throughout the Internet, applications should not rely on the existence of this record to recognize the presence or absence of a service. Instead, the application should simply attempt to use the service.
X25	Representation of X.25 network addresses (experimental)

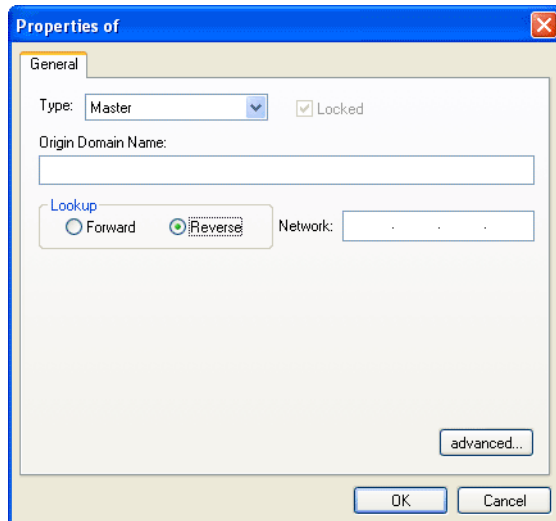
### 3.4.9 Reverse Lookup Zones

Each of the four available zones can be defined as reverse lookup zone.

To do so, switch the lookup box from **forward** to **reverse** when creating a new zone.

The input mask will change and you will be able to enter the address of the network you wish to create a reverse lookup zone for.

**Fig. 11-11** Create reverse lookup zone



An appropriate name for the reverse lookup zone will automatically be created from the network address. In our example, the network address is 10.0.0.0 which results in an automatically created reverse lookup zone named 0.0.10.in-addr.arpa.

By clicking the **advanced ...** button the advanced option window will pop up allowing you to define the same options as described in 3.4.2 Add a New Zone, page 318.

# Proxy

<b>1.</b>	<b>HTTP Proxy</b>	
1.1	Installation .....	324
1.2	Configuration .....	324
1.2.1	General .....	325
1.2.2	Network .....	325
1.2.3	Access Control .....	327
1.2.4	Content Inspection .....	335
1.2.5	Advanced .....	335
1.3	Transparent Proxy .....	335
1.4	Reverse Proxy .....	336
1.4.1	Example Setup .....	336
<b>2.</b>	<b>Secure Web Proxy</b>	
2.1	Overview .....	337
2.2	Technical Details .....	337
2.3	Installation .....	337
2.4	Configuration .....	338
2.4.1	Secure-Web-Proxy Settings .....	338
2.5	Operation .....	339
2.5.1	Access Tab .....	339
2.5.2	Tickets Tab .....	340
2.5.3	Certificates Tab .....	340
2.5.4	RSS-Feeds Tab .....	341
2.5.5	Webservices Tab .....	341
<b>3.</b>	<b>ISS Proventia Web Filter</b>	
3.1	General .....	342
3.2	Installation .....	344
3.3	Configuration .....	344
3.3.1	Configuring Proventia Web Filter Redirectors .....	344
3.3.2	Configuration of the Proventia Web Filter Daemon .....	344
3.3.3	Configuring of IIS Proventia Web Filter - Redirector Parameters .....	345
3.3.4	Adapting the Local Firewall Rule Set .....	347
3.4	Communication & Categories .....	347
3.4.1	Communication with External HTTP Server .....	347
3.4.2	Proventia URL Categories .....	348
3.5	Logging .....	348
3.6	Load Sharing and High Availability .....	349

# 1. HTTP Proxy

## 1.1 Installation

### Note:

The proxy service integrated into netfence gateway is based on the **Squid Web Proxy Cache**. The labelling of configuration parameters thus follows the labelling applying in the initial product. If you are not familiar with terms used for Squid proxy configuration, refer to the official Squid documentation available at [www.squid-cache.org](http://www.squid-cache.org).

### Note:

**DNS Server IP** and **Box DNS Domain** must be specified in the **Box Settings** file before creating the proxy service (**Configuration Service** - 2.2.3.3 DNS, page 55). The proxy service will otherwise fail to start.

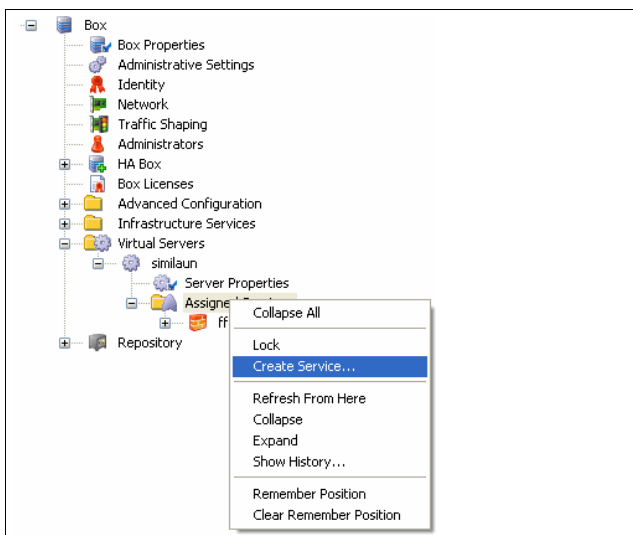
A box server has already to exist before an HTTP Proxy service can be created.

### Note:

When two proxy instances are configured on one box (for example a **HTTP Proxy** and a **Secure Web Proxy**), they have to be configured to use two different ports, even if they use separate bind-IPs.

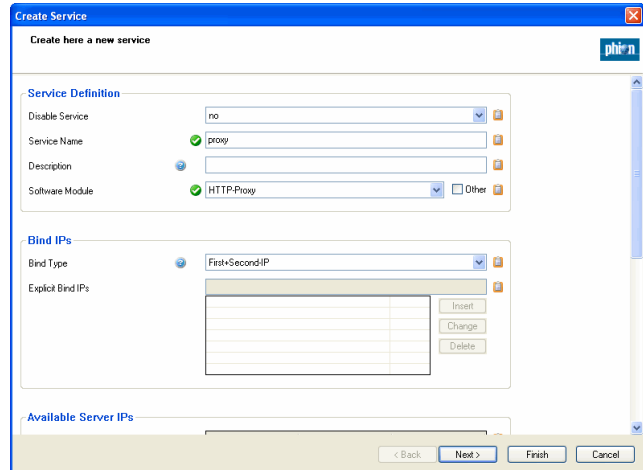
To create an HTTP Proxy service, select **Create Service** from the context menu of **Config > Box > Virtual Servers > <servername> > Assigned Services**.

Fig. 12-1 Creating the HTTP Proxy service



Insert a name for the proxy service and assign **HTTP-Proxy** as software module.

Fig. 12-2 Creating the HTTP Proxy service



Click the **Activate** button to activate the changes. The newly installed HTTP Proxy service is now ready for configuration.

For service configuration details, refer to **Configuration Service** - 4. Introducing a New Service, page 97.

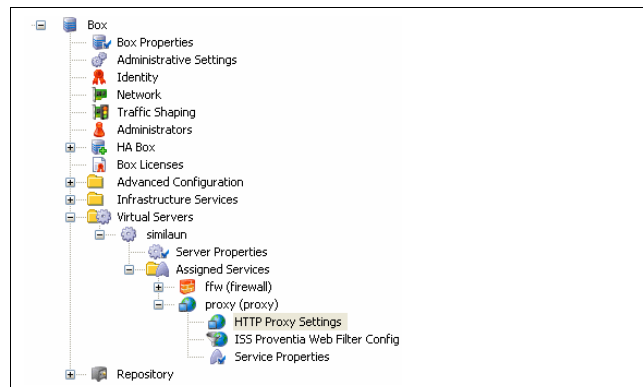
### Note:

Regarding the proxy service, customised statistics settings are not configurable. By default, the service will always generate all available statistics types.

## 1.2 Configuration

To configure specific proxy service settings double-click **HTTP Proxy Settings**.

Fig. 12-3 HTTP Proxy Config node in the Configuration Tree



### 1.2.1 General

List 12-1 HTTP Proxy Service Parameters - General - section Basic Settings

Parameter	Description
<b>Contact Mail</b>	Mail address of administrative contact used for designation of user and error messages.
<b>Visible Hostname</b>	Host name displayed in error messages generated by the proxy service. Defining a host name is mandatory. <b>Note:</b> Do not use special characters in the visible hostname. <b>Attention:</b> If you are running a Forwarding/Caching DNS server (parameter see Run Forwarding / Caching DNS, page 55) the Visible Hostname MUST NOT be identical to the Box Hostname (parameter see Hostname, page 62).
<b>Language of Error Pages</b>	This parameter defines the language for <i>Access Denied</i> error messages. <b>German</b> and <b>English</b> are available for choice.
<b>Disable FTP</b>	If set to <b>yes</b> (as it is by default) the proxy server denies FTP request. Set to <b>no</b> to enable FTP traffic

List 12-2 HTTP Proxy Service Parameters - General - section Log Settings

Parameter	Description
<b>Write Store-Log</b>	The store log file records information about storage and deletion of cached objects. This information is essentially important for troubleshooting.
<b>Write Cache-Log</b>	The cache log file records debug and failure messages generated by squid during operating time. Amongst others, it includes information about service start and termination, and execution of ACLs.
<b>Debug Level</b>	The debug level defines the verbosity of the cache log file (default: normal). <ul style="list-style-type: none"> <li>➤ <b>normal</b> - Setting to normal results in minimal logging. Errors will not be listed exhaustively; statistical information will not be generated.</li> <li>➤ <b>verbose</b> - Setting verbose generates statistical information and logs most errors.</li> <li>➤ <b>debug</b> - Setting to debug results in exhaustive logging of errors and statistical information.</li> </ul> <b>Attention:</b> Use option debug with care, as full logging claims high disk capacity.
<b>Log via Syslog</b>	This parameter determines handling of log files that are generated by the HTTP Proxy service. Setting to <b>no</b> triggers local log file generation. Setting to <b>yes</b> forwards logging data to the local Syslog-Proxy ( <b>Configuration Service</b> - 5.2.3 Syslog Streaming, page 115) where further data processing can be defined. Setting to <b>Auto</b> (default) queries the Syslog-Proxy configuration prior to log data processing. If a streaming profile for HTTP-Proxy log files is defined, it will be used. <b>Note:</b> Set to <b>no</b> if you encounter performance issues in conjunction with remote logging of busy servers.

List 12-3 HTTP Proxy Service Parameters - General - section Misc. Settings

Parameter	Description
	This part of the configuration offers manual control of size and structure of the cache directories. Click <b>Set</b> to open the cache config.
<b>Size in MB</b>	Specifies the maximum size of the cache directory in MB. The cache is located in <code>/var/phion/squid-cache_SERVERNAME_SERVICE_NAME</code> . Using at least 100 MB is recommended.
<b>Level1 Directories / Level2 Directories</b>	These settings define the structural organisation of the proxy service's cache directory. The default values (16 / 256) are the recommended minimum values for Level1 and Level2 directories respectively. Define settings with deliberation, since high values result in a vast number of subdirectories.

### 1.2.2 Network

Fig. 12-4 HTTP Proxy Service Parameters - Network

List 12-4 HTTP Proxy Service Parameters - Network - section Network Settings

Parameter	Description
<b>TCP Outgoing Address</b>	The proxy server uses this IP address when executing HTTP requests. Available for selection are: <b>First-IP</b> , <b>Second-IP</b> , <b>Dynamic</b> , <b>Other</b> (which means an explicit IP address). With setting <b>Dynamic</b> a suitable address for request execution is chosen automatically from the available server address pool. <b>Note:</b> Explicitly defined IP addresses must be available in the <b>Additional IP</b> list in the Server Configuration file (see 3. Configuring a New Server, page 94).
<b>TCP Listening Port</b>	The TCP Listening Port defines the port the proxy service is listening on for incoming TCP connections. (TCP Incoming is set as <b>Bind Type</b> in the service configuration window; see <b>Configuration Service</b> - List 3-88 Service Configuration - General - section Service Definition, page 97). <b>Note:</b> The TCP Listening Port configured here is directly related to the <b>Service Object "PROXY"</b> which is configured in the <b>Services</b> tab of the Local Firewall. If you change the value of the TCP Listening Port to another value than the default 3128, remember to change the value of the Service Object "PROXY" as well because this one is used in the default http-proxy Local Firewall rule set. If port settings are not adapted in the Service Object, all HTTP traffic is blocked.
<b>UDP Incoming Address</b>	The proxy server uses this IP address when responding to ICP queries. Available for selection are: <b>First-IP</b> , <b>Second-IP</b> , <b>None</b> , <b>Other</b> (which is an explicit IP address). <b>Note:</b> Explicitly defined IP addresses must be available in the <b>Additional IP</b> list in the Server Configuration file (see 3. Configuring a New Server, page 94).
<b>UDP Outgoing Address</b>	The proxy server uses this IP address when executing ICP and DNS queries. Available for selection are: <b>First-IP</b> , <b>Second-IP</b> , <b>Other</b> (which is an explicit IP address). <b>Note:</b> Explicitly defined IP addresses must be available in the <b>Additional IP</b> list in the Server Configuration file (see 3. Configuring a New Server, page 94). <b>Note:</b> Insert <code>255.255.255.255</code> into this field when accessing the Internet through a dynamically assigned IP address (like using an xDSL line).
<b>ICP Port</b>	This is the port through which the proxy service handles ICP (Internet Cache Protocol) connections with its neighbour caches (default: <b>3130</b> ). If not needed set to <b>0</b> to disable.
<b>Neighbour Settings</b>	see Section Neighbour Settings
<b>SNMP Settings</b>	see SNMP Settings, page 326



## Section *Neighbour Settings*

Use this section to configure this proxy server's behaviour towards neighbouring proxies. Adjacent proxies can rank before or be coequal with the proxy, which means they can either be treated as parents or siblings. Click **Insert ...** to create a new neighbouring proxy and specify a **Name** for it.

### Attention:

The name specified in this place is used as expression in the proxy server's ACL list. The same applies to the **Name** field specified for a new record in the ACL Entries section (see 1.2.3.4 Access Control - Section ACL Entries, page 329). To avoid conflicts, make sure these two names never match.

The following parameters are available for configuration.

List 12-5 HTTP Proxy Service Parameters - General - Neighbour Settings

Parameter	Description
<b>IP/Hostname</b>	This field contains either IP address or hostname of the neighbouring proxy server.
<b>Neighbour Type</b>	This field defines the relationship to the neighbouring proxy server. Possible values are <b>parent</b> or <b>sibling</b> . <b>Attention:</b> In a sibling relationship, a peer may only request objects already held in the cache. A sibling cannot forward cache misses on behalf of the peer.
<b>Exclusive Parent</b>	This parameter is only activated with <b>Neighbour Type</b> set to <b>parent</b> . When set to <b>yes</b> all requests are forwarded to the Exclusive Parent. This setting is recommended if the parent proxy is a virus scanning proxy server.
<b>Proxy Port</b>	Specifies the port, on which the neighbour server listens for incoming HTTP requests (default: 3128).
<b>ICP Port</b>	Specifies the port, on which the neighbour server listens for incoming ICP connections (default: 3130). To configure a neighbour cache not using ICP, enable the UDP echo port on it and specify 7 as ICP port value. For neighbours, which do not support ICP queries, specify 0 as ICP port value and define <b>no-query</b> in the <b>Options</b> parameter (Section <b>Options Settings</b> ) below.
<b>Cache Priority</b>	Setting a value for the Cache Priority is mandatory. Lower numbers mean higher priority. The neighbour cache with the highest priority number will be considered first. The priority may be set to any value, if only one neighbour cache exists. It will then be ignored. <b>Attention:</b> The Cache Priority may not be set to value 0. <b>Note:</b> An example for cache priority weighing is described in 1.2.3.11 Cache Behaviour Configuration Example.

List 12-6 HTTP Proxy Service Parameters - General - Neighbour Settings - section Option Settings

Parameter	Description
<b>Authentication</b>	This parameter specifies the authentication mechanism from the proxy to its neighbour. Possible values are <b>NONE (default)</b> , <b>noPASS</b> and <b>PASS</b> . <ul style="list-style-type: none"> <li>➤ Use <b>PASS</b> (=log in) if authenticating against an upstream proxy (parent). To combine this with proxy_auth both proxies have to share the same user database as HTTP only allows for one proxy login. <b>USE WITH CAUTION</b>, as this will expose your user's proxy password to the parent.</li> <li>➤ Use <b>noPASS</b> with a personal or workgroup proxy when the parent requires proxy authentication. In this case <b>User</b> and <b>Password</b> are set in the fields below.</li> </ul>
<b>User/Password</b>	This is the login data needed with <b>Authentication Setting noPass</b> (see above).
<b>Options</b>	Additional options for the specified parent proxy can be inserted here. Amongst others, the following options can be used: <b>proxy-only</b> , <b>weight=n</b> , <b>ttl=n</b> , <b>no-query</b> , <b>default</b> , <b>round-robin</b> , <b>multicast-responder</b> , <b>closest-only</b> , <b>no-digest</b> , <b>no-netdb-exchange</b> , <b>no-delay</b> , <b>connect-timeout=nn</b> , <b>digest-url=url</b> , <b>allow-miss</b> . Please consult the squid documentation for further information.

List 12-7 HTTP Proxy Service Parameters - General - Neighbour Settings - section Cache Behaviour

Parameter	Description
	<b>Note:</b> Activities related to the caching parameters are logged to the files <server_servicename>\proxy_store and access. These files can be viewed in the phion.a LogGUI ( <b>DHCP</b> , page 271).
<b>URL Fetching</b>	This parameter takes complete URLs or a list of words, which if found in an URL cause the object to be handled directly by the proxy itself. Before communicating with any of the cache peers, squid first tries to fetch the requested URL directly from the server. If it cannot find it, it tries to establish a connection to the configured parent cache(s). <b>Note:</b> URLs entered without protocol specification are applied on both possible protocols, HTTP and FTP (like www.phion.com, *phion*). Please consider the following characteristic, when fetching FTP URLs with virus scanner and FTP scanning activated at the same time: If directly fetched FTP URLs ought to be virus scanned, specify their protocol as well (like ftp://www.phion.com, ftp://*phion*). The data stream will otherwise be forwarded without virus scanning. <b>Note:</b> It is recommended to include dynamic pages into this tag (like jsp, asp, php, ...). <b>Attention:</b> Though configured in context per neighbour cache, the value of the URL Fetching parameter is inherited by all neighbours in use. A specific domain, once configured for direct access in a single configuration section, will always be fetched directly, even if not inserted in other configuration sections.
<b>Cache Direct Objects</b>	This parameter is linked to parameter <b>URL Fetching</b> . Set to <b>yes</b> to enable caching of URLs with characteristics specified above. Set to <b>no</b> to disable caching.
<b>Domain Restrictions</b>	This parameter takes a list of explicit domains for which the neighbour caches shall be queried. The following syntax applies: .domainname.tld .subdomain.domainname.tld *.domainname.tld ... A domain name preceded by an exclamation mark means that all domains shall be requested from the cache except the specified one. !.domainname.com ... Cache hosts with no domain restrictions configured will be queried for all domains.
<b>Cache Domain Objects</b>	This parameter is linked to parameter <b>Domain Restrictions</b> . Set to <b>yes</b> to cache URLs fetched from the parent.
<b>Cache Peer Access</b>	This parameter takes a list of IP addresses/IP address ranges which shall be directed to a specific neighbour cache. If restrictions are not configured, the cache will be queried for all requests.
<b>Cache IP Objects</b>	Set to yes to cache requests originating from the IPs specified above.

## SNMP Settings

The integrated Squid proxy server can handle statistics and status information transmitted through the Simple Network Management Protocol (SNMP). This is especially useful for management of non SNMP manageable network nodes. The SNMP daemon (snmpd) supports protocol versions SNMPv1 and SNMPv2c. It accepts and responds to SNMP messages that have been sent to the SNMP port.

For a general overview of SNMP features please see **SNMP - 1. Overview**, page 480.

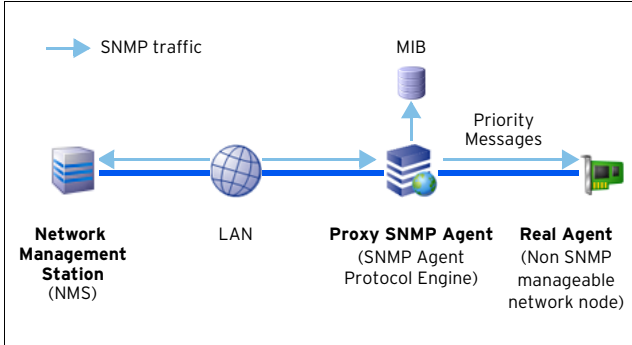
In a network management system, SNMP communication is processed over two components, the **Network Management Station (NMS)** and its managed agent. When the managed agent is not capable of SNMP, a **Proxy SNMP Agent** may take over the task of querying the **Management Information Base (MIB)** and forwarding the



retrieved information to agent and network management station as queried.

The following scheme depicts the proxy server's position in an environment communicating through SNMP.

Fig. 12-5 SNMP message handling



Click **Set** to configure the Proxy **SNMP** Agent settings. The following parameters are available for configuration:

List 12-8 HTTP Proxy Service Parameters - General - section SNMP

Parameter	Description
<b>Enable SNMP</b>	This option enables the Proxy SNMP Agent. If set to No, the proxy will not listen for SNMP traffic.
<b>SNMP Address</b>	This parameter defines the address the Proxy SNMP Agent listens on for SNMP traffic. The agent uses the defined SNMP address(es) to accept messages from SNMP agents and to return packets to them.
<b>SNMP Port</b>	Listening port for SNMP queries. <b>Attention:</b> Do not use the default SNMP port, if a SNMP service is configured on this server.
<b>IP/Mask</b>	<b>IP/Mask</b> Defines which hosts/networks are granted to query the SNMP service. Access to the SNMP port is allowed for all peers with the source network addresses configured here. Squid checks all snmp_access ACL operators when it is queried by a SNMP management station.
	<b>Community</b> Defines the community name (acts as a sort of password) to identify membership of a community.

## 1.2.3 Access Control

### 1.2.3.1 Section Authentication

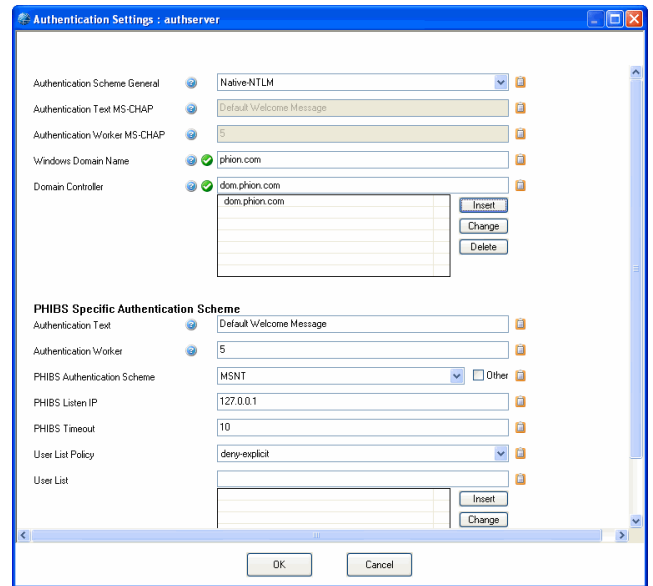
A user authentication scheme has to be configured if you want your users to authenticate themselves when using the proxy.

**Note:**

If an authentication scheme has been configured, all users will be asked to authenticate themselves by default. Defining ACLs in the **Access Control - Section ACL Entries** 1.2.3.4, page 329 revokes this default setting. From now on, ACLs making use of ACL Type **proxyauthentication** have to be defined explicitly (see User Authentication, page 330).

Click the **Set ...** button to open the **User Authentication** configuration window:

Fig. 12-6 Config Section Dialogue - Authentication Settings



**Note:**

The availability of the options depends on the set **Authentication Scheme**.

List 12-9 HTTP Proxy Service Parameters - Authentication Settings

Parameter	Description
<b>Authentication Scheme General</b>	Defines the authentication method applying: <ul style="list-style-type: none"> <li>Use <b>Native-NTLM</b> (default) for old windows domains or Windows 2003 Server domains in mixed-mode.</li> <li>Use <b>Remote-MS-CHAP-Phibs</b> for Windows 2003 Server domains in native mode.</li> <li>Use <b>PHIBS-Specific-Schemes</b> for non windows network environments.</li> </ul> <b>Note:</b> When using one of the first two methods, a fallback scheme has to be configured in the PHIBS Specific Authentication Scheme section to allow for authentication of non windows clients as well. <b>Attention:</b> When using a Windows 2003 server domain with scheme Native-NTLM take the following into consideration: Domain has to be in Mixed-Mode (NOT Native) AND registry key HKLM/SYSTEM/CurrentControlSet/Services/lanmanserver/parameters/requiresecuritysignature has to be set to 0
<b>Authentication Text MS-CHAP</b>	The following parameters are only available with <b>Remote-MS-CHAP-Phibs</b> selected as <b>Authentication Scheme</b> . This field contains the text that is displayed in the authentication window of the client. Enter a significant text to let the user know, which server requires authentication. Supplying an authentication text is mandatory.
<b>Authentication Worker MS-CHAP</b>	Number of workers started for authentication. The default value is <b>5</b> . <b>Note:</b> For proxy servers with great load this value may be set up to 48.
<b>Windows Domain Name</b>	The following parameters are only available with <b>Native-NTLM</b> selected as <b>Authentication Scheme</b> . This is the name of the domain the authentication server resides in.

List 12-9 HTTP Proxy Service Parameters - Authentication Settings

Parameter	Description
<b>Domain Controller</b>	This is the host name of the Windows domain controller providing authentication operation. Enter the host name without its domain suffix. The name has to be DNS resolvable. <b>Attention:</b> Do not enter IP addresses instead of host names. No restrictions apply to the number of domain controllers in use. Multiple domain controllers improve performance due to load balancing ability.
	<b>Note:</b> Since Native-NTLM uses small time-out values, it may be necessary to add the parameters <b>auth_param ntlm max_challenge_reuses</b> and <b>auth_param ntlm max_challenge_lifetime</b> within the <b>Generic squid.conf Entries</b> (Section <b>ADVANCED SQUID CONFIGURATION</b> , page 335) for fine tuning. <b>Attention:</b> Do not use Domain Controllers in conjunction with low speed connections, for example 10MBit network connections or VPN tunnels.

List 12-10 HTTP Proxy Service Parameters - Authentication Settings - section PHIBS Specific Authentication Scheme

Parameter	Description
	<b>Note:</b> This section has to be configured with either authentication method selected. It is either applied solely, otherwise the settings represent a fallback scheme, in case the other authentication methods are not applicable (see parameter <b>Authentication Scheme General</b> ).
<b>Authentication Text</b>	This field contains the text that is displayed in the authentication window of the client. Enter a significant text to let the user know, which server requires authentication.
<b>Authentication Worker</b>	Number of workers started for authentication. The default value is <b>5</b> . <b>Note:</b> For proxy servers with great load this value may be set up to 48.
<b>PHIBS Authentication Scheme</b>	A pull-down menu gives five different schemes to choose from: <b>MSNT, MSAD, RADIUS, LDAP, RSAACE</b> <b>Note:</b> The authentication schemes are activated and configured in the box configuration ( <b>Configuration Service</b> - 5.2.1 Authentication Service, page 111).
<b>PHIBS Listen IP</b>	Defines the IP address of the box where the PHIBS-authentication daemon is running on.
<b>PHIBS Timeout</b>	Specifies the response timeout for the authentication server.
<b>User List Policy</b>	The option <b>deny-explicit</b> means that all domain-users who are listed in the user list are not allowed to use the proxy service. The option <b>allow-explicit</b> means that only domain users that are listed in the user list are allowed to use the proxy service. This does not mean that they do not require authentication.
<b>User List</b>	List of usernames that are used for the <b>User List Policy</b> .

### 1.2.3.2 Section Access Control - Proxy Access Handling Scheme

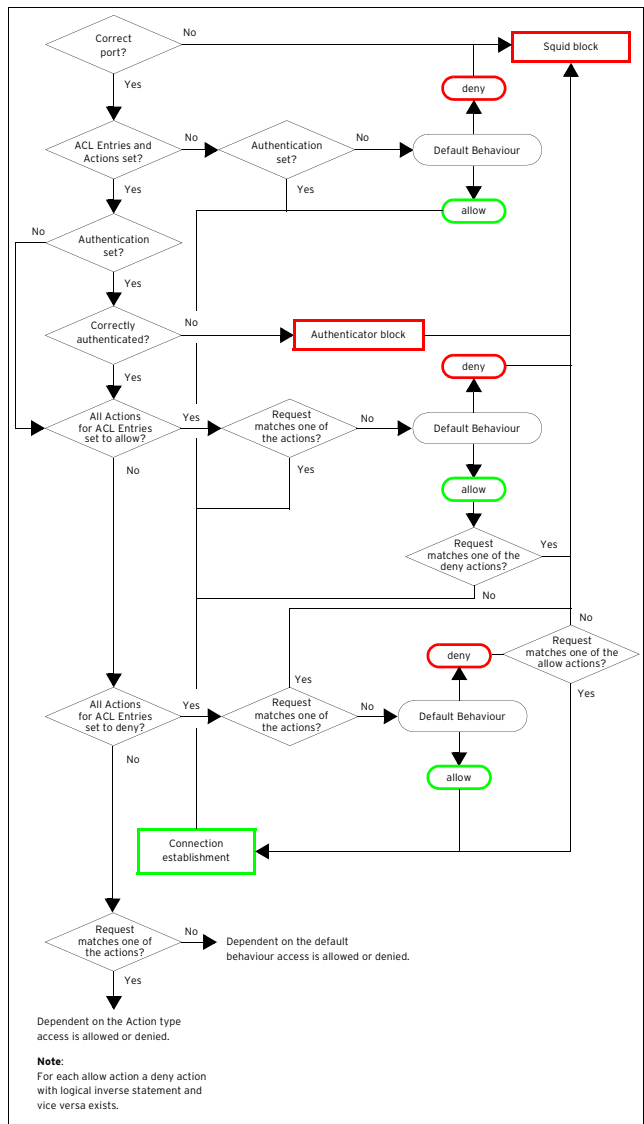
In the Access Control section, access control lists can be defined exhaustively. Sections **ACL ENTRIES** and **ACTIONS** make GUI helpers available for configuration. Sections **ACL FILELIST** and **LEGACY** allow integration of complete ACL files.

The parameter **Access Configuration** influences the configuration mode. With **default** selected, access control is managed through **ACL ENTRIES**, **ACTIONS**, and **ACL FILELIST** sections. If set to **legacy** all ACLs may be specified manually in the **LEGACY** section without using GUI helpers.

**Note:**  
When configuring Access Control in legacy mode or through an **ACL FILELIST**, ACLs have to match **squid.conf** syntax exactly.

The value **Default** is related to the use of the default **Access Configuration** mode. It sets all ACLs, which have not been set to allow explicitly, to deny by default. Squid first looks for ACL files in the **ACL FILELIST**, then continues the workflow by processing entries in the **ACL ENTRIES** and **ACTIONS** sections.

Fig. 12-7 Proxy Access Handling Scheme



### 1.2.3.3 Access Control - Using Regular Expressions

In phion netfence Perl-compatible regular expressions (PCRE) show to advantage, for example in the HTTP Proxy server ACL configuration section. Here they may be used in various configuration fields where the aim is to substitute hard coded character strings against expressions that match in multiple cases. The table below summarises those regular expressions, which are most frequently applicable for this purpose.

**Note:**

Abundant reading is available for an exhaustive instruction of how to use regular expressions. A handy quick syntax overview can be found at <http://www.perl.com/doc/manual/html/pod/perlre.html>.

**Note:**

Regular expressions in the HTTP proxy server configuration are treated case insensitive.

**Attention:**

In fields where both, combinations of words AND regular expressions are applicable, take care not to use characters, which could lead to misinterpretation without due care.

**Note:**

For lucidity reasons strive for formulating regular expressions as simple as possible.

**Table 12-1** Short overview of metacharacters in regular expressions

Metacharacter	Description
.	Matches any single character (including space). For example, the regular expression <b>b.g</b> would match the strings <b>big</b> , <b>bug</b> , <b>b g</b> , but not <b>blog</b> .
\$	Matches the end of a line. For example, the regular expression <b>mp3\$</b> would match the end of the string "song.mp3" but not the string "mp3 download". The expression <b>mp3\$</b> may for example be used in an ACL entry with type <b>urlextension</b> or <b>urlpathextension</b> to exclude download of mp3 files where the string <b>mp3</b> represents the URL ending.
^	Matches the beginning of a line. For example, the regular expression <b>^mp3</b> would match the beginning of the string "mp3 player available for download" but would not match "get your free mp3 player".
*	Matches zero or more occurrences of the character immediately preceding. For example, the regular expression <b>.*</b> means match any number of any characters.
\	This is the quoting character, use it to treat the succeeding character as an ordinary character. For example, <b>\\$</b> is used to match the dollar sign character (\$) rather than the end of a line. Similarly, the expression <b>\.</b> is used to match the dot character rather than any single character. For example, the expression <b>\.mp3</b> may be used in an ACL entry with type <b>urlextension</b> or <b>urlpathextension</b> to exclude access to links containing the file ending <b>.mp3</b> , where <b>.mp3</b> does not necessarily have to represent the URL ending.
[ ]	Matches anyone of the characters between the brackets. For example, the regular expression <b>[aiu]g</b> matches <b>bag</b> , <b>big</b> , and <b>bug</b> , but not <b>beg</b> .
[0-9] [a-z]	Matches a range or multiple ranges of characters or ciphers between the brackets. For example, the regular expression <b>[1-5]</b> matches all ciphers from 1 to 5. The regular expression <b>[a-cg-k]</b> matches all letters from a to c and g to k.
[^1-5] [^a-k]	Use the caret as first character after an opening bracket to match any character except those in the range. For example, the regular expression <b>[^1-3a-k]</b> matches all characters except 1 to 3 and a to k.

**Table 12-1** Short overview of metacharacters in regular expressions

Metacharacter	Description
?	Matches 0 or 1 occurrence of the character or regular expression immediately preceding. For example, the regular expression <b>z?</b> would match the string <b>warez</b> but not the string <b>intermezzo</b> .

### 1.2.3.4 Access Control - Section ACL Entries

This section allows defining ACL Types, which afterwards when set together in the ACL ACTION section, build up an access control list. Click **Insert ...** to generate a new ACL and specify a significant **Name** for it. The following objects are available for configuration:

**List 12-11** HTTP Proxy Service Parameters - Authentication Settings - ACL Entries

Parameter	Description								
<b>ACL Type</b>	In this place a pull-down menu displays all ACL Types available for configuration in the fields below. Choosing a type activates the corresponding field's <b>Edit ...</b> and <b>Clear</b> buttons. After type choice click <b>Edit ...</b> to open the succeeding parameters configuration dialogue.								
<b>Time Restrictions</b>	This parameter defines access during specific times (ACL Type: <b>time</b> ). <table border="1" data-bbox="1066 898 1544 1601"> <thead> <tr> <th>Name (predefined)</th> <td>timeconfig</td> </tr> <tr> <th>Use Local Box Time</th> <td>If checked, time restrictions apply according to box time zone settings.</td> </tr> <tr> <th>Time Zone</th> <td>This parameter is only active, if local box time settings do not apply. In this case, configure a time zone explicitly.                             <p><b>Note:</b> ACL entries regarding time settings are always converted to local box time settings in squid.conf. Only in case you are using local box time, conversion is not necessary and time in the ACL entries is exactly going to match box time. Do not let yourself be confused, if ACL entries written to squid.conf do not seem to be what you have configured. Have a look at the configuration example below (1.2.3.9 ACL Time Restrictions Configuration Examples).</p> </td> </tr> <tr> <th>Time Settings</th> <td>By default, the configuration is always active. Click the <b>Always</b> button to define the ACLs validity period explicitly. The button's label turns to <b>Restricted!</b> when time settings have changed. See 1.2.3.8 ACL Time Restrictions for a detailed description of Time Restrictions configuration.</td> </tr> </thead></table>	Name (predefined)	timeconfig	Use Local Box Time	If checked, time restrictions apply according to box time zone settings.	Time Zone	This parameter is only active, if local box time settings do not apply. In this case, configure a time zone explicitly. <p><b>Note:</b> ACL entries regarding time settings are always converted to local box time settings in squid.conf. Only in case you are using local box time, conversion is not necessary and time in the ACL entries is exactly going to match box time. Do not let yourself be confused, if ACL entries written to squid.conf do not seem to be what you have configured. Have a look at the configuration example below (1.2.3.9 ACL Time Restrictions Configuration Examples).</p>	Time Settings	By default, the configuration is always active. Click the <b>Always</b> button to define the ACLs validity period explicitly. The button's label turns to <b>Restricted!</b> when time settings have changed. See 1.2.3.8 ACL Time Restrictions for a detailed description of Time Restrictions configuration.
Name (predefined)	timeconfig								
Use Local Box Time	If checked, time restrictions apply according to box time zone settings.								
Time Zone	This parameter is only active, if local box time settings do not apply. In this case, configure a time zone explicitly. <p><b>Note:</b> ACL entries regarding time settings are always converted to local box time settings in squid.conf. Only in case you are using local box time, conversion is not necessary and time in the ACL entries is exactly going to match box time. Do not let yourself be confused, if ACL entries written to squid.conf do not seem to be what you have configured. Have a look at the configuration example below (1.2.3.9 ACL Time Restrictions Configuration Examples).</p>								
Time Settings	By default, the configuration is always active. Click the <b>Always</b> button to define the ACLs validity period explicitly. The button's label turns to <b>Restricted!</b> when time settings have changed. See 1.2.3.8 ACL Time Restrictions for a detailed description of Time Restrictions configuration.								
<b>Source IP Config</b>	This parameter defines a connection's source IP (ACL Type = <b>source</b> ). <table border="1" data-bbox="1066 1653 1544 1964"> <thead> <tr> <th>Name (predefined)</th> <td>sipconfig</td> </tr> <tr> <th>IP Configuration</th> <td>A pull-down menu makes configuration of <b>IP Ranges</b> or <b>Single IPs</b> available. The following menu entries exist:                             <ul style="list-style-type: none"> <li>➤ Singlemode</li> <li>➤ Rangemode</li> </ul>                             phion syntax applies.                         </td> </tr> <tr> <th>IP Ranges (from/to)</th> <td>Insert an IP range into these fields.</td> </tr> <tr> <th>Single IPs (Set IPs)</th> <td>Insert a single IP or multiple single IPs into this field.</td> </tr> </thead></table>	Name (predefined)	sipconfig	IP Configuration	A pull-down menu makes configuration of <b>IP Ranges</b> or <b>Single IPs</b> available. The following menu entries exist: <ul style="list-style-type: none"> <li>➤ Singlemode</li> <li>➤ Rangemode</li> </ul> phion syntax applies.	IP Ranges (from/to)	Insert an IP range into these fields.	Single IPs (Set IPs)	Insert a single IP or multiple single IPs into this field.
Name (predefined)	sipconfig								
IP Configuration	A pull-down menu makes configuration of <b>IP Ranges</b> or <b>Single IPs</b> available. The following menu entries exist: <ul style="list-style-type: none"> <li>➤ Singlemode</li> <li>➤ Rangemode</li> </ul> phion syntax applies.								
IP Ranges (from/to)	Insert an IP range into these fields.								
Single IPs (Set IPs)	Insert a single IP or multiple single IPs into this field.								

List 12-11 HTTP Proxy Service Parameters - Authentication Settings - ACL Entries

Parameter	Description
<b>Destination IP Config</b>	This parameter defines a connection's destination IP (ACL Type = <b>destination</b> ).
	<b>Name</b> (predefined) dipconfig
	<b>IP Configuration</b> A pull-down menu makes configuration of <b>IP Ranges</b> or <b>Single IPs</b> available. The following menu entries exist: <ul style="list-style-type: none"> <li>➤ Singlemode</li> <li>➤ Rangemode</li> </ul> phion syntax applies.
	<b>IP Ranges (from/to)</b> Insert an IP range into these fields.
<b>Single IPs (Set IPs)</b> Insert a single IP or multiple single IPs into this field.	
<b>Domain Config</b>	This parameter defines client domains (ACL Type = <b>sourcedomain / destinationdomain</b> ). Processing delays may be caused when using domain names as Squid needs to reverse DNS lookups (from client IP address to client domain name) before it can interpret the ACL.
	<b>Name</b> (predefined) domainconfig
	<b>Domains</b> Insert domain names into this field. <b>Note:</b> Domains names have to be preceded by a dot. Example: .phion.com
<b>User Authentication</b>	Defines users authenticating themselves in an external authentication program. (ACL Type = <b>proxyauthentication</b> ). This ACL type can only be used with user authentication set.
	<b>Name</b> (predefined) userconfig
	<b>Required for All Users</b> Set to <b>yes</b> (default: <b>no</b> ) if generally all users using the proxy should authenticate themselves. With setting to <b>yes</b> , the <b>Users</b> field below is deactivated. With setting to <b>no</b> , users have to be defined explicitly. <b>Note:</b> An ACL with setting <b>yes</b> can only be created <b>once</b> . You will be warned when trying to create a further identical ACL.
	<b>Users</b> Define user names for authentication. If authentication should apply, the ACL containing the user names has to be added to the ACL entry. Actions may be allowed or denied for the specified users after they have authenticated themselves.
<b>URL Path Config</b>	This parameter defines URL path regular expressions ( <i>urlpath_regex</i> ) (ACL Type = <b>urlpathextension</b> ) matching the URL but skipping protocol and hostname.
	<b>Name</b> (predefined) pathextconfig
	<b>URL Path Extensions</b> This field takes regular expressions (see 1.2.3.3 Access Control - Using Regular Expressions, page 329) or simply words or word patterns. All entries are treated case insensitive. <i>urlpath_regex</i> looks for the specified value in the URL path following the hostname, that is in URL <code>http://www.exampledomain.com/example/domain/index.htm</code> the word "example" will only be looked for within the path <code>"/example/domain/index.htm"</code> .

List 12-11 HTTP Proxy Service Parameters - Authentication Settings - ACL Entries

Parameter	Description
<b>URL Config</b>	This parameter defines URL extensions ( <i>url_regex</i> ) considering protocol and hostname (ACL Type = <b>urlextension</b> ).
	<b>Name</b> (predefined) extconfig
	<b>URL Extensions</b> This field takes regular expressions (see 1.2.3.3 Access Control - Using Regular Expressions, page 329) or simply words or word patterns. All entries are treated case insensitive. <i>url_regex</i> looks for the specified value in the URL path including protocol and hostname.
<b>Maximum Connections Config</b>	This parameter limits the maximum number of connections from a single client IP address (ACL Type = <b>maxconnections</b> ).
	<b>Name</b> (predefined) maxconnconfig
	<b>Define Maximum Connections</b> Insert a value for the maximum number of connections (default: <b>5</b> ). The value of the ACL is TRUE if the number is larger than the specified one.
<b>Protocol Config</b>	This parameter specifies the transfer protocol (ACL Type = <b>protocol</b> ).
	<b>Name</b> (predefined) protocolconfig
	<b>Define Transfer Protocol</b> Specify a transfer protocol, for example HTTP, FTP, ...
<b>Requestmethod Config</b>	This parameter specifies the request method (ACL Type = <b>method</b> ).
	<b>Name</b> (predefined) methodconfig
<b>Port Config</b>	<b>Define Request Method</b> Specify a request method, for example GET, POST, UPDATE, ...
	This parameter specifies the destination's port addresses (ACL Type = <b>destinationport</b> ).
<b>Browser Config</b>	<b>Name</b> (predefined) portconfig
	<b>Specify Destination Port Address</b> Insert the destination server's port number.
	This parameter defines regular expression patterns or words, matching the user-agent header transmitted during the request (ACL Type = <b>browser</b> ).
<b>Browser Config</b>	<b>Name</b> (predefined) browserconfig
	<b>Define Browser Access</b> This field takes regular expressions (see 1.2.3.3 Access Control - Using Regular Expressions, page 329) or words. If, for instance, the word <i>Firefox</i> is configured, it will be searched for in the user-agent header of an incoming request.

**Attention:**

Each ACL Entry may only consist of one ACL Type.

**Attention:**Do not forget to delete values configured for use in the ACTIONS section, parameter **ACL Entries for this Action** manually when deleting an ACL Entry, as the conjoined actions are not deleted automatically. Actions with broken links to its parent will cause the proxy to fail.

### 1.2.3.5 Access Control - Section Actions

This section serves to construct an ACL list, which the proxy server works through one by one, according to the action's priority number. The **Default** parameter setting below the Actions section specifies the final measure to take after the workflow of the list has been completed.

**Note:**

In an analogous manner to firewall rule handling, proxy settings are processed from top to bottom.

Click **Insert ...** to generate a new **Action** and specify a significant **Name** for it.

**Attention:**

The name specified in this place is used as expression in the proxy server's ACL list. The same applies to the **Name** field specified for a new record in the Section Neighbour Settings section (Access control section, see Section Neighbour Settings, page 326). To avoid conflicts, make sure these two names never match.

The following objects are available for configuration:

List 12-12 HTTP Proxy Service Parameters - Authentication Settings - Actions

Parameter	Description
<b>ACL Description</b>	Describe briefly, what this action should effect.
<b>ACL Priority</b>	Insert a value for this action's priority. Lower numbers mean higher priority. ACLs with higher priority are processed first.
<b>ACL Entries for this Action</b>	In this place a pull-down menu displays all configured ACL entries. Choose the ACL entries this action shall refer to and insert them into the field on the right side. <b>Note:</b> A maximum of 6 ACL entries can be inserted into an action. <b>Attention:</b> Remember to delete ACL entries from an action when deleting the value in the ACL ENTRIES section.
<b>Action</b>	This parameter sets the action to <b>allow</b> or <b>deny</b> .

**Note:**

See 1.2.3.10 Access Control List (ACL) Interpretation, page 333 for a workflow description of ACL lists.

### 1.2.3.6 Access Control - Section ACL FileList

ACL FileLists may be used as supplement to **ACL Entries** and **Actions**.

**Note:**

The ACL FileList is processed before those entries configured through ACL ENTRIES and ACTION sections.

Click the **Insert ...** button to define a new ACL List and specify a list **Name**. List Names may consist of ciphers only (max. length 12 ciphers). The number defined for an ACL Filelist is a direct marker for its priority. Lower numbers

mean higher priority. ACL Filelists are processed one by one according to their priority.

List 12-13 HTTP Proxy Service Parameters - Authentication Settings - ACL FileList

Parameter	Description
<b>ACL Filelist</b>	<b>Filename</b> All <b>ACL Entries</b> (see below) are stored in the specified <b>Filename</b> after clicking <b>OK</b> . The default location of the file is <code>/var/phion/preserve/proxy/&lt;servername&gt; &lt;servicename&gt;/root/</code> . In addition, it is also possible to change the location by specifying an absolute path in front of the filename (not recommended). In this case, the destination directory must exist. <b>Note:</b> Do not use <b>Filenames</b> such as <code>squid.conf</code> , <code>ftpsquid.conf</code> , ... This could lead into loss of configuration information. To avoid such situations, it is recommended to use the default location and <code>.acl</code> as the preferred filename extension (example: <code>aclfile.acl</code> ).
	<b>ACL Entries</b> These are the entries, which are written to the file defined through the parameter <b>Filename</b> . <b>ACL Entries</b> are processed line by line. A line must not exceed 1012 characters. If a greater length cannot be avoided, use <code>"/</code> to section lines. <b>Attention:</b> <b>ACL Entries</b> must exactly match the <code>squid.conf</code> syntax. They are not checked against <code>squid.conf</code> for compatibility. Do not use <code>phion</code> netmask syntax. <b>Note:</b> To include ACL entries specified in the ACL filelist, include them in the <b>Generic squid.conf Entries</b> field (see following syntax example).

### ACL Filelist Usage Example

**Step 1 Insert an ACL entry into the ACL filelist section**

Open the Access Control tab, lock the data set, then click **Insert ...** in the ACL Filelist section to add a new ACL file.

List 12-14 ACL Filelist Usage Example

Parameter	Description
<b>Name</b>	1
<b>Filename</b>	prxacl.acl
<b>ACL Entries</b>	10.0.8.20/255.255.255.255

**Step 2 Include the ACL file into the configuration**

Change to the Advanced tab and insert the following line at the beginning of the file displayed in the **Generic squid.conf Entries** field:

```
acl STAFF src "prxacl.acl"
acl WORLD dst 0.0.0.0/0.0.0.0
http_access allow STAFF WORLD
```

The value `STAFF` and `WORLD` specify the ACL names. In the example HTTP access to the Internet is allowed for the network client with the address 10.0.8.20.



### 1.2.3.7 Access Control - Section Legacy

This section enables creation of an ACL file exactly matching squid.conf syntax.

This parameter set is only available if parameter **Access Configuration** is set to **legacy**.

**List 12-15** HTTP Proxy Service Parameters - Authentication Settings - Legacy

Parameter	Description
<b>Name</b> (predefined)	aclconfexpert
<b>Access Control Entries</b>	Insert the ACL Entries into this field. <b>Attention:</b> ACL Entries must exactly match the squid.conf syntax. They are not checked against squid.conf for compatibility. Do not use phion netmask syntax. <b>Note:</b> This field either takes complete ACLs, but may as well include entries from the ACL filelist. Syntax usage as given in the example above applies.

**Note:**

squid.conf can be located in the path `/var/phion/preserve/proxy/<servername_service/>/root/`.

**Note:**

A quick syntax check for squid.conf can be executed by entering the following command at the command line interface: `sudo squid -N -f /var/phion/preserve/proxy/<servername_service/>/root/squid.conf`. If commands have been misarranged, the row number containing the flawed configuration will be thrown to the output.







### 1.2.3.8 ACL Time Restrictions

ACL Time Restrictions are a configuration part of the Access Control - Section ACL Entries parameter **Time Settings**. Clicking the button **Always** opens the **Time Interval** configuration window. If time restriction applies, the label of the button changes to **Restricted!**.

The granularity of time restriction is 1 hour on a weekly base.

The time settings ACL entry is preset to always active by default, which means that all checkboxes in the **Time Interval** dialogue window are unchecked. Checking a box deactivates a time interval for the given time.

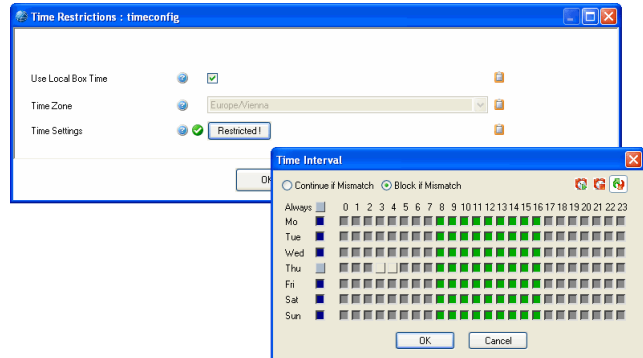
**List 12-16** HTTP Proxy Service Parameters - Authentication Settings - Time Restriction configuration

Parameter	Description
 Set allow	Select  to clear selected checkboxes.
 Set deny	Select  to select checkboxes as disallowed time intervals.
 Set Invert	Select  to configure allowed and disallowed time intervals simultaneously.
<b>Continue if mismatch / Block if mismatch</b> (default)	<b>Attention:</b> Always leave the default setting Block if mismatch.

### 1.2.3.9 ACL Time Restrictions Configuration Examples

#### Example 1

**Fig. 12-8** ACL Time Interval configuration - Example 1



In the example above, local box time applies to time restriction settings.

In the time interval window, access has been activated for all times except Wednesday 03:00 to 05:00.

After saving and execution of **Send Changes** and **Activate**, the following ACL entries will be generated:

**Note:**

In squid.conf the days of the week are stated as follows: **M** - Monday, **T** - Tuesday, **W** - Wednesday, **H** - Thursday, **F** - Friday, **A** - Saturday, **S** - Sunday.

```
acl mytime time M 00:00-24:00
acl mytime time T 00:00-24:00
acl mytime time W 00:00-03:00
acl mytime time W 05:00-24:00
acl mytime time H 00:00-24:00
acl mytime time F 00:00-24:00
acl mytime time A 00:00-24:00
acl mytime time S 00:00-24:00
```

**Interpretation:**

An ACL entry has been generated for each day of the week, spanning the whole day (except for Wednesday).

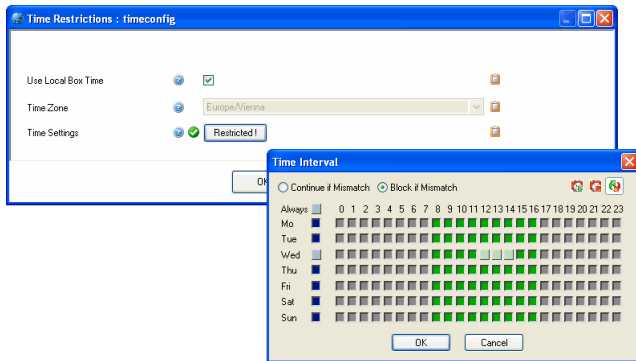
Two ACL entries have been created for Wednesday, as there time flow has been intercepted between 03:00 and 05:00.

Inserted into the Actions section with policy allow and default policy denied, this ACL entry will cause allowed proxy access on every day of the week, except Wednesday, 03:00 and 05:00.



## Example 2

Fig. 12-9 ACL Time Interval configuration - Example 2



In the example above, time zone Europe/London applies to time restriction settings.

In the time interval window, access has been activated for all times except Wednesday 14:00 to 15:00.

After saving and execution of **Send Changes** and **Activate**, the following ACL entries will be generated:

```
acl mytime time M 01:00-24:00
acl mytime time T 00:00-01:00
acl mytime time T 01:00-24:00
acl mytime time W 00:00-01:00
acl mytime time W 01:00-13:00
acl mytime time W 16:00-24:00
acl mytime time H 00:00-01:00
acl mytime time H 01:00-24:00
acl mytime time F 00:00-01:00
acl mytime time F 01:00-24:00
acl mytime time A 00:00-01:00
acl mytime time A 01:00-24:00
acl mytime time S 00:00-01:00
acl mytime time S 01:00-24:00
acl mytime time M 00:00-01:00
```

### Note:

Multiple entries are generated for each day in squid.conf due to time conversion.

### Interpretation:

Two ACL entries have been generated for each day of the week, spanning the whole day (except for Wednesday).

Three ACL entries have been created for Wednesday, as there time flow has been intercepted between 14:00 and 15:00 Note, that the missing time span has been generated as gap between 13:00 and 16:00.

Inserted into the Actions section with policy allow and default policy denied, this ACL entry will cause allowed proxy access on every day of the week, except Wednesday, 14:00 to 15:00. Europe/London time or 15:00 and 16:00 local box time respectively.

A user from London trying to access the proxy at 14:59 London/Europe time will be rejected, because this corresponds 15:59 local box time and is still within the disallowed time span.

## 1.2.3.10 Access Control List (ACL) Interpretation

The following example configuration attempts to explain the logics of

- how to create ACL entries and put them together in an action.
- how actions are processed by the proxy server.

Fig. 12-10 ACL Entries and Actions configuration example

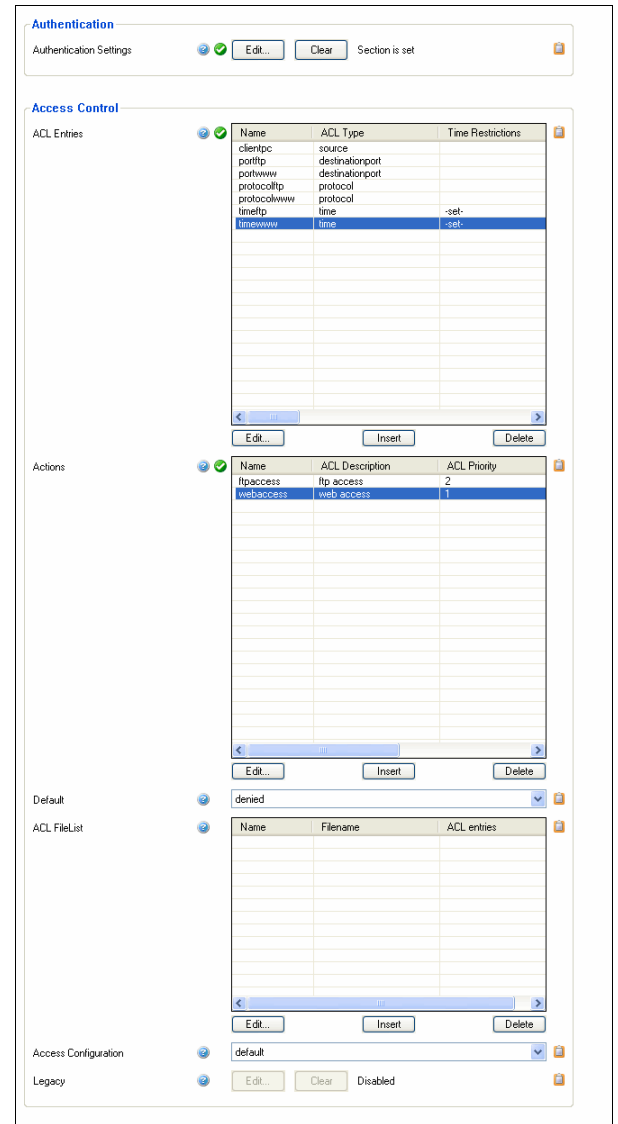


Figure 12-10 depicts an exemplary Access Control configuration, with the following ACL Entries and Actions configured in detail:

### ➤ ACL Entries

List 12-17 ACL ENTRIES configuration

Name	ACL Type	Value
<b>clientpc</b>	source	10.0.8.1
<b>portftp</b>	destinationport	21
<b>portwww</b>	destinationport	80
<b>protocolftp</b>	protocol	FTP
<b>protocolwww</b>	protocol	HTTP
<b>timeftp</b>	time	Access activated Mo, 09:00 - 13:00
<b>timeweb</b>	time	Access activated Mo-Fr, 08:00 - 17:00

## ➤ Actions

Fig. 12-11 Configuration of Action webaccess

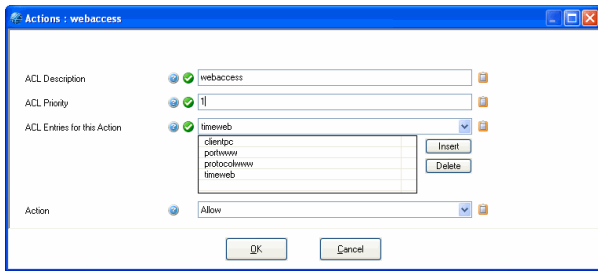


Table 12-2 Actions configuration

ACL Description	ACL Priority	ACL Entries for this Action
<b>webaccess</b>	1	clientpc, portwww, protocolwww, timeweb
<b>ftpassess</b>	2	clientpc, portftp, protocolftp, timeftp

## ➤ Default policy: denied

These actions are summarised to the following lines in squid.conf:

```
http_access allow clientpc portwww
protocolwww timeweb
http_access allow clientpc portftp
protocolftp timeftp
```

This is interpreted as follows:

Allow access, if **clientpc AND portwww AND protocolwww AND timeweb is TRUE**

--- if **TRUE**, stop processing further rules ---

--- **OR** proceed to the next rule, if this is not the case ---

Allow access, if **clientpc AND portftp AND protocolftp AND timeftp is TRUE.**

Let us consider the following scenarios:

It is Monday, 09:00. The user working at `clientpc` tries to access the Internet on port 80. His connection attempt will be considered by the rule `http_access allow clientpc portwww protocolwww timeweb`, access will be granted and no further rules processed.

It is Monday, 14:00. The user working at `clientpc` tries to access an FTP server on port 21. On his connection attempt, the first rule will be processed and considered false because none of the parameters matches except of Access Entry `clientpc`. Subsequently the second rule `http_access allow clientpc portftp protocolftp timeftp` will be processed, and again, it will be considered false, because the Access Entry `timeftp` does not match. The connection attempt will be rejected, as none of the rules matches, and the default policy as well denies it.

## 1.2.3.11 Cache Behaviour Configuration Example

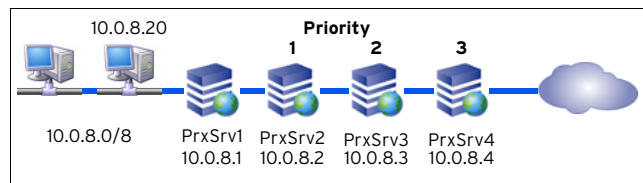
Correct **Cache Behaviour** configuration becomes important when the proxy server is surrounded by multiple adjacent neighbour caches. In particular, **Cache Priority** settings have an immediate effect on execution of **Cache Peer Access** and **Domain Restrictions** settings.

The following example is meant to point up the importance of correct configuration.

ProxySrv1 is surrounded by three neighbour caches ProxySrv2, ProxySrv3 and ProxySrv4, each of them configured as its parents.

The aim is to direct all requests with source IP 10.0.8.20 to ProxySrv2 and all requests with the destination `exampledomain.com` to ProxySrv3. All other requests shall be fetched from the cache of ProxySrv4.

Fig. 12-12 Proxy neighbour cache configuration - Example setup



A **Cache Peer Access** filter has to be set for ProxySrv2 and a **Domain Restrictions** filter has to be set for ProxySrv3. ProxySrv4 is set up without any filters, which means that all requests not matching the configured filters will be directed to it.

### ➤ Neighbour Configuration settings for **ProxySrv2**:

```
Name: ProxySrv2
IP/Hostname: 10.0.8.2
Neighbour Type: parent
Exclusive Parent: no
Cache Priority: 1
Cache Peer Access: 10.0.8.20
Cache IP Objects: no
```

### ➤ Neighbour Configuration settings **ProxySrv3**:

```
Name: ProxySrv3
IP/Hostname: 10.0.8.3
Neighbour Type: parent
Exclusive Parent: no
Cache Priority: 2
Domain Restrictions: *.exampledomain.com
Cache Domain Objects: no
```

### ➤ Neighbour Configuration settings for **ProxySrv4**:

```
Name: ProxySrv4
IP/Hostname: 10.0.8.4
Neighbour Type: parent
Exclusive Parent: no
Cache Priority: 3
```

#### **Note:**

ProxySrv4 is vital for the example setup to work. If not present, requests not matching the configured filters cannot be directed to any neighbour. ProxySrv1 cannot process the requests spontaneously without appropriate directive.

## 1.2.4 Content Inspection

### 1.2.4.1 Section Virus Scanner

Via this section the integrated virus scanner is enabled/disabled. Due to the complexity please have a look at **Anti-Virus**, page 367.

### 1.2.4.2 Section Data Leak Prevention

List 12-18 Proxy Service Parameters - section Data Leak Prevention

Parameter	Description
<b>DLP</b>	Data Leak Prevention consists on disallowing HTTP POST requests. Set to <b>Enable</b> to enable Data Leak Prevention.
<b>DLP Exception URLs</b>	Define here exceptions for Data Leak Prevention, that is HTTP POST requests on those URLs are allowed even if DLP was set to <b>Enable</b> . Patterns (* and ?) are allowed here.

### 1.2.4.3 Section Redirector Settings

This section has to be configured when the ISS Proventia Web Filter or another external filter is implemented into the HTTP proxy server for URL filtering. See 3. ISS Proventia Web Filter, page 342 for configuration details.

## 1.2.5 Advanced

#### Note:

The section **Optimizations** is only available for the Secure Web Proxy.

List 12-19 Proxy Service Parameters - Advanced view - section Optimizations

Parameter	Description
<b>Read Timeout (sec.)</b>	Define here the read timeout of the Secure Web Proxy in seconds.  <b>Note:</b> This timeout affects connections to the internet and to the ICAP server.

List 12-20 Proxy Service Parameters - Advanced view - section Advanced

Parameter	Description
<b>Generic squid.conf Entries</b>	The whole configuration file of the proxy service is displayed. This field offers the possibility to edit the whole configuration file (except the access control part) manually. Use this section to configure a transparent proxy (see 1.3 Transparent Proxy, page 335) or reverse proxy (see 1.4 Reverse Proxy, page 336).  <b>Attention:</b> These entries must exactly match the squid.conf syntax. Entries are not checked against squid.conf for compatibility. <b>Do not use phion netmask syntax.</b>

#### Note:

A quick syntax check for squid.conf can be executed by entering the following command at the command line interface:

```

squid -N -f
/vary/phion/preserve/proxy/<servername_servicename>/root/squid.conf.
    
```

If commands have been misarranged, the row number containing the flawed configuration will be thrown to the output.

## 1.3 Transparent Proxy

This mode allows the proxy to work transparently to the client. With a transparent proxy the clients do not have to be configured in a special way, whereas a firewall or a router must be configured to redirect proxy traffic (port 80) to the proxy listening on port 3128 (for example). Since clients are not configured to use a proxy, http traffic will be passed to port 80. A firewall or a router then has to redirect this traffic to the proxy. The usage of a transparent proxy may be useful, for example in a migration scenario, where multiple existing clients were not configured to use a proxy and a reconfiguration of them would be a unreasonable big effort.

To configure a proxy as a transparent one, the following configuration lines have to be entered into the genericsquid configuration section (see 1.2 Configuration, Generic squid.conf Entries, page 335):

```

httpd_accel_host virtual      IP address of web
server (use virtual for multiple servers)

httpd_accel_port 80          port of web server

httpd_accel_with_proxy on

httpd_accel_uses_host_header on
    
```

The `httpd_accel_port` directive defines the port the origin server is listening on (port 80). For virtual port support use 0 instead of 80. Squid does not need to know how requests arrive at its listening port (3128). This has to be done by the firewall or router.

Squid sees a request for an URL and connects to port 80 (or virtual) of the server where the URL resides. Squid does not have any control over the arriving request types. If Squid is listening on port 3128 it assumes that data arrives using a protocol it can handle (HTTP, FTP over HTTP). The packet type redirected to Squid is determined entirely by the host's firewall (or an external router) and is out of Squid's control.

#### Attention:

`proxy_auth` cannot be used in conjunction with a transparent proxy because it collides with any authentication done by origin servers.

#### Attention:

HTTP 1.0 must not be used in conjunction with a transparent proxy since the header of HTTP 1.0 does not contain the address of the destination server. The information gets lost, when the request is redirected to the firewall (or the router).

## 1.4 Reverse Proxy

The Squid reverse proxy is designed for supplying static content served by web servers placed behind of it from its own cache. This way, reverse proxy mode reduces load on web servers and is thus also known as **httpd-accelerator mode**.

To configure a reverse proxy, add options assigned to the `httpd_accel` directive to the `squid.conf` file. Refer to the official `squid.conf` documentation for details. You may edit `squid.conf` in the generic squid configuration section (see 1.2 Configuration, Generic `squid.conf` Entries, page 335).

The following options are configurable:

- `http_port 80`  
The reverse proxy listens for connections on this port. Normally, this is set to port **80** paying regard to the fact that incoming requests will mostly be directed to the default HTTP port.
- `httpd_accel_host <server_IP>/virtual`  
This option specifies the address of the actual web server. Specify an IP address, if only a single web server serves web content. If the proxy is meant to supply cached content from multiple web servers, use `httpd_accel_host virtual`.

**Note:**

HTTP 1.0 is not applicable with option `httpd_accel_host virtual`.

- `httpd_accel_port 80`  
The web server listens for connections on this port. As the web content will be served from a separate physical machine, you may consider using the default listening HTTP port **80**. Optionally, switch the listening port to another value.

**Note:**

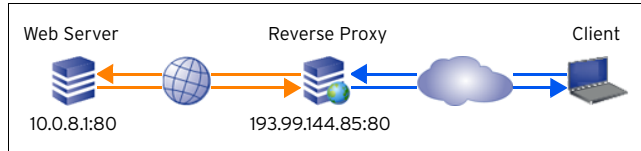
Multiple web servers must provide content on one port uniformly.

- `httpd_accel_single_host on/off`  
This option specifies whether to forward uncached requests to a single back end web server. If set to `on`, requests will be forwarded regardless of what any redirectors or host headers say.
- `httpd_accel_with_proxy on/off`  
This option specifies if Squid should act as both, standard and reverse proxy or only as reverse proxy. Note that generally better performance will be achieved when this option is set to `off`.
- `httpd_accel_uses_host_header off`  
Requests in HTTP version 1.1 include a host header, specifying host name or IP address of the URL. This option should remain `off` in reverse proxy mode.
- `hosts_file /etc/hosts`  
This option defines the location of the `hosts` file. This has to be specified, when requests to your back end web servers are addressed to FQDNs and the proxy server itself fetches DNS entries from external name servers. In the `hosts` file, map the FQDNs of your web sites to the actual IP the site is published on. Configure

mappings in **Config** > **Box** > **Settings** > **DNS** section > **Known Hosts** (see 2.2.3.3 DNS, page 55).

### 1.4.1 Example Setup

Fig. 12-13 Reverse proxy example configuration



In the example setup, a web server is configured running three virtual hosts on an internal IP address 10.0.8.1. Clients direct requests to these sites to `www.myDomain.com`, `sub.myDomain.com`, and `sub2.myDomain.com`. These names are resolvable to the IP address 193.99.144.85, which is the official external address of the reverse proxy server.

The reverse proxy forwards not yet cached requests to the appropriate virtual host running on the IP address 10.0.8.1, and otherwise serves the requested content from its cache.

The following parameters determine settings in the `httpd_accel` directive of the `squid.conf` file:

Table 12-3 Example: `squid.conf` file - `httpd_accel` directive

Parameter	IP address	Domain
Web Server	10.0.8.1	<code>www.myDomain.com</code> <code>sub.myDomain.com</code> <code>sub2.myDomain.com</code>
DNS	IN A 193.99.144.85	<code>www.myDomain.com</code> <code>sub.myDomain.com</code> <code>sub2.myDomain.com</code>
/etc/hosts	10.0.8.1 <code>mySite1 mySite2 mySite3</code> <code>www.myDomain.com sub.myDomain.com</code> <code>sub2.myDomain.com</code>	

In the `squid.conf` file, the corresponding options have to be specified as follows:

Table 12-4 Example: `squid.conf` file - corresponding options

Option	Setting
<code>http_port</code>	80
<code>httpd_accel_host</code>	10.0.8.1
<code>httpd_accel_port</code>	80
<code>httpd_accel_single_host</code>	on
<code>httpd_accel_with_proxy</code>	on/off (recommended)
<code>httpd_accel_uses_host_header</code>	off
<code>hosts_file</code>	/etc/hosts

## 2. Secure Web Proxy

### 2.1 Overview

phion's Secure Web Proxy ensures that SSL traffic doesn't pass unchecked through your network's HTTP proxy chain. Encrypted data sent and received by clients is decrypted transparently so that it can be inspected for viruses and other malicious content - just like any other normal HTTP traffic.

That's not the only advantage. Many HTTPS servers aren't able to issue a valid certificate signed by an official Certificate Authority (herein referred to as "CA"), thereby proving their authenticity. And displayed browser alerts don't always catch the attention of today's average user. Not realising their possible consequences, they are often simply ignored. That's why phion's Secure Web Proxy provides diverse options for "Certificate Verification". Depending on your security requirements, you can configure your certificate settings from low to very high.

Once it has been determined that a certificate is invalid, the client will be prohibited from communicating with the website, an incident ticket will be generated and its reference number will appear. This ticket helps the administrator determine the cause of nonconformity and decide what further action should be taken. The questionable site can either be blacklisted permanently or added to the whitelist, which would allow the user to connect to the site despite any previous problems with its certificate. In addition, most CAs provide so-called "Certificate Revocation Lists" (CRLs) or lists of revoked or no longer valid certificates (due to misuse or other reasons). Web browsers don't usually retrieve and update such lists themselves. Not so with phion's Secure Web Proxy - revocation lists are kept up-to-date at all times.

### 2.2 Technical Details

A basic knowledge of SSL certificates, certificate signing and CAs is assumed in the following remarks:

The Secure Web Proxy effects transparent decryption by acting as the endpoint of the client's SSL connection and maintaining a cryptographically independent connection to the target web server. As a result, there are two separate SSL connections to forward data from one to the other by the proxy on one logical channel: one between the client and the proxy and the other between the proxy and the target web server. This means that the actual payload is decrypted by the proxy on both sides and is inspected just like any other normal clear text traffic.

Without the client being alerted to the invalid certificate, the proxy generates a valid certificate for the site

on-the-fly using a proper "CommonName". The certificate is signed by the proxy's root certificate. This root certificate must first be installed in the client's known CA database.

As mentioned above, the proxy checks a server's certificate for validity. There are numerous options for determining a certificate's validity. This will be explained later. Only once a certificate has been validated will the proxy begin forwarding data to and from the client.

### 2.3 Installation

#### Attention:

Using the Secure Web Proxy requires additional software packages which are not part of the installation CD-ROM due to import/export regulations. Please contact your local phion Partner in order to request these specific packages.

A box server already has to exist, before a Secure Web Proxy service can be created.

#### Note:

When using a HTTP proxy and a Secure Web Proxy on the same virtual server, it is mandatory to modify the listening port of the Secure Web Proxy, since both types of proxy use port 3128 as default listening port.

To create a Secure Web Proxy service, select **Create Service** from the context menu of **Config** > **Box** > **Virtual Servers** > **<servername>** > **Assigned Services**, select **Secure-Web-Proxy** as software module and configure services basic settings.

By clicking **Activate**, the new service is sent to the netfence gateways and the newly installed Secure Web Proxy service is ready for configuration.

The Secure Web Proxy service will generate a number of log files. These can be viewed via the Log Viewer (**Log Viewer**, page 289).

#### Note:

Installation via PAR file requires this procedure:




- Install the box via PAR File
- Install the additional software package
- Perform a config dummy change and execute **Send Changes** > **Activate**










## 2.4 Configuration

If you have ever configured a "regular" proxy, many of the options will be familiar to you. In fact, with a few small differences, everything except the SSL-related options is the same. The SSL options are described in the following.

The Secure Web Proxy Service configuration area provides three configuration entities:

-  **ISS Proventia Web Filter Config** (see 3. ISS Proventia Web Filter, page 342)
-  **Service Properties (Configuration Service - 4. Introducing a New Service, page 97)**
-  **Secure-Web-Proxy Settings** (see below)

### 2.4.1 Secure-Web-Proxy Settings

Browse to  **Config** >  **Box** >  **Virtual Servers** >  <servername> >  **Assigned Services** >  <servicename> (**sslprx**) >  **Secure-Web-Proxy Settings** to access the configuration dialogue.

#### Note:

The parameters enlisted in the following are SSL-related only. For a general description of view **General**, **Network**, **Access Control**, **Content Inspection** and **Advanced**, please consult 1. HTTP Proxy, page 324.

However, note the following restrictions:

#### Note:

FTP is by default disabled. If enabled, FTP traffic will not be scanned for viruses.

- **General** view:  
There are no Log Settings. The system automatically logs access and cache.
- **Network** view:  
The most significant difference between a Secure Web Proxy and a normal proxy is that the Secure Web Proxy is configurable for one parent proxy only. If the setup has multiple parent proxies, the Secure Web Proxy will have to be daisy-chained with a normal proxy, where the parents can be configured as usual.

#### 2.4.1.1 SSL Settings

List 12-21 Secure Web Proxy - section SSL Settings

Parameter	Description
<b>Enable SSL Decryption</b>	Allows SSL decryption, the process of decrypting and inspecting data (default: <b>Yes</b> ).
<b>Enable Certificate Verification</b>	Validates certificates (default: <b>Yes</b> ). <b>Attention:</b> When this parameter is disabled, server certificates will not be validated. This means that clients will be able to communicate with malicious sites (like phishing sites) without realising there is a threat. It is recommended that this option only be disabled by someone who knows what they are doing.
<b>Use Self-Signed Certificate</b>	Define whether using a self signed or external certificate.

List 12-21 Secure Web Proxy - section SSL Settings

Parameter	Description
<b>Root CA Private Key / Root CA Certificate</b>	Generates the proxy's issuing root certificate. The <b>Root CA Certificate</b> should be exported and added to all client CA databases. <b>Note:</b> All SSL client-connections will receive a temporarily created certificate signed by this configured CA instead of the real certificate when establishing a HTTPS connection. The certificate and the corresponding private key are used for SSL/TLS encryption and decryption. If this root certificate is not installed on the client computers, users will get certificate-error warnings by the browser on each new HTTPS connection.
<b>External Root CA Private Key / External Root CA Certificate</b>	Use this parameters to import external root certificates. Instead of using a self signed certificate (parameters above), one can import an external root certificate and its corresponding private key. <b>Note:</b> The root certificate <b>must</b> be signed by the private key. <b>Note:</b> The notes from the parameters above apply to these parameters too.
<b>Notify User</b>	Specifies whether or not the user should be notified whenever SSL connections are decrypted, logged or inspected (default: <b>Yes</b> ). When enabled, a splash screen will appear in the user's browser at regular intervals (see Notify Again After (min)).
<b>Notify Again After (min)</b>	When enabled, a notification will reappear after a specified amount of time. The default value is <b>60</b> minutes.

#### 2.4.1.2 SSL Certificates

List 12-22 Secure Web Proxy - SSL Certificates - section Certificate Verification

Parameter	Description
<b>Allow CommonName Wildcards</b>	Accepts wildcards in the CommonName such as *.domain.com. Browsers such as IE or Firefox allow wildcards and/or regular expressions. Disabling this parameter provides more security (default: <b>No</b> , which means disabled).
<b>Deny Expired Certificates</b>	Determines whether or not expired certificates should be denied (default: <b>Yes</b> ).
<b>Allow Visit After Confirm</b>	If a certificate is not valid, an information page will appear in the browser. If this parameter is disabled, an incident ticket will be generated and access to the site will be denied. When this parameter is enabled, the user can connect to the site by clicking <b>Allow</b> (default: <b>No</b> ). <b>Note:</b> It is recommended that this parameter be disabled as it is, essentially, the same override mechanism provided by web browsers.

List 12-23 Secure Web Proxy - SSL Certificates - section Certificate Revocation

Parameter	Description
<b>Enable Revocation Check</b>	Checks every certificate against the revocation list of the issuing CA (provided one is available) (default: <b>Yes</b> ).
<b>Download CRLs at Hour (0..23)</b>	Specifies when Certificate Revocation Lists (CRLs) should be retrieved from the CAs.
<b>User Real-Time Check (OCSP)</b>	In addition to CRLs, it is possible to do a real-time check of the OCSP (Online Certificate Status Protocol)(default: <b>Yes</b> ). If a CA supports OCSP, a certificate's validity will be checked in real time and the result will be cached for one day.
<b>Block Unknown State</b>	When enabled, certificates will be denied if their revocation status is not determinable (either via CRLs or OCSP)(default: <b>No</b> ). This parameter is usually enabled in high-security environments. However, it results in many incident reports.



List 12-24 Secure Web Proxy - SSL Certificates - section Client Certificates

Parameter	Description
	This section discusses actions to be taken should a server request a client certificate - a seldom but, nevertheless, possible SSL transaction. Since private details of the client certificate are known only to the client, the SSL proxy will not be able to interact as it would with other SSL connections.
<b>Client Certificate Action</b>	Establishes the action to take when a client certificate is requested. The connection will either be tunnelled (without decryption) or denied (default).

### 2.4.1.3 SSL Exceptions

This section explains how to configure exceptions, which are made up of a server name (without the leading `https://`) or an IP address. There are three different types of exception lists:

- The **Blacklist** prohibits the client from accessing the listed servers or websites.

**Note:**  
Restriction is based on the site's certificate rather than on the actual server name or IP address.

- The **Whitelist** allows clients to access the listed servers or websites, even should there be something wrong with its certificate.
- The **Tunnellist** specifies which servers or website connections should be tunnelled (neither intercepted nor decrypted).

## 2.5 Operation

In addition to configuration, certain administrative actions can be taken in the Graphical User Interface (GUI). To access the GUI, select **SSL Proxy** in the box menu.

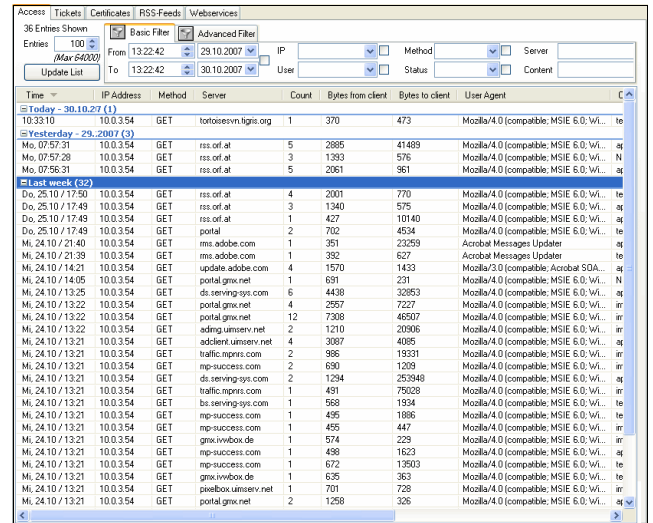
The following tabs are available:

- **Access** - view accumulated real-time log.
- **Tickets** - manage incident tickets created when a user encounters an invalid certificate.
- **Certificates** - inspect and manage all known Root CAs.
- **RSS-Feeds** - inspect and manage all known RSS-Feeds
- **Webservices** - inspect and manage all known webservices (including sub functions)

**Note:**  
Each tab, except for **Certificates**, provides additional filter settings. The options in these filter settings are taken from the available entries and will become active as soon as the checkbox to the right of each entry is selected.

## 2.5.1 Access Tab

Fig. 12-14 Secure Web Proxy GUI - Access tab



Following columns organize the **Access** tab of the Secure Web Proxy.

- **Time** - point in time when the connection was established. The content of this column may differ depending on selected time "groups" and set UTC time flag (see 2.5.1.1 Access Context Menu, page 340).
- **IP Address** of the client who requested the connection.
- **Method** that is used for connecting (according to Method Definitions in RFC2616). Possible entries are: **GET, HEAD, PUT, DELETE.**
- **Server** name of the destination.
- **Count** shows the number of connections.
- **Bytes from client / Bytes to client** indicates the amount of data sent/received by the client.
- **User Agent** displays the signature of the clients browser.
- **Content type** displays the sort of sent/received data.
- **Boxname** provides the name of the server where the Secure Web Proxy is running on.
- **HTTP status** as retrieved from the destination (according to Status Code Definitions in RFC2616).
- **User / Group displays**, if configured, the group authentication scheme the requesting client resides in.

### 2.5.1.1 Access Context Menu

- **Show Details ...** - This entry opens an additional window providing detailed information concerning the selected entry (alternatively, this view is also available by double clicking on an entry).
- **Flush Cache** - removes either the selected entry (option **Entry**) or the complete access cache (option **-ALL-**)
- **Ungroup** - Removes the sorting selected below.
- **Group by** - Via this entry you may sort the tickets for column wise.
- **Show time in UTC** - switches the time format within the **Time** columns.

### 2.5.2 Tickets Tab

In this tab incident tickets can be viewed or deleted or their status can be changed.

By clicking **Update List**, all incident tickets will be retrieved from the server.

Clicking **Lock** activates a lock required for editing the database. Once all changes have been made, click the same button (which has now been renamed to **Unlock**) to release the lock.

**Note:**

User permission is required to edit incident tickets. For more information, **phion management centre** - 8. MC Admins, page 432.

### 2.5.2.1 Tickets Context Menu

**Show Details ...** - This entry opens an additional window providing detailed information concerning the selected ticket (alternatively, this view is also available by double clicking on a ticket).

**Ungroup** - Removes the sorting selected below.

**Group by** - Via this entry you may sort the tickets for ID, Server, Action or Type

**Set Action** allows the user to modify the status of an incident ticket. The following commands are possible:

- **Blacklist/Whitelist/Tunnel** - Blacklist, whitelist or tunnel connections to a server. For more details, see 2.4.1.3 SSL Exceptions, page 339.
- **Block** - Has almost the same status as blacklist except that the user can override the blacklist by enabling parameter **Allow Visit After Confirm** (see 2.4.1.2 SSL Certificates, List 12-22 Secure Web Proxy - SSL Certificates - section Certificate Verification, page 338).
- **Delete** - Deletes the incident ticket.

**Note:**

It is possible to make exceptions to the configuration (see 2.4.1.3 SSL Exceptions, page 339). Exceptions are also listed with the incident tickets, however - unlike regular incident tickets - it is not possible to edit or delete them.

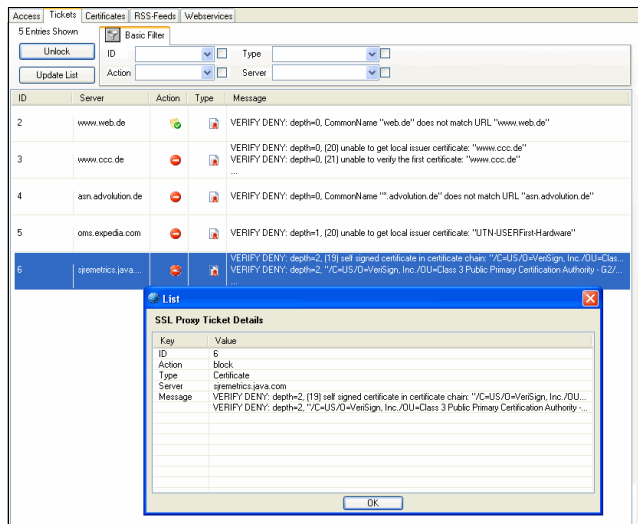
### 2.5.3 Certificates Tab

All known CAs (or instances of trusted servers issuing valid certificates) are displayed in this tab. Certificates can be deleted, denied or unconditionally allowed and certain attributes (like name, CRL, and OCSP-URL) can be changed.

**Note:**

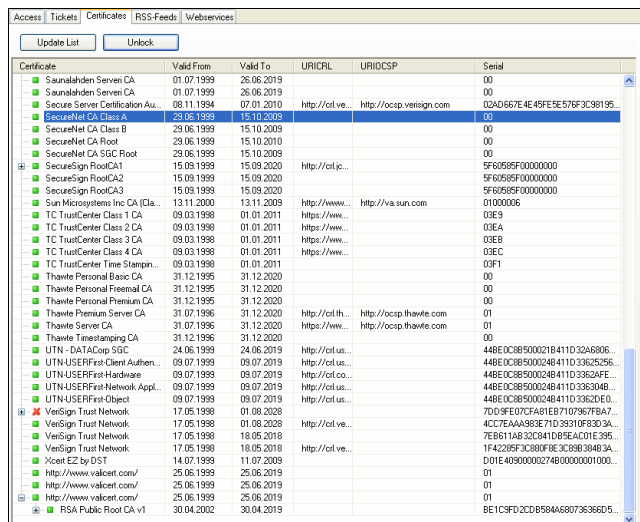
As with incident tickets, a user must have permission in order to make any changes to the CA tree.

Fig. 12-15 Secure Web Proxy GUI - Tickets tab with detail info



View details of an incident ticket by double clicking on the entry. Make changes using the context menu.

Fig. 12-16 Secure Web Proxy GUI - Certificates tab



The **Update List** and **Lock** buttons work just the same as in the **Tickets** tab.

A green square (■) in front of a CA signifies that any certificates issued by this CA will be allowed.

A red "X" (✘) in front of a CA signifies that any certificates issued by this CA will be denied.

### 2.5.3.1 Certificates Context Menu

The following commands are available over the context menu:

- **Show certificate** - Retrieves a certificate from the server and displays it as a standard certificate dialogue.
- **Edit Name** - Alter a CAs name. The CA name is for purposes of this list only and is not used for any other purpose.
- **Edit URICRL/URI OCSP** - Change URL of CRL and OCSP queries. Usually, it is not necessary to edit these attributes. They should already be correct.
- **Set Allow/Set Deny** - Manually allow or deny a CA (see above).
- **Delete CA** - Permanently removes a CA from the list. This action should only be taken by someone who knows exactly what he is doing.

**Note:**

New CAs will occasionally appear on this list as they become known to the system and are downloaded from the Internet. Initially, they will be denied. Therefore, it is recommended to check the CA tree regularly for new additions and, if necessary, change their status.

## 2.5.4 RSS-Feeds Tab

Here the handling of RSS feeds can be viewed (and edited).

### 2.5.4.1 RSS-Feeds Context Menu

The context menu is identical with the one described in 2.5.2.1 Tickets Context Menu, page 340.

## 2.5.5 Webservices Tab

The information provided in this tab is split into following columns:

- **URL** - displays the destinations URL.
- **Action** - defines the global way the connection is handled (either **Pass**, **Scan**, **Block**, or **Delete**). By opening the detail information you may set the action that is to be taken for each webservice method. However, it is not possible to delete webservice methods.
- **Subtype** - displays webservice type and version.
- **Count** - displays the number of established connections.

### 2.5.5.1 Webservices Context Menu

The context menu is identical with the one described in 2.5.2.1 Tickets Context Menu, page 340.

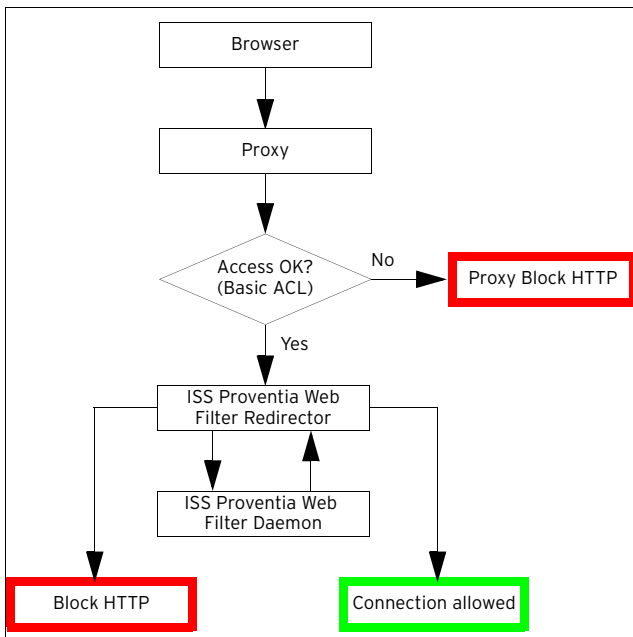
## 3. ISS Proventia Web Filter

### 3.1 General

The Proventia Web Filter, a content filtering utility, may optionally be implemented into the netfence HTTP Proxy, thus enabling access restriction to sites agreeable to the company policy.

When the filter is embedded, traffic is processed in the following succession:

Fig. 12-17 Overview: URL filtering process



#### Step 1 Proxy - Basic ACL

The request committed by a client's browser is first processed by the HTTP Proxy, where it has to pass Basic ACL configuration. If Basic ACLs do not allow browsing the Internet, the request will be dismissed by displaying the proxy server's internal block HTTP page.

##### Note:

For information on Basic ACLs, refer to 1.2 Configuration, Section Access Control - Proxy Access Handling Scheme, page 328.

#### Step 2 Proventia Web Filter Redirector

The redirector pipes the URL request into the internal checking routines (black lists, white lists, ...). When the requested URL can be verified in one of these internal categories/lists, the requester is allowed access to it, if not the request is handed over to the Proventia Web Filter Daemon (cofsd).

#### Step 3 Proventia Web Filter Daemon

The cofsd-daemon first attempts to find the requested page in the local cache. If it cannot find it there it establishes a connection to the Proventia Web Filter Database in order to retrieve an already assigned categorisation. It then either hands the local or external search result back to the redirector. The process responsible for this procedure can be viewed in the **Processes** tab of the **Control** section of phion.a and is named <servername>\_cofsd.

##### Note:

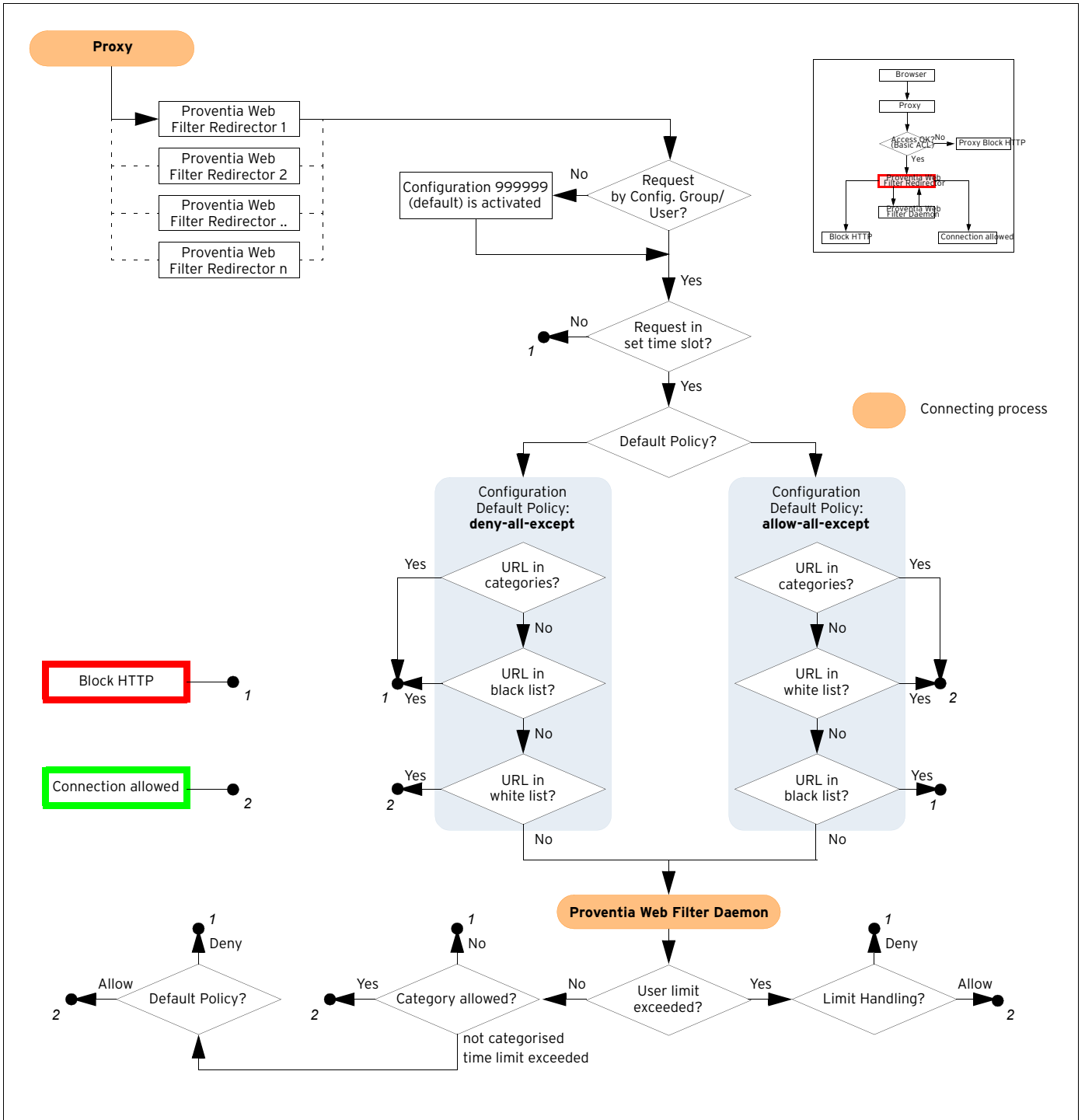
A few requirements have to be met, to enable the Proventia Web Filter to query the Web Filter Database in the Internet. See 3.3.1 Configuring Proventia Web Filter Redirectors, page 344 for configuration details.

#### Step 4 Proventia Web Filter Redirector

The redirector processes the search result by matching the URL categorisation with its internal settings. Access to the URL is then granted or denied in compliance with the specified policy.

Figure 12-18 illustrates the processes performed in Step 3 and Step 4 of the URL filtering process in detail:

Fig. 12-18 Flowchart - Proventia Web Filter Redirector & Daemon



## 3.2 Installation

To install the Proventia Web Filter, follow the instructions in **Configuration Service** - 4. Introducing a New Service, page 97, and select *ISSProventiaWebFilter* as **Software Module**.

### Note:

The Proventia Web Filter service binds to localhost and thus cannot be equipped with an individual **Bind Type**.

## 3.3 Configuration

The configuration of the Proventia Web Filter is subdivided into the following three configuration areas:

- **Proventia Web Filter Redirectors**  
(see 3.3.1 Configuring Proventia Web Filter Redirectors, page 344)
- **Proventia Web Filter Daemon**  
(see 3.3.2 Configuration of the Proventia Web Filter Daemon, page 344)
- **Proventia Web Filter - Redirector Parameters**  
(see 3.3.3 Configuring of IIS Proventia Web Filter - Redirector Parameters, page 345)

### 3.3.1 Configuring Proventia Web Filter Redirectors

Redirector configuration is part of the HTTP Proxy configuration (see 1.2.4.3 Section Redirector Settings, page 335).

Browse to **Config** > **Box** > **Virtual Servers** > **<servername>** > **Assigned Services** > **<servicename> (proxy)** > **HTTP Proxy Settings** > **Content Inspection** view > **Redirector Settings** section, to access the configuration area. The following values are available for configuration:

List 12-25 Proxy Service Parameters - section Redirector Settings

Parameter	Description
<b>Enable Redirector</b>	Set to <i>ISS-Proventia-Web-Filter</i> (default: <b>None</b> ) to enable the Proventia Web Filter. Optionally, select the <b>Other</b> checkbox and insert the name of an external redirector into the field, to implement another URL filtering tool.
<b>Firewall login</b>	Set this parameter to <b>Yes</b> (default: <b>No</b> ) if proxy authenticated users additionally have to authenticate themselves on the firewall. The proxy server will then forward the user login to the firewall. <b>Note:</b> This option will only work with usage of an User Authentication Scheme (see 1.2.3.1 Section Authentication, page 327). Please review User Authentication, page 330 if you want to define ACL Entries using ACL Type "proxyauthentication" explicitly.
<b>Number of Redirectors</b>	This parameter determines the number of simultaneously working redirectors (default: <b>5</b> ). The value may be increased for high traffic processing.

### 3.3.2 Configuration of the Proventia Web Filter Daemon

The Proventia Web Filter Service configuration area defines general service settings and allows specifying login values, if the Proventia Internet Databases have to be accessed through a proxy server.

Browse to **Config** > **Box** > **Virtual Servers** > **<servername>** > **Assigned Services** > **<servicename> (cofs)** > **ISS Proventia Web Filter Service** to access the configuration dialogue. The following values are available for configuration:

#### 3.3.2.1 General

List 12-26 IIS Proventia Web Filter Configuration - General - section ISS Proventia General Settings

Parameter	Description
<b>Max ISS Proventia processes</b>	This parameter defines how many Proventia processes may be started simultaneously at a maximum (figure 12-17, page 342).

List 12-27 IIS Proventia Web Filter Configuration - General - section ISS Proventia Database Settings

Parameter	Description
<b>Use local database</b>	Select this checkbox to enable usage of a local categorisation database. This setting is recommended on boxes with poor network connectivity to the central ISS database servers or for installations serving more than 100 concurrent web users. Querying a local database improves responsiveness of the filter. An initial database download is triggered when this option is enabled (approximate download size: 160 MB). <b>Attention:</b> On flash RAM based appliances the local database support cannot be used and has to be deactivated.
<b>Upload Unknown URLs</b>	Select this checkbox to activate collection of unknown URLs and their successive upload to an ISS server. Using this feature may contribute to evaluation of not yet categorised URLs.

List 12-28 IIS Proventia Web Filter Configuration - General - section ISS Proventia Support Options

Parameter	Description
<b>Log Categories per URL</b>	Selecting this checkbox extends Proventia log files (see 3.5 Logging, Cofsd (created by the Proventia Web Filter daemon), page 348) by adding the category classification to each requested URL. This option should only be used to assist in case of problems. Check for sufficient disk capacity before enabling it.

#### 3.3.2.2 Proxy

List 12-29 IIS Proventia Web Filter Configuration - section ISS Proventia Proxy

Parameter	Description
<b>Enable Proxy</b>	Select this checkbox if the Proventia Web Filter has to access the Proventia Internet Databases through the local proxy server. <b>Note:</b> See 3.3.4 Adapting the Local Firewall Rule Set, page 347 for a summary of access demands.
<b>Proxy Host / Port / User / Password</b>	Specify the authentication data requested by the local proxy server in this place.



### 3.3.3 Configuring of IIS Proventia Web Filter - Redirector Parameters

This section allows specification of the Proventia Web Filter's functional details, such as individual categorisation definitions, logging and statistics configuration.

Browse to **Config** > **Box** > **Virtual Servers** > <servername> > **Assigned Services** > <servicename> (**proxy**) > **ISS Proventia Web Filter Config** to access the configuration areas. The following values are available for configuration:

#### 3.3.3.1 Filter Settings

**List 12-30** IIS Proventia Web Filter Configuration - Filter Settings - section ISS Proventia Settings

Parameter	Description
<b>Timeout [s]</b>	This parameter specifies the maximum duration of a URL category research. If categorisation cannot be accomplished within this limit, the <b>Default Policy</b> (see below) determines, whether a request is granted.

**List 12-31** IIS Proventia Web Filter Configuration - Filter Settings - section Configurations

Parameter	Description
	<p>This section allows creating data sets with self contained settings for dedicated networks, user groups, or users. Data sets may be configured with explicit denial or allowance for strictly outlined time intervals. Each data set takes a number from 1 through 999998 as name. Data sets are processed in succession from lower to higher numbers, similar to a firewall rule set.</p> <p><b>Note:</b> The data set 999999 comprises the default setting including the default policy deny-all-except. The profile may be changed to allow-all-except policy and be modified, but it may not be deleted. When deleted it will be restored with the initial default settings and changes that have been made to it will get lost.</p> <p><b>Note:</b> The default data set applies to all <b>Networks/ Users/ Groups</b> accessing the Proventia Web Filter though, as the corresponding configuration fields are left empty, this seems not to be configured. In all further data sets complementing the default set at least one of the fields <b>Affected Networks/Affected Users/Affected Groups</b> has to be specified, otherwise the data set will have no validity. If values have been specified for all three fields, they will be linked with <b>OR</b>, and access to a requested URL will be granted or denied according to the default policy and on the basis of the first value applying.</p>
<b>Default Policy</b>	<p>The default policy defines the general proceeding with all following configuration values, which are defined within this data set. Available policies are:</p> <ul style="list-style-type: none"> <li>➤ <b>allow-all-except</b></li> <li>➤ <b>deny-all-except</b></li> </ul> <p><b>Note:</b> Check the <b>Timeout [s]</b> parameter (see above) to find out about the effect this setting has in case of categorisation failure.</p>
<b>Categories</b>	<p>This pull-down menu makes the category list provided by the Proventia Web Filter available. More than 60 million Web sites are part of the catalogue. Insert an arbitrary number of categories into the <b>Value</b> list by selecting a category and clicking the <b>Insert</b> button. Depending on the data set's <b>Default Policy</b> setting, access to the URLs contained in each category will be granted or denied.</p>







**List 12-31** IIS Proventia Web Filter Configuration - Filter Settings - section Configurations

Parameter	Description
<b>White List</b>	<p>The <b>White List</b> takes domain names, to which access shall always be granted, notwithstanding the domain's categorisation. Sub-domains are not included into the list automatically, but have to be specified explicitly instead.</p> <p>When the <b>Find String</b> checkbox is selected, the string inserted into the <b>White List</b> field is searched in any domain name.</p> <p><b>Note:</b> Do not specify the protocol identifier in white list entries (for example, write <code>www.domain.com</code> instead of <code>http://www.domain.com</code>).</p>
<b>Black List</b>	<p>The <b>Black List</b> takes domain names, to which access shall never be granted, notwithstanding the domain's categorisation. Sub-domains are not included into the list automatically but have to be specified explicitly instead.</p> <p>When the <b>Find String</b> checkbox is selected, the string inserted into the <b>White List</b> field is searched in any domain name.</p> <p><b>Note:</b> Do not specify the protocol identifier in white list entries (for example, write <code>www.domain.com</code> instead of <code>http://www.domain.com</code>).</p>
<b>Affected Networks</b>	<p>If settings within this data set should apply to specific networks accessing the proxy server, define these networks here.</p>
<b>Affected Groups / Users</b>	<p>If settings within this data set should apply to specific users or user groups accessing the proxy server, define these users or user groups here.</p> <p>The syntax of the user/user group entries depends on the used authentication method (see 1.2 Configuration, Section Authentication, page 327). The usage of pattern matching (via wildcards * and ?) is supported.</p> <p><b>Note:</b> Affected Groups and Affected Users may contain space characters. The inserted strings are treated case-insensitively (that means A-Z = a-z).</p> <p><b>Note:</b> If you are using <b>MSNT</b> or <b>RSAACE</b> as authentication method, the parameter <b>Affected Groups</b> will have no impact, because these methods do not provide group names.</p> <ul style="list-style-type: none"> <li>➤ <b>Radius:</b> Radius servers supply group names that have to be inserted exactly the way they are provided.</li> <li>➤ <b>LDAP, MSAD:</b> Both methods supply so-called distinguished names that have to be entered exactly the way they are provided (for example <code>CN=Group,OU=Unit,DC=Company,DC=com</code>).</li> </ul> <p><b>Note:</b> For information how to retrieve distinguished names, refer to <b>Appendix - 1.1</b> How to gather Group Information, page 524.</p> <p><b>Note:</b> In case group conditions are not matched correctly using an LDAP authentication scheme, verify that you have specified the <b>Group Attribute</b> field correctly (see page 113).</p> <p><b>Note:</b> If you encounter problems applying this filter due to incorrect user/group allocation, see <b>Netbios Domain Name</b>, page 112 for details on domain name assignment.</p>

**List 12-32** IIS Proventia Web Filter Configuration - Filter Settings - section TIME SETTINGS

Parameter	Description
	This section allows defining a number of time settings.
<b>Use Local Time checkbox/ Time Zone</b> pull-down menu	When the checkbox is selected, the data set's validity period is measured according to local box time settings. If you want another time zone to apply as calculation base, clear the checkbox and select the time zone from the pull-down menu.

**List 12-32** IIS Proventia Web Filter Configuration - Filter Settings - section TIME SETTINGS

Parameter	Description
<b>Time Settings</b>	Clicking the <b>Always</b> button opens the <b>Time Interval</b> configuration window, allowing for temporary activation/deactivation of the Proventia Web Filter with 1-hour-granularity on a weekly base. If time restriction applies to a profile, the label of the button changes to <b>Restricted!</b> . A profile is valid at all times by default, that means all checkboxes in the Time Interval dialogue window are unchecked. Checking a box deactivates a profile for the given time.
 Set allow	Select  to clear selected checkboxes.
 Set deny	Select  to select checkboxes as disallowed time intervals.
 Set Invert	Select  to configure allowed and disallowed time intervals simultaneously.
<b>Continue if mismatch</b>	Process the URL request even if the Proventia Web Filter is not available.
<b>Block if mismatch (default)</b>	Block the URL request when the Proventia Web Filter is not available.

### 3.3.3.2 Deny Message

**List 12-33** IIS Proventia Web Filter Configuration - section ISS Proventia Deny Message

Parameter	Description
<b>Message for Deny</b>	This parameter determines the message type displayed for connection denials. The message page can either be configured locally using a custom HTML text ( <b>Page</b> ) or be retrieved from an external HTTP server ( <b>URL</b> ). Depending on what has been chosen, either a <b>Deny Page</b> or a <b>Deny URL</b> has to be configured.
<b>Deny URL</b>	This field takes the URL of an external HTTP server capable of CGI used for display of customised block-pages in case of connection rejection. The URL of the message server (for example msgsrv) has to be specified including server protocol and IP address. Port specification is optional (like http://msgsrv.com:80). <b>Note:</b> For information concerning the use of external HTTP server, see 3.4.1 Communication with External HTTP Server, page 347.
<b>Deny Page</b>	This field takes an HTML page that is displayed via the internal firewall authentication daemon (fwauthd) when a connection request is rejected. <b>Note:</b> The reason for connection denial is contained in the \$\$MESSAGE\$\$ variable. Use this variable in the custom block-page to inform users about relevant security policy. <b>Note:</b> In case the Proventia Web Filter Daemon (cofsd) is not available, the user will still get informed why the connection was refused, if the URL request can be found in the internal categories/lists.

### 3.3.3.3 Exceptions

This tab allows configuring users who may bypass the Proventia Web Filter Redirector. Users may be identified either by their source IP address or by their user name.

**List 12-34** IIS Proventia Web Filter Configuration - section ISS Proventia Exceptions

Parameter	Description
	<b>Note:</b> Be sure to use the phion notation for the following two parameters. ( <b>Getting Started</b> - 5. phion Notation, page 25)

**List 12-34** IIS Proventia Web Filter Configuration - section ISS Proventia Exceptions

Parameter	Description
<b>Unrestricted IPs</b>	This parameter defines IP addresses whose URL requests are not going to be filtered. <b>Note:</b> The <b>Unrestricted IPs</b> involve IP addresses configured in the Access Control - Section ACL Entries 1.2.3.4 of the HTTP Proxy Server (ACL Type <b>source</b> , parameter <b>Source IP Config</b> (IP Ranges or Single IPs).
<b>Unrestricted Users</b>	Via this parameter you can enter users by using their proxy login. This is handy when your network works with DHCP. <b>Note:</b> The <b>Unrestricted Users</b> involve users configured in the Access Control - Section ACL Entries 1.2.3.4 of the HTTP Proxy Server (ACL Type <b>proxyauthentication</b> , parameter <b>User Authentication</b> (Users).

### 3.3.3.4 Cascaded Redirector

For inclusion of additional scanning procedures with third party software products installed on the phion netfence (for example virus scanning), the redirector may optionally be cascaded.

#### Note:

Use this functionality on your own responsibility.

**List 12-35** IIS Proventia Web Filter Configuration - section ISS Proventia Cascaded Redirector

Parameter	Description
<b>Cascaded is Primary</b> checkbox	Ticking this checkbox defines the cascaded redirector as primary component in the scanning chain. The URL request is then first routed through the additional scanner and then through the Proventia Web Filter.
<b>Cascaded Redirector</b>	This parameter defines the location (full pathname) of the cascaded redirector in the phion netfence.

### 3.3.3.5 Logging

#### Note:

Use the following parameters with care as they may produce huge log files.

**List 12-36** IIS Proventia Web Filter Configuration - section ISS Proventia Logging Settings

Parameter	Description
<b>Log Denied URL's</b>	Ticking this checkbox creates a log entry for each denied URL request.
<b>Log Allowed URL's</b>	Ticking this checkbox creates a log entry for each allowed URL request.

### 3.3.3.6 Statistics Tab

#### Section *ISS Proventia Statistics Settings*

Selecting a checkbox within this section creates corresponding statistics for:

- **Unrestricted Users**
- **Unrestricted IPs**
- **Denied URLs per User**
- **Denied URLs per IP** (selected by default)
- **Allowed URLs per User**
- **Allowed URLs per IP**

The generated statistics data pays regard to the following:

- URL distribution over the available categories.
- Usage distribution of categories per user.

### 3.3.3.7 Limit Handling

List 12-37 IIS Proventia Web Filter Configuration - section ISS Proventia Limit Handling

Parameter	Description
<b>Block If User Limit Exceeded</b>	When selected (default), the Proventia Web Filter blocks URL requests, when the license dependent Proventia Web Filter user limit is exceeded.

### 3.3.4 Adapting the Local Firewall Rule Set

The Proventia Web Filter Database first attempts categorisation of URL requests through its local settings and cache. If the requested URL cannot be retrieved in these places, it attempts accessing the Proventia Web Filter Databases in the Internet. This access has to be enabled by meeting the following requirements:

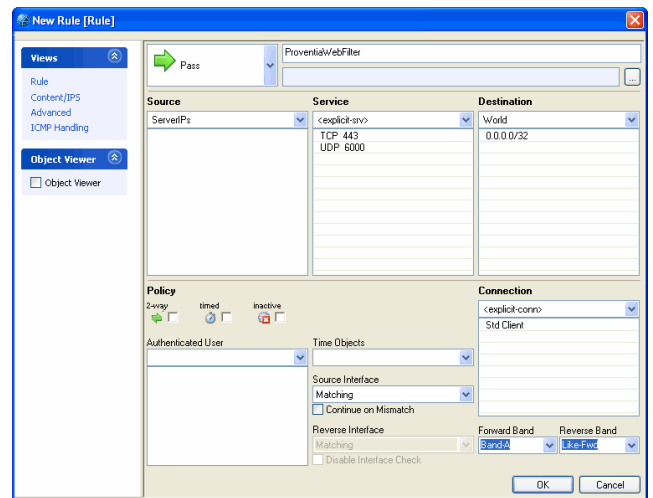
- From the netfence gateway the Proventia Web Filter Daemon is running on check, if the address `license.cobion.com` is DNS-resolvable. The daemon has to contact the license server for license verification through `https://license.cobion.com`. TCP port 443 has to be enabled on the firewall.
- Access to the the Proventia Internet Databases for URL categorisation running on the IP addresses 195.127.173.135 and 195.127.173.136 has to be enabled on TCP port 6000.
- From the netfence gateway the Proventia Web Filter Daemon is running on, the pointer (PTR) records of the addresses 195.127.173.135 and 195.127.173.136 have to be recallable.

Introduce a rule in the **Outbound-User** tab of the local rule set with the following setting parameters

- **Source** *ServerIPs*
- **Action** *Pass*
- **Destination** *World*

- **Service** *Explicit* with *006 TCP*, Port *443* and *006 TCP*, Port *6000*

Fig. 12-19 Local rule granting access from Proventia Web Filter to Proventia Internet Databases



#### Attention:

When using flash RAM based appliances, pay special attention to correct rule configuration in order to guarantee for uninterrupted Internet connectivity. If the Proventia Web Filter Daemon is unable to access the license server it will attempt to write to disk, which might lead to hardware malfunctions.

On flash RAM based appliances, configure Internet access before enabling the Proventia Web Filter Daemon.

## 3.4 Communication & Categories

### 3.4.1 Communication with External HTTP Server

#### Note:

The external HTTP server has to act as Common Gateway Interface (CGI).

The block-page on the external HTTP server has to be designed as HTML page, including a parameter line that is processed through the CGI with all parameters desired for explaining the reason for connection rejection.

The following parameters can be processed in a block-page:

- `categories=[1-63],99`  
indicating the categories that caused the block; category 99 marks a not found one; see 3.4.2 Proventia URL Categories, page 348, for a list of available categories.
- other reasons
  - `urlfd_not_running`  
The URL Filter Daemon is not running
  - `urlfd_read_error`  
Could not read from URL Filter Daemon
  - `no_more_memory`  
Machine is running out of memory

- `udp_not_received`  
Could not receive an answer for the requested URL.  
Please try later ...
  - `filter_timeout`  
Could not receive an answer for the requested URL.  
Please try later ...
  - `request_not_correct`  
The proxy has sent an incorrect request
  - `black_list`  
This site is on the **BLACK LIST**
  - `no_category`  
This domain is in no category
  - `timestamp_not_active`  
Sorry, but at this time the access is blocked
  - `user_limit_exceeded`  
Sorry, but the Proventia Web Filter user limit exceeded
- `url=www.[url].com`

A parameter line included in a custom block-page can look as follows (www.msgsrv.com is the external HTTP-server displaying the customised block-page):

```
www.msgsrv.com/block_page?filter_timeout&url=
www.forbidden.com
www.msgsrv.com.com/block_page?categories=1,6
,35&url=
www.forbidden.com
```

### 3.4.2 Proventia URL Categories

#### Note:

The following list is provided by Proventia.




Table 12-5 URL categories overview



Category	Description
01	Pornography
02	Erotic/Sex
03	Swimwear/Lingerie
04	Online_Shopping
05	Auctions/Classified_Ads
06	Governmental_Organizations
07	Non_Governmental_Organizations
08	Cities/Regions/Countries
09	Education
10	Political_Parties
11	Religion
12	Sects
13	Illegal_Activities
14	Computer_Crime
15	Hate/Discrimination
16	Warez/Hacking/Illegal_Software
17	Extreme
18	Gambling
19	Computer_Games
20	Toys

Table 12-5 URL categories overview

Category	Description
21	Cinema/Television
22	Recreational_Facilities/Amusement/Theme_Parks
23	Art/Museums
24	Music
25	Literature/Books
26	Humour/Comics
27	General_News/Newspapers/Magazines
28	Web_Mail
29	Chat
30	Newsgroups/Bulletin_Boards/General_Discussion_Sites
31	SMS/Mobile_Phone_Accessories
32	Digital_Postcards
33	Search_Engines/Web_Catalogs/Portals
34	Software_and_Hardware_Vendors/Distributors
35	Web_Hosting/Broadband
36	IT-Security
37	Translation
38	Anonymous_Proxies
39	Illegal_Drugs
40	Alcohol
41	Tobacco
42	Self-Help/Addiction
43	Dating/Relationships
44	Restaurants/Bars
45	Travel
46	Fashion/Cosmetics/Jewelry
47	Sports
48	Building/Residence/Architecture/Furniture
49	Nature/Environment
50	Private_Homepages
51	Job_Search
52	Investment_Brokers/Stocks
53	Financial_Services/Investment
54	Banking/Home_Banking
55	Vehicles/Transportation
56	Weapons
57	Health/Recreation/Nutrition
58	Abortion
60	Spam_URLs
61	Malware
62	Phishing_URLs
63	Instant_Messaging

## 3.5 Logging

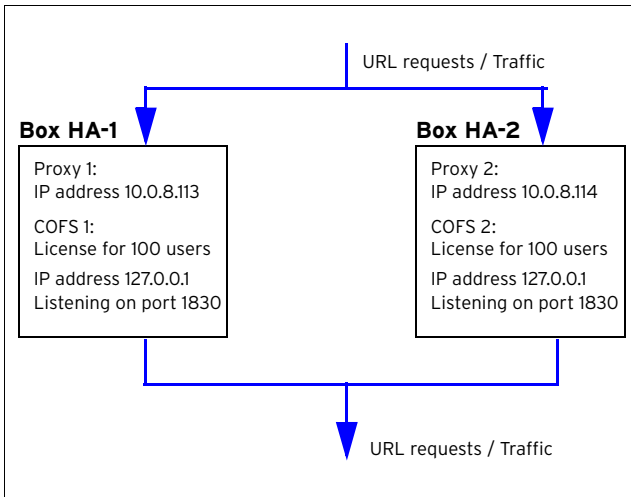
Activities, which are processed through the Proventia Web Filter, generate two log files. These log files can be viewed in the Log GUI of the graphical administration tool phion.a via  **Logs** >  <servername> >  <servicename> >

-  **Cofsd** (created by the Proventia Web Filter daemon)
-  **Fwauthd** (created by the firewall authentication client processing the "block-page").

### 3.6 Load Sharing and High Availability

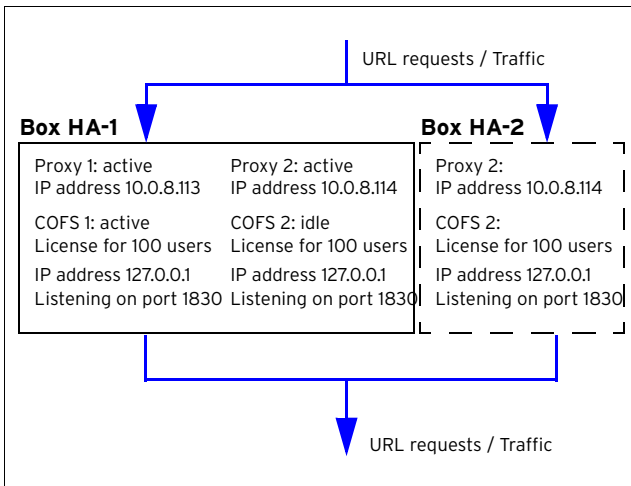
If a HA pair of netfence gateways is available it may be useful to install a second Proventia Web Filter on the second gateway to share the load and to take benefit of the available hardware. A second Proventia Web Filter license is required for this scenario.

Fig. 12-20 Principle of Load Sharing



In case Box HA-2 is down (for example because of a hardware failure), Box HA-1 takes over the Proxy server and Proventia Web Filter server that were hosted by Box HA-2.

Fig. 12-21 Principle of High Availability



**Note:**

Although both servers are displayed as active in the control view of phion.a, the second Proventia Web Filter server is idle. This inevitably happens because Proventia Web Filter servers bind to the localhost IP 127.0.0.1, and the second server will not be able to bind to an IP, which is already in use by another server (a corresponding log entry will be created in the log file *Cofsd*, see 3.5 Logging, page 348).

This behaviour is necessary to avoid fraud with multiple Proventia Web Filter servers using the same Proventia license. The anti-fraud procedure as well causes that still only 100 users (number of users is depending on the Proventia licenses installed on the now active box) are allowed at the same time.

**Note:**

Make sure that the parameter *Block If User Limit Exceeded* (page 347) is set properly.





# FTP Gateway

<b>1.</b>	<b>Overview</b>	
1.1	General .....	352
<b>2.</b>	<b>Installation</b>	
2.1	Create Service .....	352
<b>3.</b>	<b>Configuration</b>	
3.1	Service Properties .....	352
3.2	FTP-GW Settings .....	352
3.2.1	Settings .....	353
3.2.2	User specific .....	353
3.2.3	Authentication .....	354

# 1. Overview

## 1.1 General

The phion netfence FTP-gateway service is completely maintainable via the management console phion.a.

**Note:**

For detailed information on the file transfer protocol (FTP) see [www.w3.org/protocols/rfc959](http://www.w3.org/protocols/rfc959).

## 2. Installation

An installed box server is a pre-requisite to the installation of the FTP-Gateway service.

### 2.1 Create Service

Choose **Create Service** from the context menu of **Config** > **Box** > **Virtual Servers** > <servername>

## 3. Configuration

The configuration tree of the box provides all configuration options for the FTP-gateway service and contains the following items (listed according to their sequence of usage):

- **Service Properties**
- **FTP-GW Settings**, Page 352

**Note:**

Boxes maintained via a management centre (MC) can be configured locally only if an **Emergency Override** is performed (**Configuration Service** - 2.2.1.1 Box Context Menu, page 51).

### 3.1 Service Properties

Select the **Service Properties** item in the config tree to enter the configuration dialogue. Please consult **Configuration Service** - 4. Introducing a New Service, page 97 for a review of the configuration options.

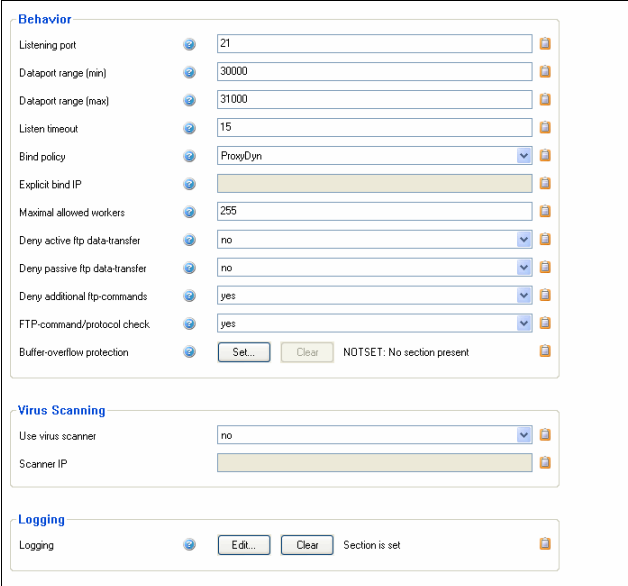
> **Assigned Services** and assign **FTP-Gateway** as software module to create a FTP-Gateway.

Activate the changes by clicking **Activate**. Your newly installed FTP-gateway service is now ready for configuration.

### 3.2 FTP-GW Settings

To enter the configuration, select the **FTP-GW Settings** entry in the configuration tree.

Fig. 13-1 FTP-GW Settings



Behavior	
Listening port	21
Dataport range (min)	30000
Dataport range (max)	31000
Listen timeout	15
Bind policy	ProxyDyn
Explicit bind IP	
Maximal allowed workers	255
Deny active ftp data-transfer	no
Deny passive ftp data-transfer	no
Deny additional ftp-commands	yes
FTP-command/protocol check	yes
Buffer-overflow protection	Set... Clear NOTSET: No section present
Virus Scanning	
Use virus scanner	no
Scanner IP	
Logging	
Logging	Edit... Clear Section is set

### 3.2.1 Settings

List 13-1 FTP-GW Settings configuration - section BEHAVIOR

Parameter	Description														
<b>Listening Port</b>	This parameter specifies the TCP port the gateway is listening on (default: <b>21</b> ).														
<b>Dataport range (min)</b>	Here the smallest possible allowed TCP port the gateway uses for data connections is defined (default: <b>30000</b> ).														
<b>Listen timeout (s)</b>	This timeout defines the maximum allowed duration for connection establishment (default: <b>15 seconds</b> ). If the timeout is exceeded the gateway terminates the attempt.														
<b>Bind policy</b>	Here the to-be-used Bind IP is defined. The available options are: <b>ProxyDyn</b> (default) - The bind IP is defined by the routing table. <b>Server-First</b> - The FTP gateway uses the first server IP for connections. <b>Server-Second</b> - The FTP gateway uses the second server IP for connections. <b>Explicit</b> - The FTP gateway uses an explicit IP for connections (to be defined below)														
<b>Explicit Bind IP</b>	Via this parameter the explicit IP to be used by the FTP gateway on connection has to be entered. Take into consideration that this parameter is only available if <b>Explicit</b> has been selected as parameter for <b>Bind policy</b> (see above).														
<b>Maximal allowed workers</b>	This parameter determines the number of processes that the gateway may fork (default: <b>255</b> ).														
<b>Deny active ftp-data transfer</b>	By setting this parameter to <b>yes</b> , any <code>port</code> command will be denied by the gateway (default: <b>no</b> ). This way only passive data transfer is possible, which means that the server connects to the client.														
<b>Deny passive ftp data-transfer</b>	By setting this parameter to <b>yes</b> , any <code>PASV</code> command will be denied by the gateway (default: <b>no</b> ). This way only active data transfer is possible, which means that the client connects to server.														
<b>Deny additional ftp- commands</b>	Setting this parameter to <b>no</b> allows additional FTP commands that are not included in RFC 959 (like status display in percentage) (default: <b>yes</b> ).														
<b>FTP-command/ protocol check</b>	If active this parameter (default: <b>yes</b> ) parses the protocol and checks FTP commands for correctness.														
<b>Buffer-overflow protection</b>	The button <b>Set</b> opens a new window with several parameters for buffer-overflow protection configuration which can be activated or deactivated. Each of the parameters controls two input fields: the first one activates or deactivates a length restriction (possible values <b>yes/no</b> ), the second one defines the length limitation if the first value has been set to <b>yes</b> . The following table displays the configured default settings:														
	<table border="1"> <thead> <tr> <th>Parameter group</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>(Max.) Filename Length</b> [default: yes / 255]</td> <td>This parameter affects the following commands: RETR, STOR, SMNT, APPE, RNFR, RNTD, DELE, RMD, MKD, LIST, NLST and STAT due to the fact that all of those commands may contain a parameter with file or directory name.</td> </tr> <tr> <td><b>(Max.) Username Length</b> [yes / 255]</td> <td>Length limitation for username (USER).</td> </tr> <tr> <td><b>(Max.) Account Info Length</b> [yes / 255]</td> <td>Length limitation for account (ACCT).</td> </tr> <tr> <td><b>(Max.) Password Length</b> [yes / 255]</td> <td>Length limitation for password (PASS).</td> </tr> <tr> <td><b>(Max.) String Length</b> [yes / 255]</td> <td>Limits the parameter length for commands REST, SITE and HELP.</td> </tr> <tr> <td><b>(Max.) Parameter Length</b> [yes / 255]</td> <td>Limits the parameter length for all other FTP commands.</td> </tr> </tbody> </table>	Parameter group	Description	<b>(Max.) Filename Length</b> [default: yes / 255]	This parameter affects the following commands: RETR, STOR, SMNT, APPE, RNFR, RNTD, DELE, RMD, MKD, LIST, NLST and STAT due to the fact that all of those commands may contain a parameter with file or directory name.	<b>(Max.) Username Length</b> [yes / 255]	Length limitation for username (USER).	<b>(Max.) Account Info Length</b> [yes / 255]	Length limitation for account (ACCT).	<b>(Max.) Password Length</b> [yes / 255]	Length limitation for password (PASS).	<b>(Max.) String Length</b> [yes / 255]	Limits the parameter length for commands REST, SITE and HELP.	<b>(Max.) Parameter Length</b> [yes / 255]	Limits the parameter length for all other FTP commands.
Parameter group	Description														
<b>(Max.) Filename Length</b> [default: yes / 255]	This parameter affects the following commands: RETR, STOR, SMNT, APPE, RNFR, RNTD, DELE, RMD, MKD, LIST, NLST and STAT due to the fact that all of those commands may contain a parameter with file or directory name.														
<b>(Max.) Username Length</b> [yes / 255]	Length limitation for username (USER).														
<b>(Max.) Account Info Length</b> [yes / 255]	Length limitation for account (ACCT).														
<b>(Max.) Password Length</b> [yes / 255]	Length limitation for password (PASS).														
<b>(Max.) String Length</b> [yes / 255]	Limits the parameter length for commands REST, SITE and HELP.														
<b>(Max.) Parameter Length</b> [yes / 255]	Limits the parameter length for all other FTP commands.														

List 13-2 FTP-GW Settings configuration - section Virus Scanning

Parameter	Description
<b>Use local virus scanner</b>	Set to <b>yes</b> (default: <b>no</b> ) to enable the virus scanning on files retrieved via FTP download. Virus scanning settings are configured in 2.5 FTP Gateway Integration, page 372.

List 13-3 FTP-GW Settings configuration - section Logging

Parameter	Description
	Click the <b>Show ...</b> button to start the configuration dialogue for logging settings. The following actions are logged by default. <b>Log download file</b> <b>Log upload file</b> <b>Log append file</b> <b>Log rename file</b> <b>Log delete file</b> <b>Log delete directory</b> <b>Log create directory</b> <b>Log other file-actions</b> <b>Log denied ftp-commands</b> <b>Log protocol denies</b> <b>Log logins</b> <b>Log succeeded local logins</b> <b>Log denied local logins</b> <b>Log destination denies</b> <b>Log file-upload denies</b> <b>Log file-download denies</b> <b>Log structure-mount denies</b> <b>Log delete file-denies</b> <b>Log rename-file denies</b> <b>Log change to upper dir denies</b> <b>Log extension denies</b> <b>Log create dir denies</b> <b>Log delete dir denies</b> <b>Log other ftp-commands</b>

### 3.2.2 User specific

#### User specific

Define different user profiles for FTP access here.

List 13-4 FTP-GW Settings Configuration - User specific - section Configuration Assignment

Parameter	Description
	As a matter of fact the processing sequence goes from up to down (similar to the firewall rule set). The sequence is defined by specification of the profile name (a profile number).
<b>Affected Groups</b>	Enter the groups here to which the profile and its restrictions apply.
<b>Affected Users</b>	Enter the users here to which the profile and its restrictions apply.
<b>Affected IPs for Anonymous</b>	Here you may assign IP addresses to the profile that need no authentication for accessing the FTP gateway (see 3.2.3 Authentication, page 354, parameter No local authorization needed, Page 354).

List 13-5 FTP-GW Settings Configuration - User specific - section Special Destinations

Parameter	Description
	Via the parameters of this section you are able to define restrictions for explicit FTP destinations (overruling the global configuration defined in FTP-GW Settings Configuration - User specific - section Default User Specific, Page 354).
<b>Destination</b>	Here the IP address or DNS-resolvable hostname of the FTP destination has to be entered.
<b>Redirection</b>	This parameter allows connection redirection to another host.
<b>Policy</b>	This parameter defines whether the destination is accessible for this user profile or not (default: <b>allow</b> ).
<b>Initial directory</b>	This parameter defines the "start" directory after login.
<b>Top most directory</b>	This parameter defines the highest possible directory level.
<b>Deny file-upload</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit file upload for this user profile.
<b>Deny file-download</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit file download for this user profile.

List 13-5 FTP-GW Settings Configuration - User specific - section Special Destinations

Parameter	Description
<b>Deny file-delete</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit file deletion for this user profile.
<b>Deny file-rename</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit renaming of a file for this user profile.
<b>Deny structure mount</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit a structure mount for this user profile.
<b>Deny make dir</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit directory creation for this user profile.
<b>Deny delete dir</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit directory deletion for this user profile.
<b>Deny file-extensions</b>	Define prohibited file extensions for this user profile. Enter only the extension itself without the leading dot. Separate multiple entries with space (like mp3 exe doc).
<b>Timeout (sec.)</b>	This parameter specifies the timeout after which an idle connection is terminated (default: <b>0</b> ).

List 13-6 FTP-GW Settings Configuration - User specific - section Default User Specific

Parameter	Description
	Via the parameters of this section you are able to define "global" restrictions for this user profile.
<b>Destination</b>	Here the IP address or DNS-resolvable hostname of the FTP destination has to be entered.
<b>Policy</b>	This parameter defines whether the FTP gateway is available to this user profile or not (default: <b>allow</b> ).
<b>Deny file-upload</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit file upload for this user profile.
<b>Deny file-download</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit file download for this user profile.
<b>Deny file-delete</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit file deletion for this user profile.
<b>Deny file-rename</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit renaming of a file for this user profile.
<b>Deny make dir</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit directory creation for this user profile.
<b>Deny delete dir</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit directory deletion for this user profile.
<b>Deny structure mount</b>	Set to <b>yes</b> (default: <b>no</b> ) to prohibit a structure mount for this user profile.
<b>Deny file-extensions</b>	Define prohibited file extensions for this user profile. Enter only the extension itself without the leading dot (for example mp3).
<b>Timeout (sec.)</b>	This parameter specifies the timeout after which an idle connection is terminated (default: <b>0</b> ).

List 13-7 FTP-GW Settings Configuration - User specific - section Time Restrictions

Parameter	Description
<b>Use Local Time checkbox</b>	Mark the checkbox to relate time restriction settings to the system's time zone settings. If unchecked, the parameter <b>Time Zone</b> below is activated to allow specific time zone configuration.
<b>Time Zone</b>	Choose a preconfigured time zone from the pull-down menu time restriction settings are meant to relate to.
<b>Time Settings</b>	The default policy allows all possible actions. By default, these profile settings as well are always valid. Activate checkboxes in the <b>Time Interval</b> window for periods a restriction should apply. During this period, all settings lose their validity.

### Default User specific

Via this section a profile is defined that is used if no other profile matches the request. The available parameters are nearly identical to the ones described above. An additional section **TIME RESTRICTIONS** allows limiting the default profile's validity period.

List 13-8 FTP-GW Settings Configuration - User specific - Default User Specific - section SPECIAL DESTINATIONS

Parameter	Description
	see list 13-5, page 353

List 13-9 FTP-GW Settings Configuration - User specific - Default User Specific - section OTHER DESTINATIONS

Parameter	Description
	see list 13-6

List 13-10 FTP-GW Settings Configuration - User specific - Default User Specific - section Time Restrictions

Parameter	Description
<b>Use Local Time checkbox</b>	Mark the checkbox to relate time restriction settings to the system's time zone settings. If unchecked, the parameter <b>Time Zone</b> below is activated to allow specific time zone configuration.
<b>Time Zone</b>	Choose a preconfigured time zone from the pull-down menu time restriction settings are meant to relate to.
<b>Time Settings</b>	The default policy allows all possible actions. By default, these profile settings as well are always valid. Activate checkboxes in the <b>Time Interval</b> window for periods a restriction should apply. During this period, all settings lose their validity.

## 3.2.3 Authentication

List 13-11 FTP-GW Settings Configuration - section Local Authentication

Parameter	Description
<b>Denied source-networks</b>	This parameter holds networks from where users are not allowed to connect.
<b>No local authorization needed</b>	IP addresses/networks that are entered in this parameter do not need to authenticate when connecting.
<b>Welcome message</b>	This parameter allows generation of welcome messages that are displayed when logging in. The configuration dialogue is opened when clicking <b>Edit ...</b>
<b>Phibs settings</b>	The parameters of this configuration dialogue (to be entered via button <b>Edit ...</b> ) allow definition of details concerning authentication: <b>PHIBS Authentication Scheme</b> This parameter defines what kind of authentication scheme is to be used. The following schemes are available: <b>MSNT</b> (default), <b>RADIUS</b> , <b>LDAP</b> , <b>MSAD</b> and <b>RSAACE</b> . <b>Note:</b> Take into consideration that authentication schemes MSNT and RSAACE do not provide group information.
<b>PHIBS Listen IP</b>	(default: <b>127.0.0.1</b> )
<b>PHIBS Timeout</b>	(default: <b>10</b> )
<b>User List Policy</b>	This parameter defines the policy for users that are entered in the user list (see below). The following settings are available: <b>deny-explicit</b> (default) <b>allow-only</b>
<b>User List</b>	This section is used for entering the login names for which access is granted.

# Voice over IP

<b>1.</b>	<b>Overview</b>	
1.1	General .....	356
<b>2.</b>	<b>SCCP</b>	
2.1	General .....	356
2.2	Installing SCCP .....	356
<b>3.</b>	<b>H.323 Neighbour Gatekeeper</b>	
3.1	General .....	358
3.2	Configuration .....	359
<b>4.</b>	<b>SIP</b>	
4.1	General .....	360
4.2	SIP-related Parameters .....	360
4.2.1	Firewall Settings .....	360
4.2.2	Firewall Forwarding Settings .....	360
4.3	Installing SIP .....	360
<b>5.</b>	<b>Monitoring</b>	
5.1	Dynamic Services .....	362

# 1. Overview

## 1.1 General

Currently netfence gateways (version 2.4.2 SP1 and higher) support three different types of Voice over Internet Protocols (VoIP):

- **Skinny Client Control Protocol** (also known as SCCP by Cisco)
- **H.323**
- **SIP**

# 2. SCCP

## 2.1 General

Cisco Skinny NAT and firewall traversal is implemented by a firewall plugin. The plugin monitors the skinny signalling connection between the phone and the Cisco callmanager. The default signalling port for SCCP is TCP 2000. When the plugin intercepts a Skinny packet that establishes a RTP connection like an audio transmission for VoIP a pinhole for the voice stream in the firewall will be opened. A call release packet or the termination of the skinny signalling connection closes the pinhole in the firewall.

## 2.2 Installing SCCP

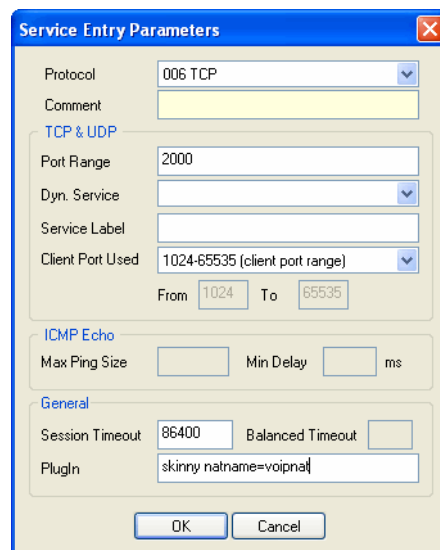
### Step 1 Create service objects for signalling and streaming purpose

For information concerning service objects, **Firewall - 2.2.5 Services Objects**, page 143).

The skinny plugin has two optional parameters which can be entered in the Plugin field:

- `natname`  
is a reference to a Address Translation Map in the Connections tab in the firewall rule set (syntax: `skinny natname=<natname>`, figure 14-1) and handles the signalling (protocol: TCP, port: 2000).

**Fig. 14-1** Provisioning the plugin in a service object for the SCCP signalling



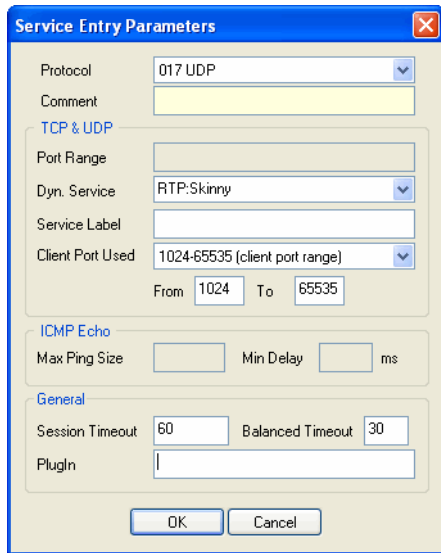
#### Note:

If this option is not specified then the default value RTP:Skinny (see below) is used instead. No address translation is performed for the RTP media streams if there is no matching entry in Connections.



➤ `srvname` is a reference to a **Dyn. Service** label that data fills a service object with the data stream of skinny calls (syntax: `skinny [srvname=<srvname>](protocol: UDP)`). The service object can be referenced by a firewall rule in order to forward the media streams between the call participants. The default value of `srvname` is `RTP:Skinny`.

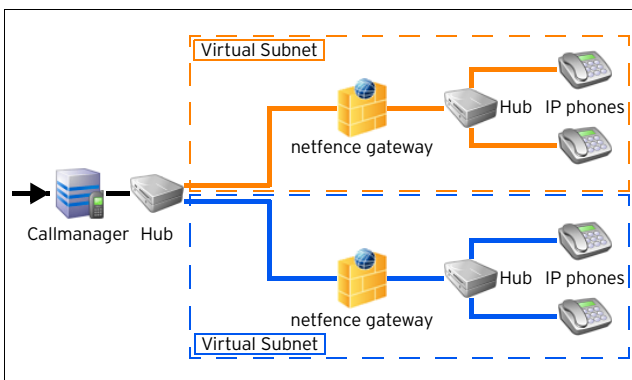
**Fig. 14-2** RTP Stream service object with the default service name set to RTP:Skinny



**Step 2 Create translation map (optional)**

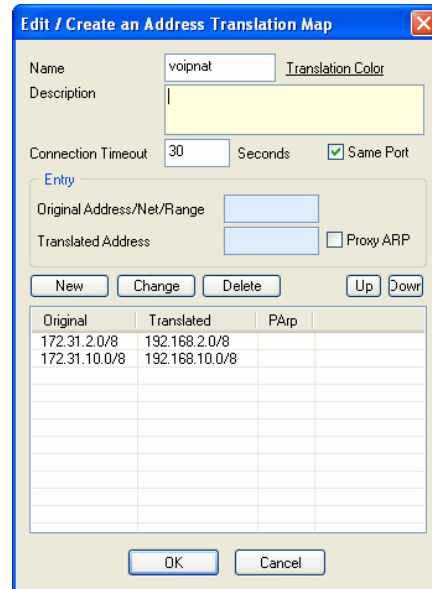
If network address translation is done between caller and callee an address translation map has to be defined, translating the real IP address of the participants to virtual addresses that are routable for all nodes in the Voice over IP network (for information concerning translation maps, see **Firewall - 2.2.6.3 Translation Map**, page 149).

**Fig. 14-3** VoIP infrastructure with 2 virtual subnets



The name of the map must match the option of the **natname** parameter of the skinny firewall plugin configured above. The **Original Address/Net** is the physical IP subnet of a node whereas the **Translated Address/Net** is the virtual address.

**Fig. 14-4** Creating an Address Translation Map



In a call setup message the real address of the phone is translated to the virtual address.

As soon as the other participant of the call receives the modified call setup message it starts sending its voice stream to the virtual address of the peer. The firewall next to the receiver of the media stream re-translates the virtual IP address back to the real address of the participant.

The firewall rule required for proper address translation handling has to contain a reference to the service object with the RTP Dyn. Service label specified in the skinny plugin (see above).

The mapping rule action controls how the address mapping is performed. To use the same address map which is used by the skinny plugin, select the same map in the **Redirection** and **Source Translation** section.

If no address translation is required then the **Pass** firewall action is to be used.

Fig. 14-5 Skinny signal protocol firewall rule with Skinny firewall plugin

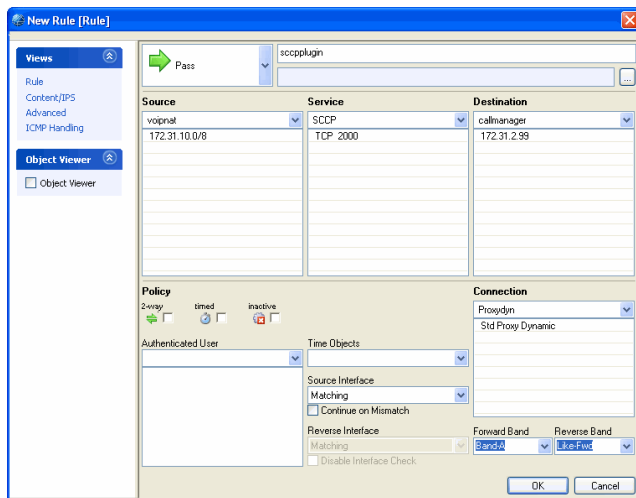
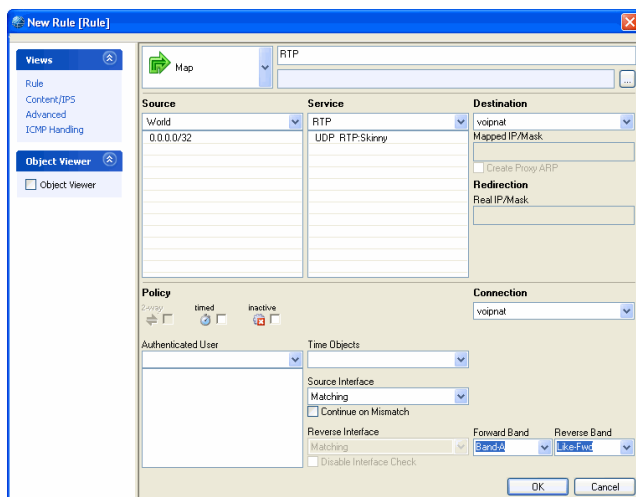


Fig. 14-6 RTP firewall rule with network address translation from the voipnat address translation map



## 3. H.323 Neighbour Gatekeeper

### 3.1 General

netfence gateways can be integrated as gatekeeper into a H.323 network. The media stream of the calls that are established by the firewall gatekeeper are redirected to a local address of the netfence and forwarded to the receiver of the stream. Special handling for network address translation or firewall traversal is not required.

The H.323 endpoints that are in direct contact with the gatekeeper can be registered with H.225 RAS, or can be provisioned in the firewall configuration. Several gatekeepers can be clustered together to handle calls for endpoints with the same prefix, which are distributed over several locations. This is called the neighbour configuration.

The following gatekeepers are allowed in neighbour configurations:

- **Gnu** Gatekeeper
- **Cisco** Gatekeeper
- **Clarent** Gatekeeper
- **Glonet** Gatekeeper

### 3.2 Configuration

H.323 is configured within the **Firewall Forwarding Settings** ( **Config** > **Box** > **Virtual Servers** > **<servername>** > **firewall** ).

Fig. 14-7 Firewall Forwarding Settings - H.323 Gatekeeper Configuration dialogue

List 14-1 Firewall Forwarding Settings - H.323 Gatekeeper tab

Parameter	Description
<b>Enable H.323 Gatekeeper</b>	Starts the firewall gatekeeper if set to yes. <b>Note:</b> In order to allow communication of the H.323 equipment with the netfence gatekeeper you have to add rules to the local firewall. We recommend to allow all incoming and outgoing UDP and TCP ip ports from the networks with H.323 nodes that are directly communicating with the netfence gatekeeper.
<b>Gatekeeper Name</b>	This is the H.323 alias name of the firewall gatekeeper.
<b>Gatekeeper Bind IP</b>	Determines whether the gatekeeper binds on first or second IP of the server or if the gatekeeper should bind all local IPs of the host. An explicit IP can also be entered by ticking the <b>Other</b> checkbox.
<b>Broadcast RAS</b>	Enable the sending of H.225 broadcast gatekeeper discovery packets. This is useful for phones that autodetect the gatekeeper.
<b>Gatekeeper Password</b>	The password that must be specified by the neighbour gatekeepers to logon to the firewall gatekeeper for allowing neighbour cluster calls.

List 14-1 Firewall Forwarding Settings - H.323 Gatekeeper tab

Parameter	Description	
<b>H.323 Neighbors</b>	<b>Gatekeeper Name</b>	The H.323 alias of the neighbour gatekeeper.
	<b>Gatekeeper Type</b>	The vendor of the neighbour gatekeeper (GnuGK, CiscoGK, ClarentGK, GlonetGK).
	<b>Gatekeeper Hostname</b>	This is the hostname of the IP address of the neighbour gatekeeper.
	<b>Gatekeeper Port</b>	This is the H.225 port number of the neighbour gatekeeper.
<b>Gatekeeper Password</b>	The specified password is used to log into the neighbour gatekeeper for neighbour clustering support.	
<b>Neighbor Timeout (sec.)</b>	The timeout of LRQ (Location Request) messages for browsing the neighbor cluster.	
<b>H.323 Endpoints</b>	Endpoints that are permanently registered at the gatekeeper. This is useful for interfaces that do not support H.225 RAS.	
	<b>H.323 Alias</b>	H.323 alias of the permanent endpoint.
	<b>Gateway Hostname/IP</b>	Hostname or IP address of the endpoint. Endpoints with dynamic IPs must use H.225 registration to connect to the firewall gatekeeper.
	<b>Prefix</b>	All calls with this number or prefix are routed to this endpoint.
<b>Call Redirect</b>	<b>Original Prefix</b>	All calls with this prefix are rerouted.
	<b>New Prefix</b>	The Original Prefix is removed from the dialled number and replaced with the new prefix.
<b>RAS Authentication</b>	The following options are available: <b>None</b> allows all H.225 RRQ (Registration Requests). <b>Radius</b> registers the username at a radius server. <b>Radius+CAT</b> uses the Cisco Access Token in the RRQ message for registration at a radius server.	
<b>Radius Server</b>	IP address or hostname of the radius server. An optional port number may be specified after a colon (:). <hostname> [:<port>]	
<b>Radius Password</b>	The shared secret of the radius server.	
<b>Radius Server Timeout (millisec)</b>	If the server does not answer within the specified time period then the authentication fails.	
<b>Radius IDCache Timeout (millisec)</b>	Lifetime of the 8-bit request cache ID. After the timeout expires the cache ID of a request may be reused. If the timeout is too short, then the radius server may drop requests with the same cache ID.	
<b>Radius Server Transmission</b>	The number of tries of authentication requests that are sent to the radius server. The Radius Server Timeout determines the time intervals between the transmissions.	
<b>Radius with Terminal Alias</b>	Include Cisco h323-ivr-out attribute in the radius request.	
<b>Fixed Radius User / Fixed Radius Password</b>	If this option is used and the RAS Authentication is set to Radius then all registration requests will use the Fixed Radius User and Fixed Radius Password for registration at the radius server. If this field is left blank then the username is used as password.	

## 4. SIP

### 4.1 General

SIP firewall traversal and NAT is supported by the phion netfence firewall service plugin. The firewall decodes the SIP packets and opens and closes firewall pinholes for the voice media connections. Due to the dynamic nature of this protocol, a table of all active calls is held in memory. This table contains the negotiated media connections, the SIP transactions for the call signalling, and the calls. When a SIP packet passes the firewall, the state of the table is altered accordingly.





The SIP plugin supports SIP signalling over UDP/IP packets. The default port for SIP signalling connection is UDP port 5060.

**Note:**

For more information about the SIP Protocol see "RFC3261: SIP: Session Initiation Protocol".

### 4.2 SIP-related Parameters








#### 4.2.1 Firewall Settings

The size of the SIP call table is defined in  **Config** >  **Box** >  **Infrastructure Services** >  **General Firewall Configuration** > **Global Limits** > **Access Cache Settings** section.

**List 14-2** Box Firewall Settings - SIP Parameters - section Access Cache Settings

Parameter	Description
<b>Max. SIP Calls</b>	The maximum number of SIP calls is the number of concurrent calls that can be handled by the firewall (min: 64; max: 8192; default: 512). A new call is created when a SIP request is received by the firewall which contains a previously unknown call-ID. An existing call is discarded when all media connections of the call are closed or timed-out and no SIP transactions are associated with the call.
<b>Max. SIP Transaction</b>	A SIP transaction is started with a SIP request packet. In reply of a SIP request a SIP response packet is generated and sent to the address that was specified in the request. The lifetime of a SIP transaction does not end with the reception of a response message. Instead a timer is started that allows the SIP signalling endpoints to handle retransmissions of any SIP packets. The SIP transaction can be discarded after the timer has expired (min: 64; max: 8192; default: 512).
<b>Max. SIP Media</b>	The SIP Media (min: 64; max: 16384; default: 1024) defines a voice connection through the firewall. Usually 2 different media connections are used by a voice call. One media connection describes the path of the actual RTP voice packets while the other connection describes the RCTP connection for quality feedback and RTP signalling. The inactivity timeout of media connections can be configured in a firewall rule by setting the "Balanced Timeout" in the "Service Entry Parameters" window.

#### 4.2.2 Firewall Forwarding Settings

SIP transaction timeouts are defined in  **Config** >  **Box** >  **Virtual Servers** >  <servername> >  **Assigned Services** >  <servicename> (**firewall**) >  **Firewall Forwarding Settings** > **SIP**.

All timeout values are set in hundredth of seconds.

**List 14-3** Forwarding Firewall Settings - SIP Parameters

Parameter	Description
<b>INVITE Timeout (csec)</b>	The invite timeout is the timeout of an "INVITE" transaction. If a reply to this request is received after the invite timeout has expired then the reply is discarded. This value can also be set in the SIP service object by the "toInvite" plugin parameter (default: 3200).
<b>ACK Timeout (csec)</b>	The ACK timeout is the timeout of a replied or acknowledged "INVITE" transaction after the transaction is discarded. This value can also be set in the SIP service object by the "toAck" plugin parameter (default: 3200).
<b>Reply Timeout (csec)</b>	The reply timeout defines how long the firewall will wait for a reply of a non-invite transaction. This value can also be set in the SIP service object by the "toReply" plugin parameter (default: 400).
<b>Transaction Timeout (csec)</b>	The transaction timeout is the timeout of a replied non-invite transaction. This value can also be set in the SIP service object by the "toTrans" plugin parameter (default: 500).

### 4.3 Installing SIP

To enable the SIP firewall plugin create a firewall rule with a SIP enabled service object. When creating this service object set the **Protocol** to **017 UDP** and the Port Range to 5060. When your equipment uses different ports for the SIP protocol you have to enter these ports instead. Set the plugin field to **sip** to finish the **Service Entry Parameters** settings.

Here you can also set additional parameters for the SIP plugin by appending plugin parameters in a whitespace separated list:

➤ **toInvite**

for example "sip toInvite=3200"

sets the invite timeout to 32 seconds

See SIP Timeouts

➤ **toAck**

for example "sip toAck=3200"

sets the acknowledge timeout to 32 seconds

See SIP Timeouts

➤ **toReply**

for example "sip toReply=400"

sets the reply timeout to 4 seconds

See SIP Timeouts

➤ **toTrans**

for example "sip toTrans=500"

sets the transaction timeout to 5 seconds

See SIP Timeouts

➤ **nonat**

for example "sip nonat=1"  
disables network address translation handling for the sip plugin

➤ **srvname**

Example: "sip srvname=voip"  
set the service name for the RTP rule lookup to "RTP:voip"  
The default value is "RTP:SIP".

➤ **via**

Example: "sip via="SIP/2.0/UDP 172.31.10.5:5060""  
sets the target address for the SIP reply message to 172.31.10.5 UDP port 5060

This parameter enables rewriting of the "Via" SIP header field in outgoing SIP request messages. The default is not to rewrite the "Via" header if no NAT is performed. In NAT configurations the default is to use the bind address of the connection slot for the "Via" header. Any "Via" header field tags of the original message persist. This is valuable when using NAT for the SIP firewall rule to force the receiving SIP peer to send SIP reply messages to the address defined in the "via" plugin parameter. In its reply message the firewall rewrites the "Via" header field to the original field value from the request message. Usually the address in the "via" plugin parameter will point the SIP peer to a port on the firewall that is redirected to the internal SIP proxy. The value must be enclosed in double quotes.

➤  **fwdcontact**

Example:  
"sip fwdcontact="< sip:proxy@gateway.extern>""  
sets the contact address for sip messages in the forward direction of the firewall rule

This parameter enables rewriting of the "Contact" SIP header field of packets that are leaving the firewall in the forward rule direction (from source to target). This is useful for NAT setups in the outgoing rule to tell the SIP peer the target address for its SIP request messages. Usually the address in the "fwdcontact" plugin parameter will point the SIP peer to a port on the firewall that is redirected to the internal SIP proxy. The value must be enclosed in double quotes.

The default is not to rewrite the "Contact" header if no NAT is performed. In NAT configurations the default is to use the bind address of the connection slot for the "Contact" header.

➤ **revcontact**

Example:  
"sip revcontact="< sip:proxy@gateway.extern>""  
sets the contact address for sip messages in the reverse direction of the firewall rule

This parameter enables rewriting of the "Contact" SIP header field of packets that are leaving the firewall in the reverse rule direction (from target to source). This is useful for NAT setups in the incoming rule to tell the SIP peer the target address for its SIP request messages. Usually the address in the "revcontact" plugin parameter will point the SIP peer to a port on the firewall that is redirected to the internal SIP proxy.

The default is not to rewrite the "Contact" header if no NAT is performed. In NAT configurations the default is to use the destination address of the connection slot for the "Contact" header.

When the firewall plugin receives a complete SIP INVITE handshake for negotiating a RTP media session it makes a lookup in the firewall rule set. The lookup for the RTP rule is done for a dynamic service name of "RTP:SIP" or the value defined in the "srvname" SIP plugin parameter. No fixed ports are required for RTP rule. The media timeout value in this rule is defined by the "Balanced Timeout" parameter in the "Service Entry Parameters" Settings. Additional attributes like traffic shaping settings for the media connection can also be defined in this rule. If the matched rule allows the RTP connection then the call table is updated so that the media packets may pass.

The RTP rule should always have a connection type of "Client". NAT rewriting is based on the rule that matches the SIP signalling connection. If source or destination NAT is used in the SIP rule then SIP ties the media session to the outgoing or incoming IP addresses of the firewall and rewrites the media portion of the SIP messages accordingly. Then the firewall forwards the media packets to the endpoints of the call. The NAT rewriting behaviour can be disabled by setting the "nonat=1" plugin parameter.

When using NAT you define an incoming and outgoing rule for the SIP messages. The outgoing rule performs the source NAT and should use the parameters "via" and "fwdcontact" to tell the outside peer the right contact address on the firewall.

Example: "sip via="SIP/2.0/UDP 172.31.10.5:5060" fwdcontact="< sip:proxy@firewall.extern>""

The incoming rule redirects SIP packets to the internal proxy and should use the "revcontact" plugin parameter to tell the outside peer the right contact address on the firewall.

Example: "sip revcontact="< sip:proxy@firewall.extern>""

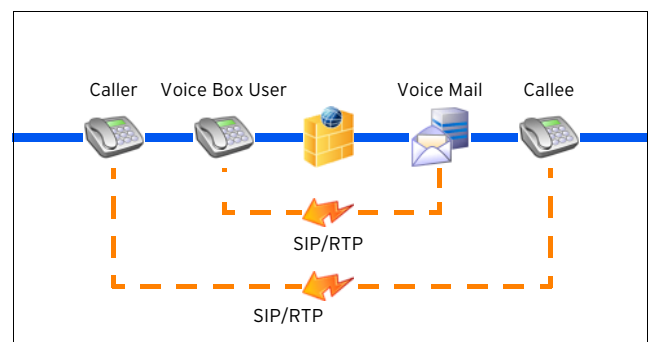
**Note:**

The firewall has no registrar functionality. Setups using NAT always have to use a SIP proxy in the net which gets translated. This proxy distributes incoming SIP messages to the appropriate SIP peers. The firewall rule set must be configured to forward SIP messages for peers in the translated net to the SIP proxy.

The state of the SIP signalling can be monitored in the firewall GUI in the **Dynamic** tab under **SIP**.

In network setups without NAT all SIP Peers may communicate directly. Ports for the RTP media streams are opened dynamically by the firewall and passed to the participants of the call.

**Fig. 14-8** Network setup without NAT - SIP/RTP



## 5. Monitoring

### 5.1 Dynamic Services

Monitoring takes place in the **Dynamic Services** tab of the **Firewall** box menu entry (tab **Dynamic**).

Clicking **Update List** refreshes the displayed information.

The following columns are in use:

**Table 14-1** SIP Monitoring parameters overview

Column	Description
	<b>first row</b> The first row gives an overview of all calls that have been executed. A call does not necessarily have to be a standard call, between active caller and callee. A phone registering with a central registrar will produce a call as well. In other words, every action producing a new Call-ID, which is then part of every SIP packet transmitted through the SIP protocol, is defined as call.
<b>Call-ID</b>	This ID is randomly generated through a caller's call.
<b>Start</b>	This is the duration of the call.
<b>Status</b>	The status column indicated the call's state. The following markers exist: <ul style="list-style-type: none"> <li>➤ <b>Init</b> - The call has just arrived.</li> <li>➤ <b>Setup</b> - Connection establishment is just taking place.</li> <li>➤ <b>Established</b> - The call has been established.</li> <li>➤ <b>Teardown</b> - The call is about being terminated.</li> <li>➤ <b>Terminated</b> - The call has been terminated.</li> </ul> <b>Note:</b> The call is not deleted from the table immediately after termination. It stays visible until no further media connections or SIP transactions related to it exist.
<b>SrvName</b>	This is the name of the Dynamic Service, which is used for RTP Rule lookup (default: RTP:SIP).
<b>SYNC</b>	not available
	<b>second row</b> The second row gives an overview of all RTP Media Connections (Audio/Video Data Streaming) and RTCP Connections (Quality Feedback and Media Signalling). Usage of RTCP is optional. If RTCP is not used during a media connection, the entry for RTCP connections vanishes after the Balanced Timeout of the service has expired. Medium and call are interconnected through the Call-ID.
<b>Call-ID</b>	This is the Call-ID belonging to this Media Connection. The Call-ID constitutes a chaining to the call, which is described through the first row.
<b>Start</b>	This is the duration of the call.
<b>Idle</b>	This is the idle time since the last data flow.
<b>Src-Addr</b>	This is the source address before address rewriting.
<b>Src-Port</b>	This is the source port before address rewriting.
<b>Dst-Addr</b>	This is the destination address before address rewriting.
<b>Dst-Port</b>	This is the destination port before address rewriting.
<b>Src-User</b>	This is the sender's account.
<b>Dst-User</b>	This is the receiver's account.
<b>Src-Addr-Used</b>	This is the source address after address rewriting.
<b>Src-Port-Used</b>	This is the source port after address rewriting.
<b>Dst-Addr-Used</b>	This is the destination address after address rewriting.
<b>Dst-Port-Used</b>	This is the destination port after address rewriting.



# SSH Gateway

<b>1.</b>	<b>SSH Proxy</b>	
1.1	Overview .....	364
1.2	Creating a SSH Proxy .....	364
1.3	Configuring a phion SSH Proxy .....	364
1.3.1	General .....	365
1.3.2	Authentication & Login .....	365
1.3.3	Default Permissions .....	366
1.3.4	Access Lists .....	366
1.3.5	Permission Profiles .....	366
1.3.6	User Authorization .....	366

# 1. SSH Proxy

## 1.1 Overview

phion's SSH Proxy allows regulating SSH connections.

Supported features:

- Based on openSSH 3.8p1 with phion proprietary modifications for the controlled termination of SSHv2 terminal access sessions
- No support for the termination of SSH protocol version 1
- No support for remote execution or secure copy or secure ftp
- No local user database required
- User authentication at the gateway via all configurable and meaningful authentication schemes (**not** OSCP) using a user/password combination.
- Access configurable based on groups (deny, allow)
- Support for public key authentication at target system due to configurable public key support and configurable agent forwarding
- Individual known\_hosts files for each user
- Optional HA synchronisation of known\_hosts files
- Optional session/activity tracing for certain users (console output cloning to file)
- Port is configurable
- DoS protection by configurable login grace time and maximum pending session limits
- Configurable client alive interval and interval count
- Configurable reverse DNS lookup behaviour of server for accessing clients
- Configurable login greeting text (banner text)
- Configurable server log level
- Compression on/off configurable
- Menu based user interface program for selection of IP-address/hostname, user, port for accessing the target system
- Separate inactivity timeout for user interface program
- Configurable number of maximum successive illegal inputs before user interface program terminates
- Configurable client log level (ssh-client)
- Configurable server alive interval and interval count

- Configurable local source IP (to use policy routing) for accessing remote systems
- Configurable SSH protocol support for accessing target systems (v2-only, or v2 and v1)
- Configurable escape character

### Note:

Parts of this document/description are taken from the manual pages of openSSH 3.8p1.

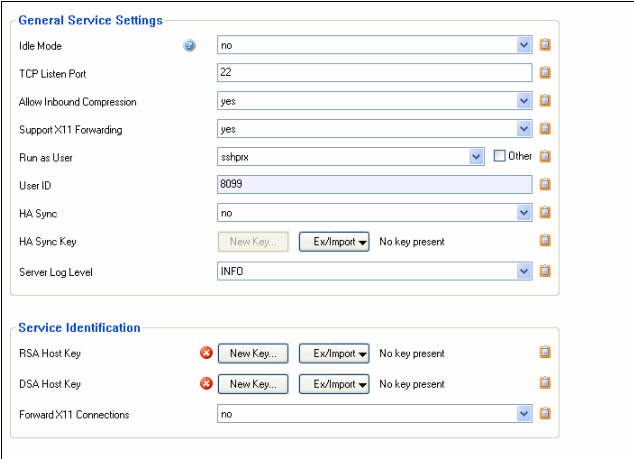
## 1.2 Creating a SSH Proxy

The SSH Proxy service is created as described in **Configuration Service - 4. Introducing a New Service**, page 97, and selecting **SSH-Proxy** as service module.

## 1.3 Configuring a phion SSH Proxy

Configuration of a SSH Proxy takes place in the **SSH Proxy** configuration dialogue (accessible through **Config > Box > Virtual Servers > <servername> > Assigned Services > <servicename>(sshprx)**).

Fig. 15-1 Configuration dialogue - SSH Proxy



The screenshot shows the configuration dialogue for the SSH Proxy service. It is divided into two main sections: 'General Service Settings' and 'Service Identification'.

**General Service Settings:**

- Idle Mode: no
- TCP Listen Port: 22
- Allow Inbound Compression: yes
- Support X11 Forwarding: yes
- Run as User: sshprx (Other checkbox is unchecked)
- User ID: 8099
- HA Sync: no
- HA Sync Key: New Key... Ex/Import No key present
- Server Log Level: INFO

**Service Identification:**

- RSA Host Key: New Key... Ex/Import No key present
- DSA Host Key: New Key... Ex/Import No key present
- Forward X11 Connections: no

### 1.3.1 General

List 15-1 SSH Proxy configuration - General - section General Service Settings

Parameter	Description
<b>Idle Mode</b>	This parameter activates/deactivates SSH proxying (default: <b>no</b> - active).
<b>TCP Listen Port</b>	Here the port the SSH Proxy is listening on has to be entered (default: <b>22</b> ).
<b>Allow Inbound Compression</b>	States whether or not data compression is supported by the server for incoming client connections. Within LAN environments using compression can create a significant CPU overhead and is typically not advisable.
<b>Support X11 Forwarding</b>	States whether or not X11 forwarding is supported by the service. If set to <b>no</b> X11 forwarding is not available regardless of any subsequent profile based settings.
<b>Run as User</b>	This parameter defines the user name that will be used when synchronising the log with the high available partner system. By default this parameter is set to system user sshprx. By ticking the checkbox Other (to the right) you may enter any other name.
<b>User ID</b>	Here the ID of the system user (parameter <b>Run as User</b> , see above) is defined. <b>Note:</b> The User ID is used as the HA sync port (default: 8099). If using a different User ID the local firewall rule set has to be changed. <b>Attention:</b> If multiple instances of the SSH proxy are run on the same box, you must choose a different user/user ID combination for each service.
<b>HA Sync</b>	Activating this parameter (default: <b>no</b> ) enable synchronisation between HA partners (SSL based with user/key).
<b>HA Sync Key</b>	Defines the key required for HA sync tasks.
<b>Server Log Level</b>	This parameter defines the intensity of log file creation.

List 15-2 SSH Proxy configuration - General - section Service Identification

Parameter	Description
<b>RSA Host Key</b>	Here the RSA host key for the server is created/imported/exported.
<b>DSA Host Key</b>	Here the DSA host key for the server is created/imported/exported.
<b>Forward X11 Connection</b>	States whether or not the proxy will forward X11 sessions to the client (default: <b>no</b> ). This setting applies to all user for whom no explicit profile has been assigned which would then have precedence. <b>Note:</b> X11 forwarding will greatly reduce the usefulness of session tracing which only applies to terminal based activities not using the X11 channel.

### 1.3.2 Authentication & Login

List 15-3 SSH Proxy configuration - Authentication & Login - section User Authentication

Parameter	Description
<b>Authentication Scheme</b>	This parameter defines the authentication scheme for login (user/password combination). <b>Note:</b> Authentication Scheme OCSP is NOT supported.
<b>Use Group Policies</b>	Setting this parameter to <b>yes</b> (default: <b>no</b> ) enables parameters <b>Allowed User Groups</b> and <b>Blocked User Groups</b> for defining access restrictions according to group information.
<b>Allowed User Groups</b>	Enter groups for which access is granted into this field and click <b>Insert ...</b> in order to add them to the listing on the right.
<b>Blocked User Groups</b>	Login names of users which are not allowed to use the proxy. This setting allows for more fine grained control of access refusal than a group based option. The user will not be refused access by the authentication subsystem but the proxy engine itself. The user will receive an appropriate message instructing her/him that no valid authorization to use the service could be determined. Enter groups for which access is denied into this field and click <b>Insert ...</b> in order to add them to the listing on the right. <b>Note:</b> Policy enforcement parameters <b>Allowed User Groups</b> and <b>Blocked User Groups</b> have the following preferences: <ul style="list-style-type: none"> <li>➤ <b>Blocked User Groups</b> overrules <b>Allowed User Groups</b> (having user in both groups causes a block)</li> <li>➤ leaving both fields empty results in allow all.</li> </ul>

List 15-4 SSH Proxy configuration - Authentication & Login - section User Session Handling

Parameter	Description
<b>Login Greeting Text</b>	Via this field you may define custom login messages that are displayed as soon as user logins were successful.
<b>Login Grace Time [s]</b>	This parameter defines the maximum amount of time a login attempt may last (default: 120 seconds).
<b>Pending Session Limit</b>	Here the maximum number of pending sessions (initiated but not established) is specified.
<b>Client Alive Interval [s]</b>	Sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client. This option applies to protocol version 2 only.
<b>Client Alive Max Count</b>	Sets the number of client alive messages (see above) which may be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, therefore terminating the session. It is important to note that the use of client alive messages is very different from <b>KeepAlive</b> (below). The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option enabled by <b>KeepAlive</b> is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become inactive.
<b>DNS Reverse Lookup</b>	Specifies whether sshd should lookup the remote host name and check that the resolved host name for the remote IP address maps back to the very same IP address.

### 1.3.3 Default Permissions

List 15-5 SSH Proxy configuration - Default Permissions - section Security Options

Parameter	Description
<b>Max Illegal Inputs</b>	This parameter defines how often an illegal option may be selected by the user until the connection is terminated.
<b>Record Terminal Session</b>	User terminal activity is being recorded into a file.
<b>Recorded Users</b>	User login names for whom the recording will take place.
<b>Blocked Users</b>	These users have no access to any of the configured SSH destinations.
<b>Inactivity Grace Time [s]</b>	As soon as a SSH connection has no longer traffic, this limit waited until the connection is terminated (default: 120).
<b>Supported SSH Protocol</b>	This parameter defines the to-be-used SSH protocol (v2-only - default - or v2-and-v1) for connecting to remote targets. <b>Attention:</b> Since SSHv1 is considered to be insecure, phion highly recommends not to use option v2-and-v1.
<b>Allow Outbound Compression</b>	States whether or not data compression is supported by the proxy for outgoing client connections. Within LAN environments using compression can create a significant CPU overhead and is typically not advisable. When connecting to remote servers over low bandwidth links compression may appreciably improve the user experience. Note that when set to yes the user is prompted if he/she would like to request compression when connecting to the target server.
<b>Forward X11 connections</b>	Allow X11 connection through the SSH proxy (transferring and displaying data used by a remote X11 application on your local workstation is permitted through the SSH tunnel).
<b>Allow Public Keys</b>	Specifies whether public key authentication is allowed by the server. Set this option to yes if you wish to allow connecting users to authenticate themselves at a target system with public key authentication. While authentication at the SSH proxy requires user/password authentication, it still supports this feature at a remote target via SSH agent forwarding.
<b>Support Agent Forwarding</b>	Specifies whether the connection to the authentication agent (if any) will be forwarded to the connecting user's machine or not. This is required when users are allowed to used cascaded agent forwarding. Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the connecting host (for the agent's Unix-domain socket) can access the local agent through the forwarded connection. An attacker cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent.
<b>Client Log Level</b>	This parameter defines the intensity of log file creation.
<b>SSH Escape Character</b>	Sets the SSH escape character (default: none). We strongly advise against the usage of an active escape character unless you completely trust your users.

List 15-6 SSH Proxy configuration - Default Permissions - section Access Options

Parameter	Description
<b>Target Alive Interval [s]</b>	Sets a timeout interval in seconds after which if no data has been received from the server, ssh will send a message through the encrypted channel to request a response from the server. The default is <b>15</b> , indicating that these messages are sent every 15 seconds to the server. This option applies to protocol version 2 only.
<b>Target Alive Max Count</b>	Sets the number of server alive messages (see above) which may be sent without ssh receiving any messages back from the server. If this threshold is reached while server alive messages are being sent, ssh will disconnect from the server, terminating the session. It is important to note that the use of server alive messages is very different from <b>TCPKeepAlive</b> (below). The server alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option enabled by <b>TCPKeepAlive</b> is spoofable. The server alive mechanism is valuable when the client or server depend on knowing when a connection has become inactive.

List 15-6 SSH Proxy configuration - Default Permissions - section Access Options

Parameter	Description
<b>Static Source IP</b>	Defines a static IP address, which is used as source address for the SSH connection.
<b>Allow Local Access</b>	Controls whether or not users may access local box addresses. We recommend to leave this turned off unless you limit access to the proxy to netfence administrators only.
<b>Access Control Policy</b>	Choose between <ul style="list-style-type: none"> <li>➤ <b>By Network ACL Restriction</b> and</li> <li>➤ <b>By Explicit Host Specification</b></li> </ul> Users given access to certain destinations based on destination hosts which are configured in the <b>Access Lists</b> section and referenced by <b>Permission Profiles</b> .
<b>Network ACL</b>	Users - who are not in the <b>Blocked User Groups</b> - can be given additional access rights due to source network restrictions.
<b>Allowed Hosts List</b>	Choose an Access List (defined at 1.3.4 Access Lists, page 366)

### 1.3.4 Access Lists

List 15-7 SSH Proxy configuration - Access Lists- section Access List Configuration

Parameter	Description
<b>Access Lists</b>	<b>Edit...</b> , <b>Insert</b> , or <b>Delete</b> an access list

List 15-8 SSH Proxy configuration - Access Lists - Access List Configuration - section Access List Configuration

Parameter	Description
<b>Allowed Hosts</b>	<b>Edit...</b> , <b>Insert</b> , or <b>Delete</b> an allowed host

List 15-9 SSH Proxy configuration - Access Lists - Access List Configuration - section Allowed Host Configuration

Parameter	Description
<b>User Visible Name</b>	Name of the target host allowed to connect, seen by the user (when connecting to the SSH proxy)
<b>Target FQDN</b>	Fully qualified domain name of the target host defined in DNS
<b>Target IP Address</b>	IP Address of the target host allowed to connect, seen by the user (when connecting to the SSH proxy)

### 1.3.5 Permission Profiles

This is nearly the same as the Default Permissions (list 15-5, page 366) but can be applied to users by way of assignments to login names, see **1.3.6 User Authorization**.

### 1.3.6 User Authorization

This view allows creating pre-defined profiles for SSH permissions. The created profiles are available in User Authorization view.

The parameters are the same as mentioned in list 15-5, page 366.

List 15-10 SSH Proxy configuration - User Authorization

Parameter	Description
<b>Permission Profile</b>	Here a pre-defined permission profile has to be selected.
<b>User Names</b>	Can be used to assign a permission profile to user login names. If there is no valid assignment for a particular user then the default permissions will apply.

# Anti-Virus

<b>1.</b>	<b>Overview</b>	
1.1	General .....	368
<b>2.</b>	<b>Configuration</b>	
2.1	Basic Setup .....	368
2.2	Archive Scanning .....	369
2.3	Scanning Options .....	369
2.4	Integration .....	369
2.4.1	Proxy Integration .....	369
2.4.2	Mail Gateway Integration .....	371
2.5	FTP Gateway Integration .....	372
<b>3.</b>	<b>Pattern Update Manipulation</b>	
3.1	Update / Disable .....	373

# 1. Overview

## 1.1 General

The AntiVir service is a tight integration of the AVIRA products into the netfence gateway.

This allows easy configuration of AntiVir parameters as well as simple integration together with the phion netfence proxy and phion netfence mail gateway services.








Introduction of the Anti-Virus Service is a pre-requisite for actually using virus scanning later on.

The squid-based phion proxy service communicates with the Anti-Virus Service by using the standardised ICAP protocol. Scanning of SMTP e-mails is based on standard SMTP communication between the netfence mail gateway and the Anti-Virus Service.

### Note:

Licenses for both, phion AntiVir service (.lic file) and AVIRA products (.key file), are required for full virus scanner integration functionality. Import the .lic file into the **Box Licenses** container (**Configuration Service** - 5.1.4 Inventory, page 103). Import the .key file into the license fields provided within the Virus Scanner service (see **AVIRA license** below). Further information on Avira Virus Scanner Licenses is available in **Licensing** - 3.2.5 Avira Virus Scanner Licenses, page 502.

## 2. Configuration

Open the configuration dialogue via  **Config** >  **Box** >  **Virtual Servers** >  <servername> >  **Assigned Services** >  <servicename> (**virscan**) >  **Virus Scanner Settings**.

### 2.1 Basic Setup

#### Attention:

Please take into consideration that virus patterns are not updated immediately when activating the service. The pattern update is carried out 1 minute after starting the service.

List 16-1 Virus Scanner Settings - Basic Setup - section Basic Setup

Parameter	Description
<b>AVIRA license</b>	Into this field, import the AVIRA License Key (.key).
<b>Contact Mail</b>	Define here the contact mail address.
<b>Quarantine Directory</b>	Here the path of the directory where blocked files should be archived can be entered (default: /var/phion/run/virscan/blocked). <b>Note:</b> The quarantine directory is NOT emptied automatically. Thus it is recommended to have look at it from time to time.
<b>Max. file RAM usage (MB)</b>	Max. file RAM usage (MB) (default: 32) Define here the maximal size of the RAM based file-system which is used to speed up virus-scanning. If the limit is reached, files are moved from memory to disk to reduce memory-usage.

To introduce the phion Anti-Virus Service, follow the instructions in **Configuration Service** - 4. Introducing a New Service, page 97, and select **Virus-Scanner** as **Software Module**.

### Note:

Since the Anti-Virus Service always binds to loopback addresses a **Bind Type** selection is not available.

List 16-1 Virus Scanner Settings - Basic Setup - section Basic Setup

Parameter	Description
<b>Max. Num. Workers</b>	Maximum number of workers that are launched to handle requests. Can be adjusted according to type/power of hardware used (default: 30).

List 16-2 Virus Scanner Settings - Basic Setup - section Updates

Parameter	Description
<b>Disable Update</b>	Setting to <b>yes</b> (default: <b>no</b> ) permanently disables automated virus pattern update. See 3. Pattern Update Manipulation, page 373 for an instruction how to override this setting in individual cases and accomplish unscheduled pattern updates or how to disable pattern updates temporarily only.
<b>Update Every (min)</b>	This parameter is used for defining the virus pattern update frequency in minutes (default: <b>60</b> ). See 3. Pattern Update Manipulation, page 373 for an instruction how to accomplish unscheduled pattern updates.
<b>Use HTTP-Proxy</b>	Since anti-virus-pattern updates are done via HTTP, it is mandatory that the box has access to Internet either directly or via a proxy. This section allows defining the configuration of the proxy server to update the virus patterns in case no direct network connection is available.
<b>Host</b>	used for entering resolvable hostname or host IP address
<b>Port</b>	specifies the port number on which the proxy server is available (default: <b>3128</b> )
<b>Requires Authentication</b>	enables usage of optional username and password to get access to the proxy server (default: <b>no</b> )
<b>Username</b>	specifies the username for accessing the proxy
<b>Password</b>	specifies the password for accessing the proxy



List 16-3 Virus Scanner Settings - Basic Setup - section Reporting

Parameter	Description
<b>HTML Templates</b>	Here the HTML template pages sent to the client browser in case a page is blocked can be defined.

List 16-4 Virus Scanner Settings - Basic Setup - section Advanced

Parameter	Description
<b>Debug Log Level</b>	Define here the level of debug output in the log.

## 2.2 Archive Scanning

List 16-5 Virus Scanner Settings - Archive Scanning - section Archive Scanning

Parameter	Description
<b>Scan Archives</b>	This parameter enables/disables scanning of archives (default: <b>yes</b> - enabled). <b>Attention:</b> Archives are NOT scanned for viruses/malicious software if this parameter is set to <b>no</b> .
<b>Max. Archive Size (MB)</b>	This field allows entering the maximum size allowed for archives to be unpacked and scanned (default: <b>1024</b> ). The policy how archives exceeding this value are handled is defined via parameter <b>Block on error</b> (see below).
<b>Max. nesting</b>	This field allows entering the maximum recursion level allowed for archives to be unpacked and scanned (default: <b>20</b> ). The policy how archives exceeding this value are handled is defined via parameter <b>Block on error</b> (see below).
<b>Max. compression ratio</b>	This parameter protects against so-called "mail bombs" that require an unexpected amount of disk space when unpacked. The value is entered in percent (default: <b>150</b> ). That means 100 % is packed status, 150 % is unpacked status.
<b>Block encrypted archives</b>	If this field is set to <b>yes</b> (as it is by default) encrypted archives will be blocked by the virus scanner.
<b>Block on error</b>	If this field is set to <b>yes</b> (as it is by default) erroneous archives will be blocked by the virus scanner.
<b>Block unsupported archives</b>	If this field is set to <b>yes</b> (as it is by default) not supported archives will be blocked by the virus scanner.

## 2.3 Scanning Options

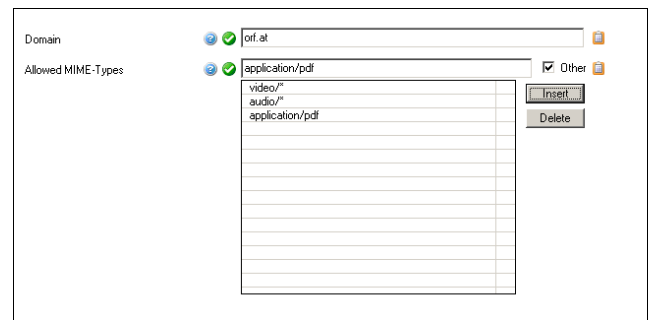
List 16-6 Virus Scanner Settings - Scanning Options - section Non-Virus Detection

Parameter	Description
<b>Detect Dialers</b>	enables/disables detection for unwanted dialers; as soon as installed on the system such programs establish Internet connections via a premium rate number (area codes 0190 in Germany, 09x0 in Austria, Switzerland and, medium-term, Germany). Dialers sometimes are installed inconspicuously and/or fraudulently which may result in horrendous phion bills.
<b>Detect Jokes</b>	enables/disables detection for (often harmless) joke programs.
<b>Detect Games</b>	enables/disables detection for games that may cause no harm but, nevertheless, are unwanted on company workstations.
<b>Detect PMS</b>	enables/disables detection for possible malicious software (PMS); PMS includes spy- and adware that are showing criteria of other malware.
<b>Heuristic Macro Detection</b>	enables/disables usage of heuristics for detecting malicious code in MS Office documents before a Macro update is performed
<b>Heuristic Others Detection</b>	enables/disables detection of known or unknown malicious code in all types of files before an update is performed. The level of intensity ranges from <b>0</b> meaning disabled to <b>3</b> meaning full intensity

List 16-7 Virus Scanner Settings - Scanning Options - section HTTP Streaming

Parameter	Description
<b>Scanning Exceptions</b>	<ul style="list-style-type: none"> <li>➤ <b>Domain:</b> Define here the domains that are excepted from being scanned. Wildcards are possible.</li> <li>➤ <b>Allowed MIME-Types:</b> Define here MIME-types that are excluded from scanning (figure 16-1).</li> </ul> <p><b>Note:</b> To find out which MIME-type has been used set the parameter <b>Debug Log Level</b> to <b>1</b> (Basic Setup, section <b>Virus Scanner Settings - Basic Setup - section Advanced</b>). Afterwards check the Logs for <b>cas</b> log files.</p>

Fig. 16-1 Scanning exceptions

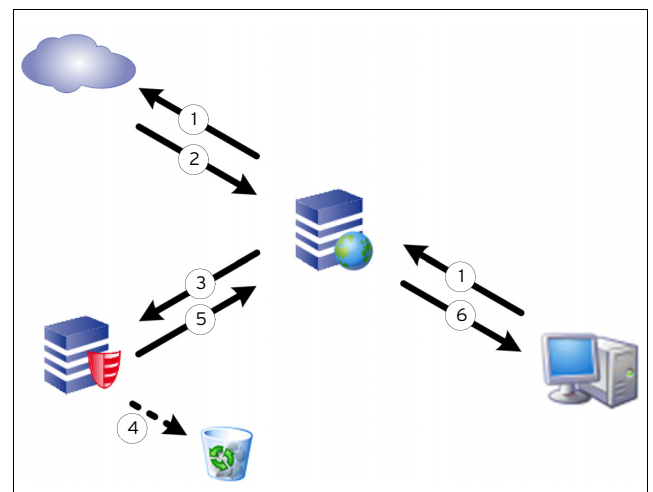


## 2.4 Integration

### 2.4.1 Proxy Integration

The squid-based phion proxy service communicates with the AntiVir WebGate by using the standardised ICAP protocol.

Fig. 16-2 Schematic overview of proxy integration



- Step 1** Request is sent from source address to the Internet.
- Step 2** Response is returned from the destination.
- Step 3** Response is forwarded to the anti virus service via ICAP.
- Step 4** If content is "infected" it is removed.

**Step 5** Scanned response is returned to the netfence gateway. In case of infected content, a corresponding block HTML is sent.

**Step 6** Requested content is delivered to source address. In case of infected content, a corresponding block HTML is displayed.

Integration of virus scanning on a HTTP proxy takes place by setting parameter **Enable Virus Scanner** to **Yes** (as it is by default).

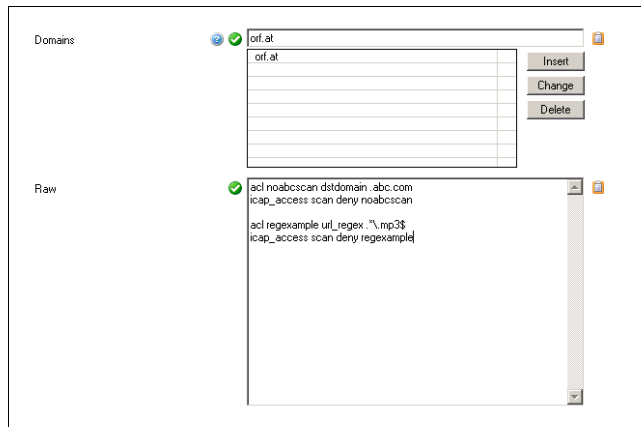
This parameter is located in  **HTTP Proxy Settings - General** tab (**Proxy** - 1. HTTP Proxy, page 324).

The following configuration options are available:

List 16-8 HTTP Proxy Settings - Content Inspection - section Virus Scanner

Parameter	Description
<b>Enable Virus Scanner</b>	This parameter enables/disables the virus scanner (default: yes - enabled).
<b>Scanner Location</b>	Define here where the Virus Scanner Service which should be used for virus scanning is located. Set to <b>Local</b> if the Virus Scanner Service is running on the same box, <b>Remote</b> otherwise. Ensure that the referenced Virus Scanner Service is existent.
<b>Scanner IP</b>	Define here the IP address of the remote Virus Scanner Service which is used for virus scanning. This option is available only if Scanner Location was set to <b>Remote</b> .
<b>Enable Trickle Feature</b>	This parameter enables/disables the trickle feature (default: no - disabled). Trickle feature enabled means that the proxy starts to send trickle packets, which are not download-related. Set the trickle feature parameters appropriately - because if it is too slow or it happens too rarely - the client might time out anyway.
<b>Trickle Size Low Watermark (MB)</b>	There will be no trickle feature running for files smaller than this value. (default: 50 MB).
<b>Trickle Period (sec)</b>	Delay between trickle packets (default: 10 seconds).
<b>Trickle HTTP 1.0</b>	This parameter enables/disables the trickle feature for HTTP 1.0 (default: no).
<b>Scan Exceptions</b>	<ul style="list-style-type: none"> <li>➤ <b>Domains.</b> Define the domains that are excepted from being scanned.</li> <li>➤ <b>Raw.</b> You may also enter raw squid configuration here (figure 16-3).</li> </ul>
<b>Progress Popup</b>	<p>Per default the proxy progress popup is disabled. Enabling the progress popup detects the following browsers per default:</p> <ul style="list-style-type: none"> <li>➤ Mozilla Firefox 2 and 3</li> <li>➤ Microsoft IE 6 and 7</li> <li>➤ Opera</li> <li>➤ Apple Safari</li> </ul> <p>The proxy progress popup is available for both phion HTTP proxy and phion Secure Web Proxy. The progress popup can only be displayed for unencrypted content (HTTP connections). This feature requires running a phion antivirus service and is not available in conjunction with third-party antivirus engines.</p> <p>See list 16-9 for parameter description.</p>

Fig. 16-3 Scan exceptions



**Note:**

Scanning of FTP over HTTP Requests is included in the HTTP Proxy Settings and configured in the AVIRA ANTIVIR WEBGATE tab. Scanning of mere FTP requests handled through settings of the FTP Gateway is configured in the AVIRA ANTIVIR FTP SCANNING tab.

List 16-9 Content Inspection - section Virus Scanner - Progress Popup

Parameter	Description
<b>Enable Progress Popup</b>	Set to <b>Yes</b> to enable the proxy progress bar.
<b>Log Decisions</b>	Set to <b>Yes</b> to enable a more granular logging where decisions why a progress bar is shown or not are written to the log.
<b>Browsers</b>	<ul style="list-style-type: none"> <li>➤ <b>Detection Regex</b> Is a regular expression which will be applied to the client requests HTTP header for browser evaluation.</li> <li>➤ <b>Exception Regex</b> Is a regular expression which will be applied to the client requests HTTP header as contraindication for a popup. If e.g. a user right clicks a URL and processes a "Save target as ..." command, no progress bar should be popped up. Most browsers are sending a slightly different request in such a case.</li> <li>➤ <b>Show Save Button</b> Set to <b>Yes</b> if the download should not be fetched automatically but the button <b>"Save file as ..."</b> should be shown instead.</li> </ul>
<b>Mime-Types</b>	Define here the mime-types for which a progress bar should be shown. The default settings already contain the most useful mime-types. Mime types which are not saved to disk but handed over to a plugin from the browser (e.g. application/pdf) usually should not be applied to a progress bar, because users are expecting such types to be opened automatically which is not possible with a progress bar. Even worse, the browser and the plugin try to download the requested file, but the temporary link is just valid for one download and thus the second download request (from the plugin) will fail.
<b>Popup After (sec)</b>	Define here after which amount of time a progress bar popup should be raised.
<b>No Popups If Less Than (sec)</b>	Define here for which download time (this value or less) a progress bar popup should be suppressed.
<b>Excluded Domains</b>	Define here a list of excluded domains (e.g. where may automated download come from). This setting overrules the settings from above, that is if a download matches one of the entries in this list a download progress bar is never shown. <p><b>Note:</b> The filter works only for domains and subdomains. (That means until the first slash (/) appears in the path).</p>
<b>Excluded Sources</b>	Define here a exception list of sources where a download progress bar always is suppressed. This setting overrules the settings from above, that is if a download matches one of the entries in this list a download progress bar is never shown.

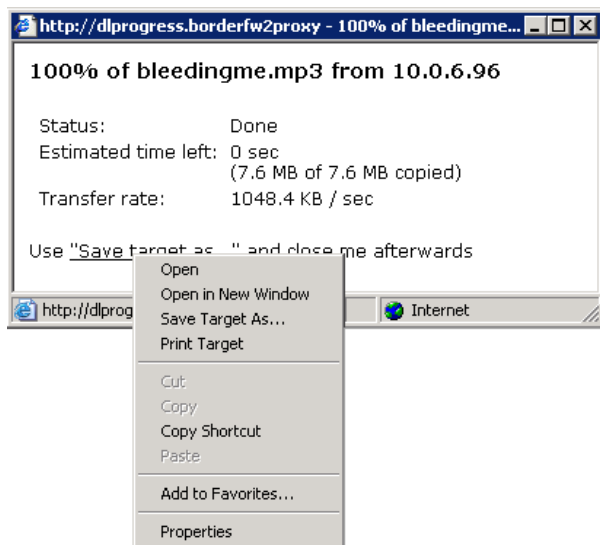
List 16-9 Content Inspection - section Virus Scanner - Progress Popup

Parameter	Description
<b>Progress Template</b>	Define here a HTML template of your customized download progress popup. <b>Note:</b> This setting may damage your progress bar popup seriously. Be sure what your are doing. Take the default template as a starting point of modification.
<b>Unknown Downloads Template</b>	Define here a HTML template of your customized "unknown download" template which is shown if someone tries to call a temporary URL which does not exist any more. <b>Note:</b> This setting may damage your progress bar popup seriously. Be sure what your are doing. Take the default template as a starting point of modification.
<b>Custom Template Logo</b>	Import here a logo.

### 2.4.1.1 Hints on Progress Popup

- The Progress Popup does not work with HTTPS connections.
- Supported browsers are Mozilla Firefox 2 and 3, Microsoft Internet Explorer 6 and 7.
- Internet Explorer 6 - mp3-files download procedure:

Fig. 16-4 Progress bar



- Right-click "Save target as..."
- Select **Save Target As...** from the context menu
- Browse to the desired folder and click **Save**

**Note:**  
Parameter **Show Save Button** has to be set to **Yes**.

- Internet Explorer 6 and 7 - PDF-files download procedure: same download procedure as with mp3-files.
- If you want to define at **Mime-Types** a type text/plain be sure to add an asterisk, otherwise it won't work (text/plain\*).
- The download bar is not working with a transparent proxy, except the <visible-hostname> is DNS-resolvable.

## 2.4.2 Mail Gateway Integration

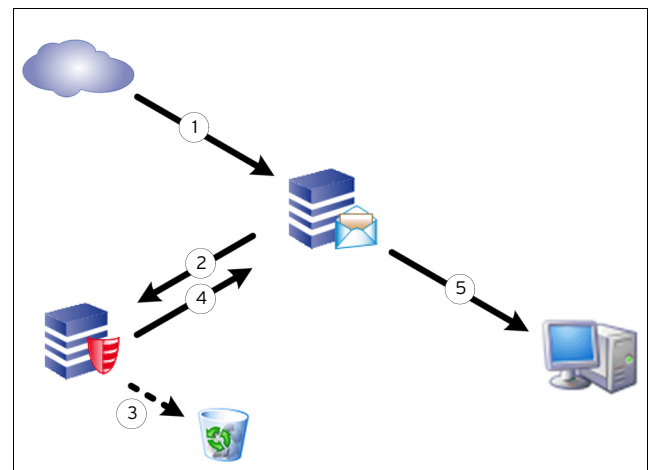
Scanning of SMTP e-mails is based on standard SMTP communication between netfence mail gateway and AntiVir MailGate.

- Step 1 Mail approaches mail gateway**
- Step 2 Mail is redirected to virus scanner**
- Step 3 (optional) Infected mail is deleted**
- Step 4 Mail is returned for delivery**
- Step 5 Mail is delivered**

Integration of virus scanning on a netfence mail gateway takes place by setting parameter **Enable virus scanning** to **yes** (as it is by default).

This parameter is located in **MailGW Settings > Content Adaption (Mail Gateway - 3.2 MailGW Settings, page 246)**.

Fig. 16-5 Schematic overview of mail gateway integration



The following configuration options are available:

List 16-10 MailGWSettings - Virus Scanning - section Virus Protection

Parameter	Description
<b>Enable Virus Detection</b>	This entry allows enabling the scan engine. The following values are available: <b>Yes</b> - specifies an external virus scanner <b>No</b> - disables virus scanning <b>external</b> - uses an external antivirus service
<b>Advanced Virus Protection Option</b>	see list 16-11
<b>External Scan Engine</b>	see list 16-15

List 16-11 MailGWSettings - Advanced Virus Protection Option - section Scanner Location

Parameter	Description
<b>Scanner Location</b>	Define here where the Virus Scanner Service which should be used for virus scanner is located. Set to <b>Local</b> if the Virus Scanner Service is running on the same box, <b>Remote</b> otherwise. Ensure that the referenced Virus Scanner Service is existent.
<b>Scanner IP</b>	This field takes the IP address(es) of SMTP scan engine(s). If multiple virus scanners have been supplied, the first available will be used for virus scanning. If connection to the actively used virus scanner breaks, the next available virus scanner will be contacted.

List 16-12 MailGWSettings - Advanced Virus Protection Option - section Notification

Parameter	Description
<b>Expose Sender Alerts</b>	Warnings can be sent to the sender of e-mails containing viruses/malicious software. The following settings are available: <b>NO</b> - Warnings are never sent to the originator. <b>YES</b> - Warning are always sent to the originator. <b>LOCAL</b> (default) - Warnings are sent only if the originator is a local domain user. <b>Note:</b> Use the <b>Extended Domain Setup</b> of the Mail Gateway to configure local domains. Users belonging to domains defined as <b>internal</b> and <b>strictly_internal</b> through parameter <b>Protection Profile</b> , are treated as local ( <b>Mail Gateway</b> - 3.2.2 Extended Domain Setup, page 247).
<b>Expose Postmaster Alerts</b>	Warnings concerning e-mails containing viruses/malicious software can be sent to the postmaster. The following settings are available: <b>yes</b> (default), <b>no</b> .
<b>Silently Drop Phishing Mail</b>	When set to <b>yes</b> (default: <b>no</b> ), the virus scanner service does not generate a DSN delay message addressed to the e-mail's sender when it recognises a phishing e-mail. The original phishing e-mail is automatically moved to the give-up folder and no further attempts are made to forward it.

List 16-13 MailGWSettings - Advanced Virus Protection Option - section Adaptions

Parameter	Description
<b>Add Status in Body</b>	Virus status is added to mail body (default: <b>no</b> ).
<b>Add X-Status in Header</b>	Virus status is added to mail header (default: <b>yes</b> ).
<b>Add Body to Notice</b>	The original body of the infected mail is appended to the postmaster notice mail (default: <b>yes</b> ).

List 16-14 MailGWSettings - Advanced Virus Protection Option - section No Scan Exceptions

Parameter	Description
<b>No Scan For (Recipients)</b>	Allows defining recipients/sender whose e-mails are not scanned. The syntax is perl-compatible regular expression (for example
<b>No Scan For (Sender)</b>	^virus@mydomain.com\.tld\$).

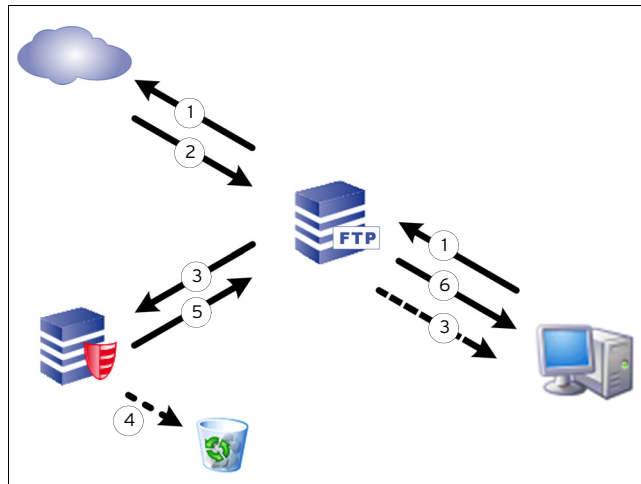
List 16-15 MailGWSettings - External Scan Engine

Parameter	Description
<b>Scan Engine IPs</b>	This field takes the IP address(es) of external SMTP scan engine(s). If multiple virus scanners have been supplied, the first available will be used for virus scanning. If connection to the actively used virus scanner breaks, the next available virus scanner will be contacted.
<b>Scan Engine Port</b>	Here the ports used to to contact the external SMTP scan engine are specified.
<b>Bind IP</b>	Here the IP address the mail gateway service listens to and awaits virus scan engine replies from can be entered. <b>Note:</b> The Bind IPs also need to be entered as part of the server configuration.

## 2.5 FTP Gateway Integration

Scanning of FTP requests is processed via internal service communication between FTP gateway and the virus scanner service.

Fig. 16-6 Schematic overview of FTP gateway integration



**Step 1** FTP request is sent from the client to the Internet passing the FTP gateway.

**Step 2** Response is returned from destination to the FTP gateway.

**Step 3** Response is split into two information streams.

Per 4096 KB package, 1 KB is directly returned to the client without being scanned, to avoid that the connection between client and FTP gateway times out. The larger part of the data package is forwarded to the anti virus service.

**Step 4** If content is "infected" it is removed.

The virus scanner returns error code and virus information to the FTP gateway, which causes termination of the client data connection. Furthermore, it returns a 505 error code containing the virus information. The FTP gateway forwards this information to the client (505 virus <virus\_name> found in file).

The not scanned part of the data package, which has already been forwarded to the client, remains on it as tiny file fragment. This fragment has to be deleted manually.


**Step 5** If content is clean, scanned response is returned to the FTP gateway.

**Step 6** FTP gateway delivers requested content to the source client.

## 3. Pattern Update Manipulation

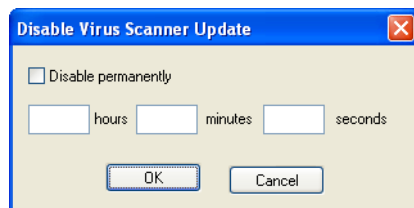
### 3.1 Update / Disable

The general virus pattern update-logic of the AntiVir service is defined through the parameters **Update Every (min)**, page 368 and **Disable Update**, page 368. Settings defined here can be overridden temporarily through, if manual interaction is desired.

To initiate unscheduled virus pattern updates or to disable the pattern update cycle browse to  **Control** > **Server** tab and in the **Service Status** section of the window select the virus scanner service with a left-click. Then right-click to make the following additional context menu entries available:

- **Update Pattern**  
Selecting this item triggers an immediate virus scanner update.
- **Disable Pattern Update**  
Selecting this item opens an interactive dialogue that allows customising the length of the pattern update blockage. The following specifications are available:

**Fig. 16-7** Disabling virus pattern updates manually



- **Disable permanently** - Select this item to disable virus pattern updates permanently.
- **hours/minutes/seconds** - These fields allow defining a time span during which general virus pattern update settings should be ignored.

Permanent and temporary virus pattern update deactivation change the context menu entry **Disable Pattern Update ...** to **Enable Pattern Update**. Select this item to revoke your modifications.

Blocked update states are appropriately visualised by an entry in the Info column appended to the service entry.

**Note:**

For security reasons access to this trigger is restricted to the administrator's role:

- On single boxes access is permitted for the Manager and Security roles (table 3-20, page 91).
- On management centres access is permitted through the VIRSCAN MODULE section within the Administrators configuration (list 18-12, page 414).





# High Availability

<b>1.</b>	<b>Overview</b>	
1.1	Main Principle of High Availability Operations .....	376
1.2	Definitions and Notions in a High Availability system (HA) .....	376
1.2.1	Primary Box / Secondary Box .....	376
1.2.2	Primary Server / Secondary Server .....	376
<b>2.</b>	<b>Setting up a HA System</b>	
2.1	General .....	378
2.2	Introduction .....	378
2.2.1	Modes of Operation .....	378
2.3	Designing a HA System .....	378
2.4	Configuring HA Pairs .....	379
2.4.1	Configuring a Stand-alone HA Pair .....	379
2.4.2	Configuring an MC-administered HA Pair .....	380
2.4.3	HA Sync Status .....	381
2.4.4	Emergency Override .....	381
2.4.5	Configuring Interception of Failure Conditions .....	382
<b>3.</b>	<b>Services with Additional HA Mechanisms</b>	
3.1	General .....	383
3.2	Transparent Failover for a HA Firewall .....	383
3.2.1	Synchronising Procedure .....	383
3.2.2	Take-Over Procedure .....	384
3.2.3	Configuration .....	384
3.2.4	Visualisation .....	384
3.3	Mail Gateway with HA .....	384
3.3.1	Automatic E-mail Synchronisation .....	384
3.3.2	Manual E-mail Synchronisation after HA Handover .....	384

# 1. Overview

## 1.1 Main Principle of High Availability Operations

The mechanism of **High Availability (HA)** works by exchanging alive packets with the HA partner and informing each other about their status. Also echo requests (pings) and ARP requests (**Address Resolution Protocol**) are exchanged. This is repeated every 10 seconds for Box IP and Server IPs. If there is no response from the active system/server the following scenario will happen:

- **Box IP** does not respond - causes the transfer of all servers to the HA partner
- **First Server IP** does not respond - causes the corresponding server to be transferred

In either situation, the state of the other system/server changes to unknown. The frequency of alive packets and pings is increased. If there is response from the primary, the cycle will fall back to normal operation. If there is no response within 10 seconds the inactive partner (normally the secondary box) will make an emergency server start. When the primary box becomes active again it will recognise the active servers on the secondary box, and will go into standby mode.

### Note:

If the primary and secondary box activate their servers at the same time, the secondary box will "win", and the primary will shut down its server immediately. This procedure makes sure that only one HA partner is in operational mode while the other one is in standby mode.

### Note:

In order to have the HA mechanism for a single service, it is necessary to create a separate server for this service on the phion netfence

Table 17-1 State table with working communication

Primary Box	Secondary Box	Control Primary	Control Secondary	Comment
Active	Active	Primary / unknown	Secondary / unknown	Instable, both boxes runs their servers, for a short amount of time, duplicate IPs are detected until the primary box will stop its servers; typical situation of a broken communication channel.
Active	Inactive	Primary / Standby	Standby / Primary	Normal operation mode
Active	Blocked	Primary / Block	Block / Primary	If the primary box fails, the HA partner is not available
Inactive	Active	Down / Secondary	Secondary / Down	Normal operation mode, the server is running on the secondary machine

Table 17-1 State table with working communication

Primary Box	Secondary Box	Control Primary	Control Secondary	Comment
Inactive	Inactive	Down / Unknown	Down / Unknown	Both boxes start their servers, if the primary starts first, it will keep up the servers, the secondary will fall into standby mode (Active/Inactive)
Inactive	Blocked	Down / Block	Block / Down	The secondary box was active, the primary was in standby mode until the secondary was blocked
Blocked	Active	Block / Secondary	Secondary / Block	If the secondary box fails, the HA partner is not available
Blocked	Inactive	Block / Unknown	Down / Block	Situation after server on primary machine is blocked and secondary is not up yet
Blocked	Blocked	Block / Block	Block / Block	No active server is running

## 1.2 Definitions and Notions in a High Availability system (HA)

### 1.2.1 Primary Box / Secondary Box

#### ➤ **Primary box**

This is the box which runs all servers and services until a serious fault occurs or servers and services have to be shut down for system maintenance.

#### ➤ **Secondary box**

Identically (to the primary box) set up box, which runs in standby-mode until the primary box is unreachable. In this case, the secondary box starts its servers and services to minimize the fail over time.

#### ➤ **Communication table**

There are various different states how the two boxes behave to each other.

Table 17-2 Communication between HA partners; ARPs are independent from a HA system.

Protocol	Active	Inactive
UDP801	1 ⇔ 2	2 ⇔ 1
ICMP	1 ⇔ 2 + primary server IP	
ARP	1 ⇔ 2	1 ⇔ 2

### 1.2.2 Primary Server / Secondary Server

#### ➤ **Primary Server**

This is the active server in the high-availability system. The position of the primary server within the HA system is completely irrelevant. In a system built up of 5 HA partners, the VPN primary server might for example run on box 4 its secondary partner on box 5.

**Secondary Server**

This is the backup server within the high-availability system, configured for taking over services in case the services on the partner box become unavailable. Note that not only box failure might result in activation the secondary server, but also unavailability of network components the service relies upon.

Always remember to make a clear differentiation in the use of nomenclature. The naming **primary box** and **secondary box** respectively is always meant from the server's point of view. Whereas, when speaking of **primary server** and **secondary server** the service itself is thought of, which has to be started on the HA partner as soon as one box or communication to a networking component the service relies upon fails.

Using HA configuration to balance the load between boxes is a very common and effective way to exploit all features given by the phion netfence architecture. Figure 17-1 visualises the behaviour of HA partners in case of services failure on the primary server

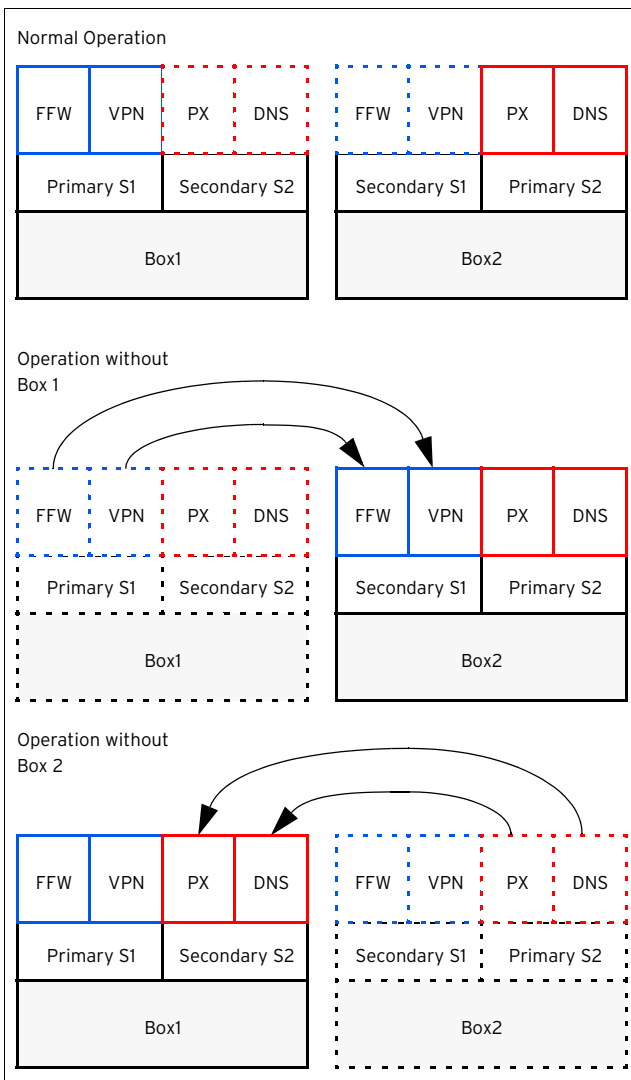
**Example:**

Primary Server S1 on HA Box1 knows Secondary Server S1 on HA Box2 as HA-Partner Server.

Primary Server S2 on HA Box2 knows Secondary Server S2 on HA Box1 as HA-Partner Server.

While both boxes are active, the services FFW and VPN are processed on the HA Box1 while the Services Proxy and DNS are processed on the HA Box2. If the state of the HA Box1 changes to "unknown" due to fatal errors either hardware or software sided, the HA Box2 starts its Secondary Server S1 and activates FFW and VPN service within a few seconds.

Fig. 17-1 Load Balancing with a HA system



## 2. Setting up a HA System

### 2.1 General

#### Note:

It is important to configure switches and routers properly to work in conjunction with a HA system. Most important is the so-called **ARP cache time** or **ARP timeout**. When the secondary box starts its services the IP addresses of the primary box are used (except the management IP) but with different MAC addresses. With an infinite timeout configured the secondary box would never be reached. With a timeout of 300 seconds, the secondary box would not be reached for 5 minutes, and the HA concept would not fulfil its purpose. The recommended setting lies between 30 and 60 seconds. Disadvantage: The amount of ARP requests will increase with a higher timeout.

When setting up a phion HA system there are typically three possible initial situations.

- A standalone netfence gateway already exists which can be upgraded to HA mode.
- Two separate standalone netfence gateways exist which can be turned into a single HA pair.
- A HA pair has to be installed from scratch. In this case install a new single system first. Then upgrade this system to HA mode (see first scenario above).

### 2.2 Introduction

We assume that a successfully installed single box already exists (**Getting Started**, page 7). Thus, the scenario explained below also applies when upgrading single box operation to HA operation mode. For the single system a so-called DHA (**Dedicated High Availability**) box is defined. The DHA box has the same configuration as its HA partner. This box is inactive as long as there is no serious fault on the other box or its services have been shut down for system maintenance.

Fig. 17-2 HA monitoring without private uplink (HA state exchanged via 10.0.8.0/8 network)

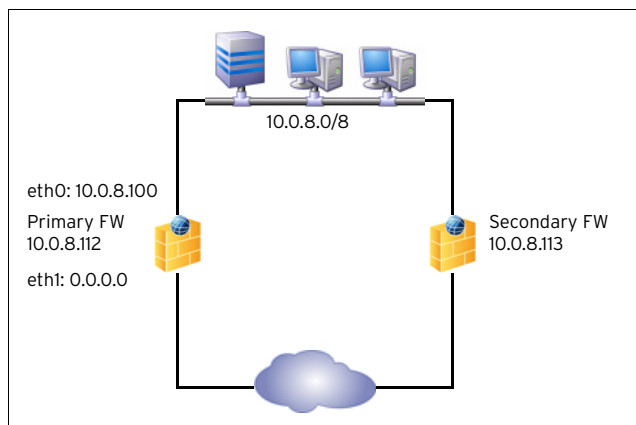
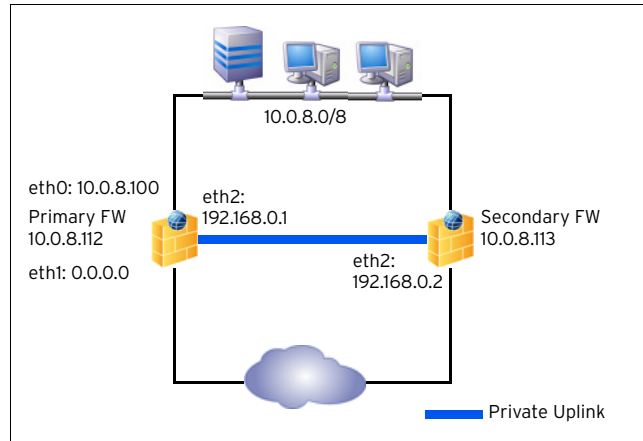


Fig. 17-3 HA monitoring with private uplink



#### 2.2.1 Modes of Operation

In a HA system with no private uplink alive packets and status information are transferred over the network which the management IP addresses belong to (figure 17-2).

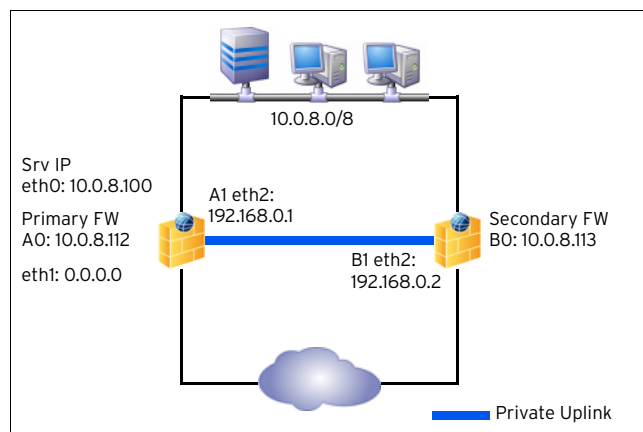
#### Note:

When the switch "dies", the connection between the HA partners will break, too, and the secondary box will start its servers albeit the primary box is still alive. When the switch is re-activated, for around 1 second both boxes are up and duplicate IPs are online until the primary box stops its servers.

In a HA system with private uplink one network interface is dedicated for HA purposes (figure 17-3). There are some routing specialities (host routes) to route the HA traffic via the private uplink. A failover route has to be configured too to make sure that the boxes can reach each other via both routes. The private uplink should be a direct connection with a cross cable to be independent from a further hardware component (switch/HUB); the subnet for the uplink should be a 2 bit network.

### 2.3 Designing a HA System

Fig. 17-4 Designing a HA system



**Used IP addresses**

**Table 17-3** Designing a HA System - Used IP addresses

	Primary box	Secondary box
Management IP	10.0.8.112 / eth0	10.0.8.113 / eth0
FW Server IP	10.0.8.100	
Further Network (Private Uplink)	192.168.0.1/2 / eth2	192.168.0.2/2 / eth2

The definition which way the heartbeat will go, can be realised in two ways:

- Via the parameter group **Translated HA IP** (🔧 *Config*) > **Box** > **Infrastructure Services** > **Control**. In our example we configure that the heartbeat uses both, the 10.0.8.0/8 network AND the private uplink to send heartbeats.

**Table 17-4** Designing a HA system - Translated HA IP

	Translated HA IP	Alternative HA IP	Usage Policy
Primary FW	10.0.8.113	192.168.0.2	Use-Both
Secondary FW	10.0.8.112	192.168.0.1	Use-Both

- Alternatively you can use the **Routing** (🔧 *Config*) > **Box** > **Network** > **Network Routes** instead.

**Table 17-5** Designing a HA system - network routes

Route	Primary box	Secondary box	Comment
Direct route	10.0.8.112 / eth0	10.0.8.113 / eth0	Preference 200
Gateway route	10.0.8.113 via 192.168.0.2	10.0.8.112 via 192.168.0.1	Preference 100

All gateway routes must have a lower preference than the direct route to make sure that HA traffic is routed via the private uplink (preference 0).

The explicit failover route via eth0 is required because the minimal scope algorithm would cause the kernel to use the HA link even if it is disabled (preference 65000).

**Attention:**

It is important to include the net of the private uplink into the box ACLs since otherwise the control daemon would disable the gateway routes because the other machine does not answer.

According to the example above the configuration looks as follows:

- Primary FW:
  - Source IP A1 via gateway B1 to Destination IP B0 (Preference 100)
  - B0 interface eth0 (Preference 200)
- Secondary FW:
  - Source IP B1 via gateway A1 to Destination IP A0 (Preference 100)
  - A0 interface eth0 (Preference 200)

## 2.4 Configuring HA Pairs

### 2.4.1 Configuring a Stand-alone HA Pair

There are several ways to reach HA. The first way is with an existing netfence and a box, which has to be installed as HA partner.

The installation of a stand-alone HA pair works as follows:

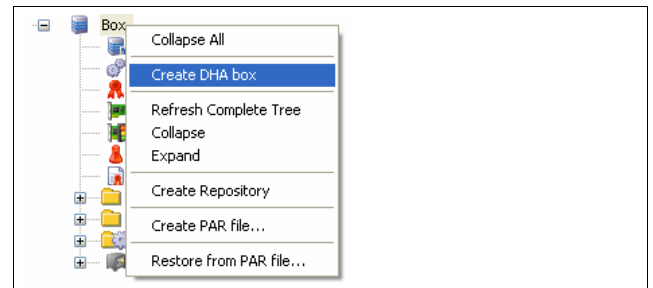
**Step 1 Installation of the primary box**

**Step 2 Complete configuration of the primary box (server, services)**

**Step 3 Creation of the dedicated HA (DHA) box**

After installation and configuration of the single box, create the DHA partner by clicking right on the box icon in the configuration tree and selecting **Create DHA box** from the context menu.

**Fig. 17-5** Context menu of Box



A new menu item in the configuration tree of the box (**HA Box**) is created.

The HA network settings tab has to contain the network interfaces, the management IP, routes, ...

**Note:**

From its first boot on, the DHA box has every information about the configuration, and works in standby mode. Every change of the primary box configuration will be transmitted to the secondary box instantly.

**Step 4 Installation of the DHA box with the PAR file for the DHA box**

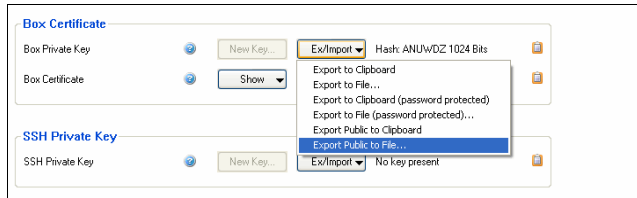
After the HA box has been configured, a PAR file has to be created. Therefore select **Create PAR file for HA box ...** from the context menu.

The procedure to setup a box with a PAR file is described in **Getting Started**, page 7.

### Step 5 Introduction of the HA Box to the Managing Workstation

To avoid connecting to an unknown system, the box key should be imported into the local phion.a settings. The two machines share their keys, hence the public key can be imported from the primary one. It is found in the configuration file **Identity**.

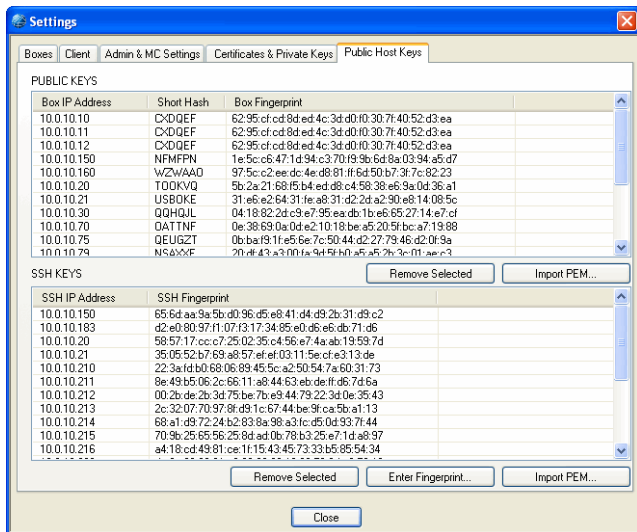
Fig. 17-6 Exporting the public key to a file



This tab is used to manage the box keys and certificates, the function **Ex/Import** is needed to export the Box Public Key to a file.

After you have selected a folder to save the public key, the key has to be imported in the phion.a settings (**File > Settings ...** or icon ). Enter the **Public Host Key** tab, click the **Import PEM ...** button and select the public key that was exported above.

Fig. 17-7 Public Host Keys



## 2.4.2 Configuring an MC-administered HA Pair

The creation of MC-administered HA pairs works slightly different, as the pairs have to be combined in the configuration section of the MC and not in the configuration section of the boxes themselves.

Perform the following step to create an MC-administered HA pair (it is supposed that the boxes already exist):

### Step 1 Creation of the server

Create a Server in the Cluster Server's interface of the MC. In this context choose the boxes which should operate together as HA partners.

Fig. 17-8 Creation of MC-administered HA partners - Step 1

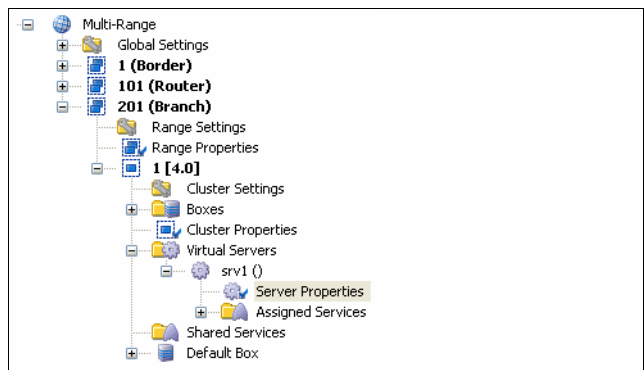
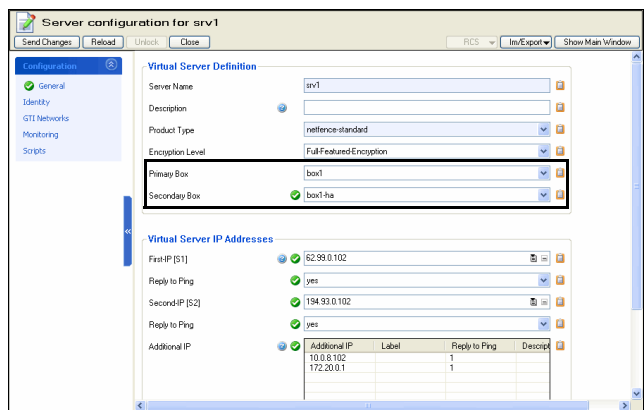


Fig. 17-9 Creation of MC-administered HA partners - Step 2



The primary and secondary servers will automatically be created and configured as HA partners on both boxes.

**Note:**  
Please consider that HA partners can only be created within one cluster.

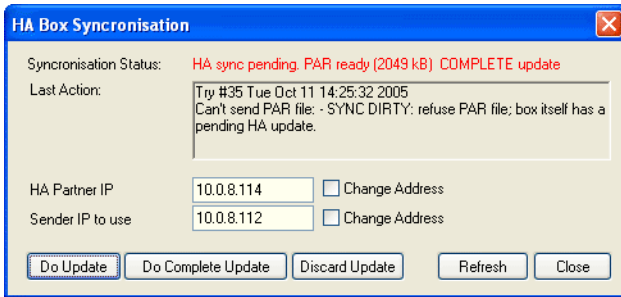


### 2.4.3 HA Sync Status

Configuration changes on the primary box will be transferred to the secondary box instantly. The sync status can be viewed via the phion.a configuration GUI.

To do so, simply click **HA Sync ...**

Fig. 17-10 Sync Status of two HA partners



- **Do Update**  
An incremental update will be performed.
- **Do Complete Update**  
A complete update will be performed.
- **Discard Update**  
Discards the changes; needed when the two HA partners are in an inconsistent state (for example when primary box was down, configuration changes had to be made on the secondary box, that means the secondary box has been set to **Emergency Override**).
- **Refresh**  
Refreshes this window to see actual changes (completion of update).

### 2.4.4 Emergency Override

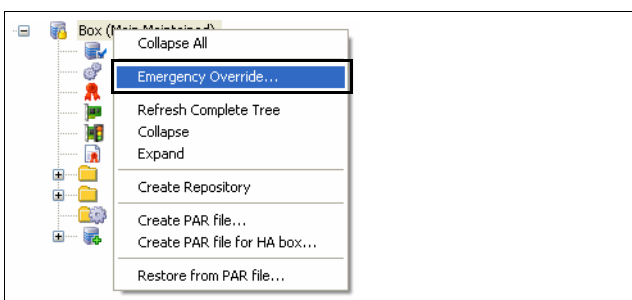
If the primary box fails, configuration changes have to be made on the secondary box. In normal operation mode it is not possible to alter configuration via the secondary box. If there is the need to do so, the DHA box has to be set in the **Emergency Override** mode. After re-establishing the primary box the synchronisation has to be started manually.

Hence the procedure after a serious failure of the primary box is the following:

#### Step 1 Enable the Emergency Override mode

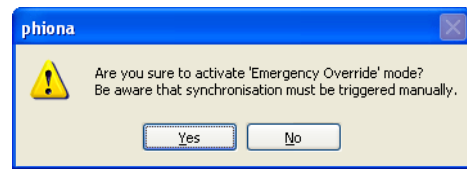
To enable the emergency override mode open the phion.a configuration GUI and establish and a connection to the secondary box. Open the context menu with right-click on Box (Backup) and select **Emergency Override**.

Fig. 17-11 Emergency Override of a HA Box



Confirm the now opened query with **Yes** to enable the Emergency Override.

Fig. 17-12 Confirmation query for Emergency Override



The box icon gets highlighted in yellow (🟡) as soon the **Emergency Override** is active.

**Note:**  
The Emergency Override option belongs to one session only, that means it must be re-established in every new session.

#### Step 2 Change the configuration

After enabling the Emergency Override mode, the configuration file can be locked and edited. As soon the files have been manipulated, the icon in the header changes and the buttons **Send Changes** and **Reload** are available.

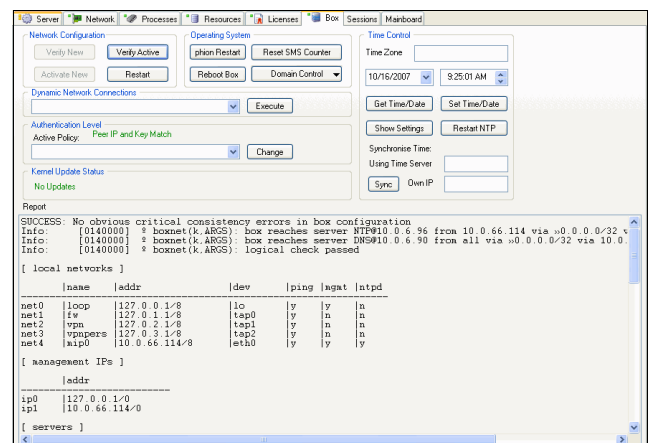
#### Step 3 Send Changes and Activate

**Note:**  
For detailed information on the functions of the buttons **Send Changes** and **Activate**, see **Getting Started**, page 7.

The **Send Changes** button sends configuration changes to the server. The configuration changes will be stored until the changes are activated. The **Reload** button loads the original file with the configuration data before having activated any changes by clicking **Activate**.

To verify the changes for their functionality, it is possible to check the changes before activation. For this purpose the **Box** tab (📦 **Control**) contains the button **Verify New**. Clicking this button results in a detailed report about the changes. When the report is OK (no errors occurred), click **Activate New** to set the changes active.

Fig. 17-13 Example for test report




#### Step 4 Manual synchronisation with the re-established primary box

After having changed the configuration of the secondary box, and the primary box is up and running again, the synchronisation of the two boxes has to be made manually.


##### ➤ Of a standalone HA pair

(it is assumed that services are still active on the secondary box)

- **Clear Dirty Status** Button (click for description)
- Open the  **Config** tree on the secondary box and click the **HA Sync ...** button in the button bar on top of the window.
- Now enter the IPs of the HA partners into the IP address fields of the HA Box Synchronisation window.  
Insert the IP address of the primary box into the **HA Partner IP** field.  
Insert the IP address of the secondary box into the **Sender IP to use** field.  
Activate the **Change Address** checkboxes to the right of both fields.  
Transfer the configuration from the secondary box to the primary box by clicking the **Do Update** button and instantly thereafter the **Do Complete Update** button.
- Block services on the secondary box so that the primary box can regain normal operation status.

##### ➤ Of a HA management centre

(it is assumed that services are still active on the secondary box)

- **Clear Dirty Status** Button (click for description)
- Open the  **Config** tree on the MC and click the **HA Sync ...** button in the button bar at the top of the window.
- Now enter the IPs of the HA partners into the IP address fields of the HA Box Synchronisation window.  
Insert the IP address of the primary box into the **HA Partner IP** field.  
Insert the IP address of the secondary box into the **Sender IP to use** field.  
Activate the **Change Address** checkboxes to the right of both fields.  
Transfer the configuration from the secondary box to the primary box by clicking the **Do Update** button and instantly thereafter the **Do Complete Update** button.
- Block services on the secondary box so that the primary box can regain normal operation status.

#### Note:

Only configuration changes on the primary box are transferred instantly to the secondary box. In Emergency Override situations the synchronisation from the secondary to the primary has to be done manually. It is recommended to perform a complete update since the updates are done incrementally.

## 2.4.5 Configuring Interception of Failure Conditions

To enable handling of failure conditions and to guarantee a quick take-over of services in case a box or networking component becomes unavailable it is vital to configure monitoring of IP addresses and services. Monitoring configuration is done on Server level (see also **Configuration Service** - 3. Configuring a New Server, page 94).

### 3. Services with Additional HA Mechanisms

#### 3.1 General

Several services can be configured as HA systems, but some of them use distinct synchronisation mechanisms. Two of these services (HA Firewall Service, Mail Gateway with HA) are described below in more detail.

Other available services are:

- DHCP:
  - for Enterprise (netfence 3.2) see **DHCP**, page 271
  - for Basic (netfence 2.4.2) see **DHCP** - 2. "Regular" DHCP, page 282
- SSH (**SSH Gateway**, page 363)
- SPAM-Filter (**Mail Gateway** - 4. Spam Filtering, page 257)

#### 3.2 Transparent Failover for a HA Firewall

We have heard now that a HA system provides safety by taking over the configured servers and services in case of a breakdown of one partner and that a HA system can be used for load balancing to exploit all features available through the phion netfence architecture.

So far so good, but having a firewall server/service taken over by the second HA partner without the open sessions is not that good. Using the function Transparent Failover (activated per rule; active by default) synchronises the forward packet session (TCP in- and outbound, UDP, ICMP-Echo and OTHER-IP-Protocols) of the Firewall server between the two HA partners.

**Attention:**  
 Take into consideration that the following session types are not synchronised:

- Local Sessions
- Stream Forwarding Sessions
- Sessions using a Box IP as Bind
- Sessions redirecting a Box IP
- Sessions explicitly classified as not to be synchronised within the advanced rule parameter of the affected rule

For a working Transparent Failover function it is mandatory to have an analogous network configuration on both HA partners. However, the NICs may differ, but the assignment of the interfaces (for example interfaces and their assignment) has to be identical. That means if the ISP is connected on eth0 and the DMZ is on eth1, it is a must that this assignment is the same on the partner box.

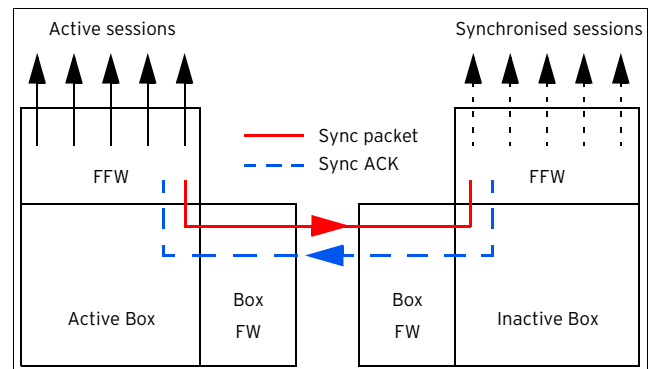
#### 3.2.1 Synchronising Procedure

Synchronisation can be carried out via the uplink connection or alternatively via the LAN connection (see 2. Setting up a HA System, page 378).

The synchronisation traffic is realised by sending UDP packets, so-called sync packets (port 689), with a AES-128 encryption to prevent infiltration. The AES keys are created by using the BOX RSA Keys and are changed every 60 seconds to maintain the high security level of the sync traffic.

Using the LAN connection for synchronising is only possible due to the small amount of necessary synchronisation traffic. This traffic is reduced by synchronising sessions and not each packet. Due to the characteristics of the TCP protocol (SYN, SYN-ACK, ...) this causes that only already established TCP connections are synchronised. When the synchronisation takes place during the TCP handshake, this handshake has to be repeated.

Fig. 17-14 Synchronising procedure



The synchronising procedure takes place immediately (if possible). If synchronisation packets are lost, up to 70 sessions per second are synchronised.

Depending on the system availability, the behaviour differs:

- **Partner box is inactive/rebooted**  
 Sometimes it may happen that the "backup" box is not available and therefore does not respond to the sync packets (for example for maintenance reasons). In this case, the active box stops synchronising. As soon as the partner box re-appears, the active box checks whether the other one was rebooted or has an obsolete session state and re-synchronises all necessary sessions.
- **Active box reboots without a take over**  
 This happens when the button **Phion Restart** is used, that means the acpf and sockets are gone but the box is not re-booted physically. In this case, the partner box recognises that its session state is obsolete and removes all synchronised sessions.

### 3.2.2 Take-Over Procedure

As soon as the HA box - where the firewall runs - does not respond to the heartbeat (Control UDP 801), the take over will be started (after a delay of 10 to 15 seconds). This delay is necessary due to potentially low network performance.

**Note:**

During this time **NO** service is available.

When the box stays inactive, the synchronised sessions on the second box are set active and all connections connections are available again.


Again, the TCP protocol has to be mentioned separately. The "backup" box does not have the current TCP sequence numbers. Hence, in case of a take over, the sequence number is not checked for correctness. As soon as the connection has traffic, the sequence number is known to the former "backup" box and the sequence number check is performable again.

The missing sequence number on the "backup" box also results in the fact that TCP connections that were taken over but have no traffic since then, cannot be reset in a "clean" way. Terminating the session via the **Terminate Session** button removes the connection but does not send a TCP-RST (TCP Reset signal).

### 3.2.3 Configuration

Each Firewall rule is equipped with a **Transparent Failover active/inactive** option that allows you to define whether sessions affected by this rule should be synchronised or not. See **Firewall - 2.3.3 Advanced Rule Parameters**, page 154, **Transparent Failover State Sync**, page 155, for additional information.

### 3.2.4 Visualisation

The state of the sessions is visualised within the **Status** tab of the  **Firewall** service. See **Firewall - 6.2 Real Time Status**, page 169, for a detailed description of this tab.

## 3.3 Mail Gateway with HA

### 3.3.1 Automatic E-mail Synchronisation

The automatic mail traffic synchronisation is quite similar to the Transparent failover that is available for the Forwarding Firewall (**High Availability**, page 375).

As soon as mails are spooled, they are synchronised on the HA partner after a maximum of 10 seconds. However, the synchronisation procedure itself is one-way only. That means changes made to the mail log and envelope on the partner box are lost when the primary box re-takes the mail gateway.

When an already synchronised mail has been delivered, it is deleted on the HA partner.

If a synchronisation attempt fails, it is stored in a transaction log for pending actions and is retried as soon as possible.

### 3.3.2 Manual E-mail Synchronisation after HA Handover

In case of HA handover, the mail gateway service on the secondary HA partner server starts and performs the mail delivery. After successful recovery of the primary HA box, the primary server takes over mail delivery again and the mail gateway running on secondary box stops delivering.

If this process of HA handover happens during mail delivery, it is, in certain cases, possible that there are mails left in the mail queue on secondary HA server. So the delivery is not finished due to HA handover. In other words, HA handover can be initiated while spooling process of mails is active. This effect appears especially during heavy load, when lots of e-mails are processed by the mail gateway service.


In this case, the administrator has to move the affected mails manually from the secondary box to the primary HA partner and initiate the delivery. Thus no mail is lost due to HA handover.

The following description shows step-by-step what has to be done in order to perform in such a case:

**Attention:**

While connected via SSH avoid to enter any commands unless you know exactly what you are doing.

**Step 1 Connecting**

Establish a connection to the secondary HA box using `phion.a`. Now select  **SSH** from the box menu and log into the secondary HA box as `root`.

Change to the spool directory of the mail gateway by using the following command line:

```
cd
/var/phion/spool/mgw/<server_service>/spool/
```

For `<server>`, type in the name of the server, and for `<service>` type in the name of the mail gateway service you have configured when introducing the service.

## Step 2 Check for undelivered mails

This check is done by listing the content of the spool directory. Therefore enter the following command:

```
ls -l
```

If the result of this command is `Total 0`, there are no undelivered mails left and it is not needed to carry on. In this case, type `exit` to close your SSH session.

However, if there are files with the extension `.body` and `.env`, continue with the next step.

## Step 3 Copy the spool directory

Copy all files to the mail input directory of the active (primary) mail gateway service. This is accomplished by using the following command line:

```
scp * <IP>:/var/phion/spool/mgw/<server>_<service>/input/
```

The parameter `<IP>` indicates the box management IP of the primary HA box, where the mail gateway service is active. You will be prompted to enter the root password of the primary box.

## Step 4 Copy the vscan directory (optional)

If the virus scanning for mails is active, it is necessary to copy this directory too.

Therefore change to the vscan directory of the mail gateway using the following command line:

```
cd ../vscan/
```

Now copy all files to the mail input directory of the active (primary) mail gateway service. This is accomplished by using the following command line:

```
scp * <IP>:/var/phion/spool/mgw/<server>_<service>/input/
```

## Step 5 Initiating delivery manually

As soon as Step 3 and Step 4 (optionally) are completed, the manually initiated delivery can be started on the primary HA box. For this purpose you need a SSH session to the active box. This session is established by using the following command line:

```
ssh <IP>
```

For `<IP>` type in the box management IP of the primary HA box, where the mail gateway service is active. You will be prompted to enter the root password of the primary box. After that the prompt of the primary box appears.

Now initiate the mail insertion and delivery of the copied mail in the input directory:





```
/bin/kill -s SIGUSR2 <server>_<service>
```


For `<server>` type in the name of the server, and for `<service>` type in the name of the mail gateway service which you have configured at the time you introduced the service on the box.

### Note:

Mind the case sensitivity.

This command inserts the imported mails from the input directory to spooling process of the active mail gateway, and performs the delivery. Active mail jobs in the current spooling queue are not affected by this action.

In order to verify whether the mails have really been inserted or not, check the mail gateway logs through  **Logs** >  `<servername>` >  `<servicename>`  mailgw). For each newly inserted mail, a log file entry, containing the text "SPOOLER new mail inserted (id=#####-#####-#####)", is generated.

After that, normal delivery of inserted mails is initiated, and can be checked via the operative mail gateway GUI ( **MailGW**).

## Step 6 Removing the obsolete mails

After successful delivery, remove mails left in the `/spool/` and `/vscan/` directories of the inactive mail gateway on the secondary box to avoid duplicate delivery.

To do so, terminate the SSH session to the primary box by entering `exit`. The system prompt of the secondary box now appears displaying the message `Connection to <IP> closed`.

### Note:

If the bash prompt of the secondary box does not contain the path `/var/phion/spool/mgw/<server>_<service>/spool`, for example because you changed to a different directory, repeat Step 1.

Now remove all mails in the current directory using the following command within the `/spool/` directory of the secondary box:

```
rm * -f
```

### Attention:

Usage of this command removes all files in the current directory irrecoverably. Make sure that you have not changed to another directory before entering `rm * -f`.

### Note:

If Step 4, page 385, was performed, it is necessary to remove obsolete mails also from the `/vscan/` directory.

## Step 7 Exit

Enter the command `exit` to terminate the SSH session.

This concludes the e-mail synchronisation after HA handover.





# phion management centre

<b>1.</b>	<b>Overview</b>	
1.1	General .....	389
<b>2.</b>	<b>Management Trust Centre</b>	
2.1	Certificates and Keys .....	390
2.2	MCs Trust Centre Model .....	391
<b>3.</b>	<b>Installing an MC</b>	
3.1	Configuring the Box .....	393
3.2	Installing the Licenses .....	394
<b>4.</b>	<b>MC User Interface</b>	
4.1	General .....	395
4.2	Standard Context Menu .....	395
<b>5.</b>	<b>MC Control Centre</b>	
5.1	General Characteristics of the Graphical Interface .....	396
5.2	Status Map Tab .....	397
5.3	Favourites Tab .....	398
5.4	Configuration Updates Tab .....	398
5.5	File Updates Tab .....	400
5.6	Sessions Tab .....	400
5.7	Floating Licenses Tab .....	400
5.8	Statistics Collection Tab .....	401
5.9	Box Execution Tab .....	401
5.10	Scanner Versions Tab .....	405
5.11	Software Update Tab .....	405
5.12	Update Tasks Tab .....	408
<b>6.</b>	<b>MC Configuration Service</b>	
6.1	General .....	410
6.2	Multi-Range .....	410
6.3	Global Settings .....	411
6.4	Range Configuration .....	416
6.5	Cluster Configuration .....	417
6.6	Box Configuration .....	419
6.7	Defining Node Properties .....	420
6.8	Repositories .....	421
6.9	Multiple Releases .....	421
6.10	Adding/Moving/Copying .....	424
6.11	Supplement - Configuring the Cascaded Firewall (cfirewall) .....	425
6.12	Supplement: Migration of an MC to a New Segment .....	428
<b>7.</b>	<b>MC Database</b>	
7.1	Database User Interface .....	431
7.2	Range Tab .....	431
7.3	Cluster Tab .....	431
7.4	Box Tab .....	431
7.5	Server Tab .....	431
7.6	Service Tab .....	431

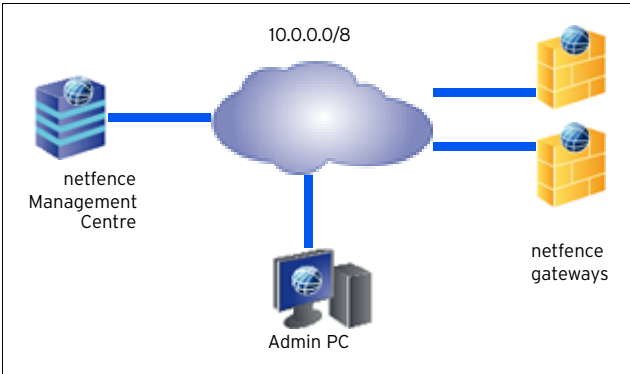
<b>8.</b>	<b>MC Admins</b>	
8.1	Introduction .....	432
8.2	Concept .....	432
8.3	Admin User Interface .....	433
<b>9.</b>	<b>MC Statistics</b>	
9.1	Service Configuration .....	436
9.2	Data Collection Configuration .....	437
9.3	Compression Cooking and Deletion .....	438
9.4	Transfer Settings .....	440
9.5	Recovery and State Analysis of Poll Sessions .....	442
<b>10.</b>	<b>MC Eventing</b>	
10.1	Example .....	443
10.2	Event User Interface .....	444
10.3	Event Configuration .....	444
10.4	Event Propagation .....	445
<b>11.</b>	<b>MC Syslog</b>	
11.1	Overview .....	446
11.2	Installing .....	447
11.3	Configuring .....	447
11.5	Supported Ciphers and Cipher Preference by the Stunnel-based Sub-processes .....	453
11.6	Filtering Policy .....	453
11.7	Example Configurations for Syslog Proxy and MC Syslog Server .....	454
<b>12.</b>	<b>MC Firewall Audit Viewer</b>	
12.1	General .....	457
12.2	<b>Activation</b> .....	<b>458</b>
12.3	<b>Limitations</b> .....	<b>458</b>
<b>13.</b>	<b>MC PKI</b>	
13.1	Installing and Configuring phion PKI .....	459
13.2	User Interface .....	459
13.3	Working with PKI .....	460
<b>14.</b>	<b>MC Firewall</b>	
14.1	General .....	464
<b>15.</b>	<b>VPN GTI</b>	
15.1	User Interface .....	464
15.2	Configuration .....	466
<b>16.</b>	<b>netfence VPN world</b>	
16.1	General .....	471
16.2	MC Settings .....	471
16.3	Requirements .....	471
16.4	netfence VPN world Settings .....	471
16.5	User Interface .....	472
16.6	Troubleshooting .....	472
<b>17.</b>	<b>MC RCS</b>	
17.1	Activating / Configuring RCS .....	473
17.2	Using RCS .....	474
17.3	Retrieve Versions .....	476
<b>18.</b>	<b>MC Reporter</b>	
18.1	General .....	477

# 1. Overview

## 1.1 General

The phion management centre (MC) is designed to manage a number of netfence gateways.

**Fig. 18-1** Schematic view of a phion netfence topology with a management centre

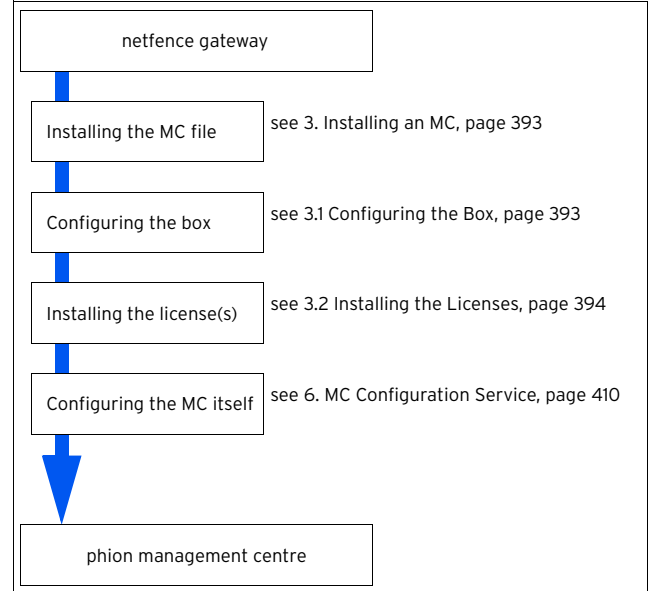


The MC itself uses the netfence platform as its basic layer. With the operative systems it shares the layer structure **Box - Server - Service**. On an MC several services are available/required:

**Table 18-1** management centre services overview

Software Module	Annotation	Comment
MC-Conf (rangeconf)	configuration module	necessary service
MC-Event (mevent)	event module	recommended service, needed for centralised event collection
MC-VPN (mastervpn)	VPN server for remote management	necessary service for remote managed systems (for example via internet)
MC-StatView (qstatm)	statistics viewing module	optional service, not available for the MC entry edition
MC-StatCollect (dstatm)	statistics collector module	optional service, not available for the MC entry edition
MC-PKI (pki)	Certificate Authority for creating X509 certificates	optional service, not available for the MC entry edition
MC-Log (msyslog)	MC Syslog Server	optional service, not available for the MC entry edition
DNS (dns)	DNS server	the same service as on almost all netfence gateways
Firewall (firewall)	Forwarding Firewall Service	recommended service if you have remote managed systems (for example via internet)

**Fig. 18-2** Flowchart - How a netfence gateway becomes a management centre



## 2. Management Trust Centre

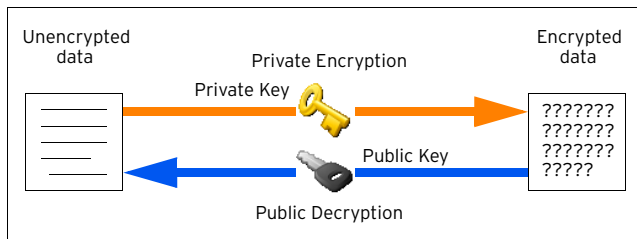
### 2.1 Certificates and Keys

X509 certificates and RSA Private/Public key pairs are used to obtain peer (IP address) and administrator authenticity. For private/public key encryption two possible encryption methods exist:

#### 2.1.1 Private Encryption

Private Encryption is used for Signatures and Authentication Checks.

Fig. 18-3 Certificates and Keys - Private Encryption

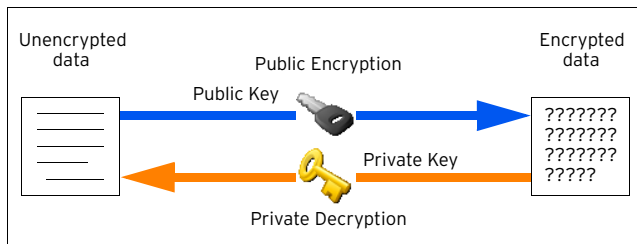


The public key owner can check if the data was encrypted with the matching private key, which is a proof of authenticity.

#### 2.1.2 Public Encryption

Public Encryption is used for challenge/response and privacy protection.

Fig. 18-4 Certificates and Keys - Public Encryption



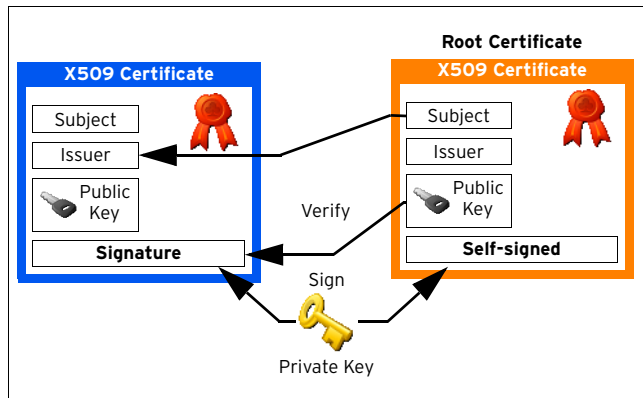
Only the private key owner can successfully decrypt the data. This way data can be transferred safely without a third party watching. This method can also be used for a challenge/response authenticity check: Public encrypt a random character sequence; send it to your partner; if the partner is capable to send back the original sequence you may assume that he is in possession of the private key.

#### 2.1.3 X509 Certificates

X509 Certificates are used to combine keys with additional credential information.

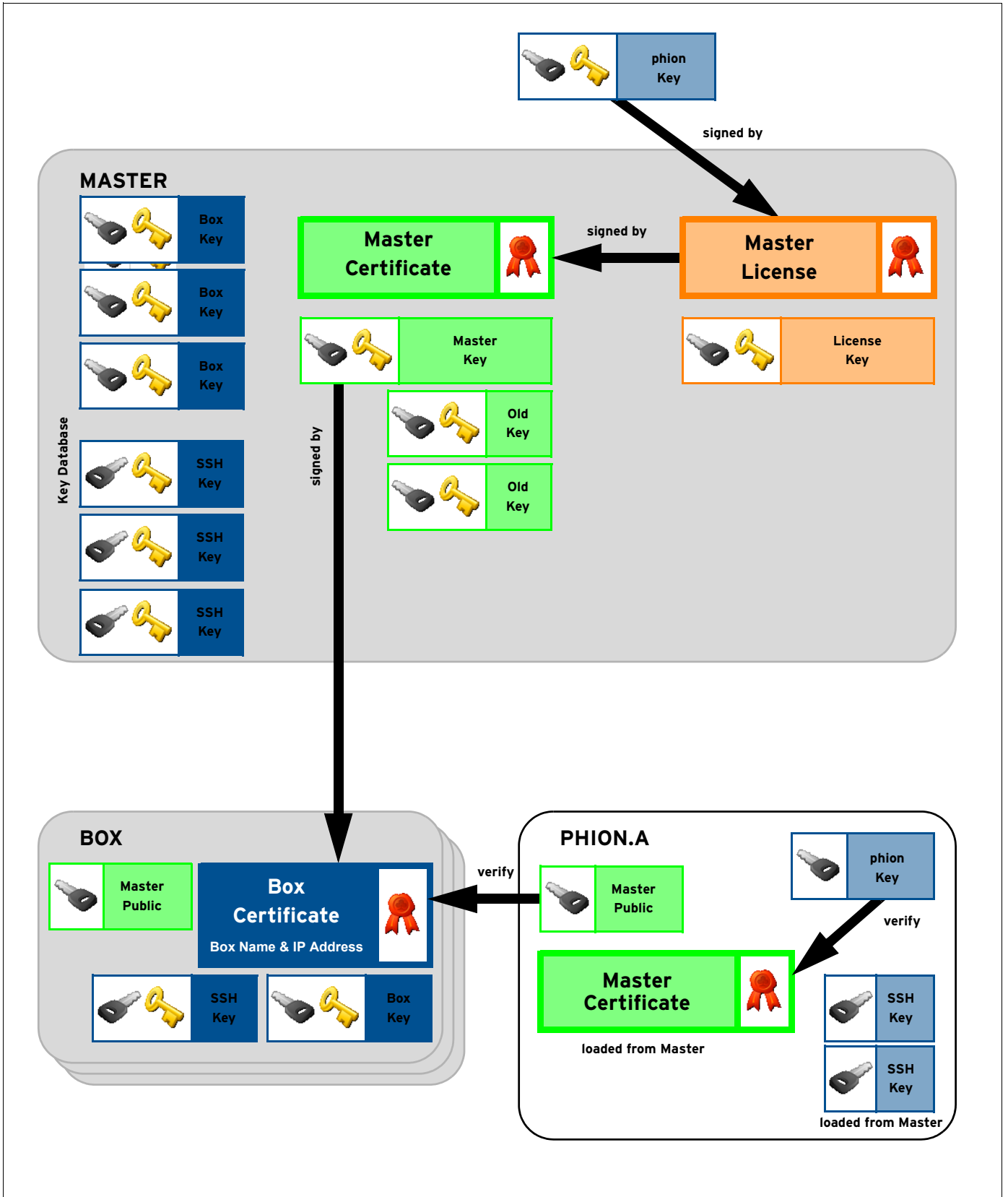
They give information of the origin and the intended usage of the public key they contain. Furthermore X509 certificates can be chained together building a **trust chain**.

Fig. 18-5 Certificates and Keys - X509 Certificates



## 2.2 MCs Trust Centre Model

Fig. 18-6 MC trust centre



With the use of X509 certificates and private/public RSA keys the following security features are obtained:

- **Secure Box- Master Communication**  
Box and Master exchange their public keys which are used for all SSL communication between the two (Strong Peer Authentication).
- **Secure Master Administration**  
When using the phion.a, the master credentials can be checked to assure that the administrative tool is really communicating with the intended management centre.
- **Secure Box Administration**  
Once a secure connection to the management centre has been established and the master certificate has been stored, all communication to the managed boxes can be verified by means of a trust chain.
- **Secure Box SSH Login**  
The master holds a database with the box SSH public keys, which can be downloaded using the phiona. This way trusted SSH login is achieved.

## 2.2.1 Authentication Levels for Master-box Communication

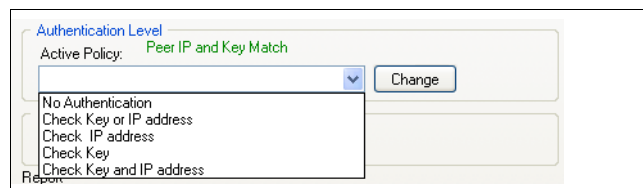
As stated above the master-box trust relationship is governed by private/public key technology. Hence in a working environment the master knows its boxes and the boxes recognise the master as their one and only reign.

The default level of authentication is that a box and its master identify themselves by their keys and IP addresses. That means that the master does not send any configuration data to untrusted boxes and no box accepts data from an untrusted master. If, however, the management centre does not have a valid license (and hence no master certificate) or major migrations are made, it may be necessary to soften the level of authenticity for a short time to establish a new trust relationship. Depending on which component is the untrusted one this has to be done either on the management centre (master **Control** window - **Configuration Updates** tab - **Untrusted Update** checkbox selected) or on the box itself to make it accept the incoming data.

**Table 18-2** Possible settings of authentication levels on the box itself

Setting	Meaning and effect
No Authentication	level -1: anything goes. The system allows any attempt to send or fetch configuration data. <b>Note:</b> Use only if necessary and change back as soon as possible.
Check IP address or key	level 0: Login is accepted if either IP address or the key challenge is successful. Still quite insecure.
Check IP address	level 1: Login is accepted if demanded IP address is at hand. Still quite insecure.
Check key	level 2: Login is accepted if key challenge is successful.
Check IP address and key	level 3: This is the default setting and should remain as such if there is no need to lower the security level temporarily.

**Fig. 18-7** Extract from the Box tab in the Box Control window where authentication level can be lowered to interaction-free authentication



### Note:

Since the phion.a uses the same communication protocol as the master, this setting applies to any phion.a based login attempt with the user **master**.



### 3. Installing an MC

Selecting *managementcenter/standard-hardware* in the Box Type Settings when creating the kickstart disk via phion.i (**Getting Started** - 2. phion.i, page 10) installs the MC automatically.

#### 3.1 Configuring the Box

To configure the management centre services use the phion.a administration tool (available on the Application&Documentation CD) and login to the box config daemon.

Proceed as follows to set up the management centre services:

##### Step 1 Create a server

The actions required for creating a server are identical to the ones described in **Configuration Service** - 3. Configuring a New Server, page 94. The **Product Type** field in **Virtual Server Definition** differs from the one in regular boxes though:

List 18-1 Server configuration - Virtual Server Definition on MC boxes - section Virtual Server Definition

Parameter	Description
<b>Product Type</b>	Each product type allocates a specific range of services ( <b>Getting Started</b> - 2.5 phion Multi-Platform Product Support, page 16). The product type chosen in this place determines, which MC-services will be available for creation. Choose the product type matching your purchased license.

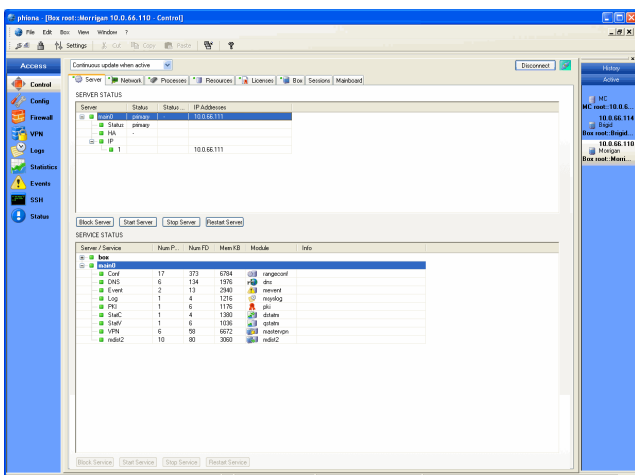
##### Step 2 Create the required services

To install the required services, simply follow the instructions given in **Configuration Service** - 4. Introducing a New Service, page 97, and select the services described in 1. Overview, page 389, as **Software Module**.

After finishing the configuration by clicking **OK**, the new configuration has to be activated by clicking **Activate**.

To verify the installation, select **Control** from the box menu and check whether the created services are running (figure 18-8).

Fig. 18-8 Control - Server tab with required/recommended MC services



You can also have a look at the log files of the modules that you just have introduced.

The log entries for a typical service start-up look similar to the following example:

Table 18-3 Example - Log file of a System Startup

Time	Type	Message
2002 07 16 09:04:21	Info	----- Configd Startup type=3 version=2.2.5.7 -----
2002 07 16 09:04:24	Notice	Server Configuration changed-----
2002 07 16 09:04:24	Notice	1st Server IP: 10.0.8.35
2002 07 16 09:04:24	Notice	2nd Server IP:
2002 07 16 09:04:24	Notice	-----
2002 07 16 09:04:24	Notice	Service Configuration changed-----
2002 07 16 09:04:24	Notice	Service Bind: 10.0.8.35
2002 07 16 09:04:24	Notice	-----
2002 07 16 09:04:24	Notice	Box Configuration changed-----
2002 07 16 09:04:24	Notice	Box Bind IP: 10.0.8.111
2002 07 16 09:04:24	Notice	-----
2002 07 16 09:04:24	Info	Listen on 10.0.8.35:810
2002 07 16 09:04:24	Info	Listen on 10.0.8.111:810
2002 07 16 09:04:24	Info	Starting Process ConfigUpdate
2002 07 16 09:04:24	Info	Starting Process Status Daemon
2002 07 16 09:04:24	Info	Starting Process Exec Daemon

Depending on the configuration of your management centre, one, more or all of the following processes are running on your system (figure 18-8).

To find out which processes are running, use the box menu entry **Control** and open the **Processes** tab. There, all running processes are listed.

Now the management centre has its basic setup and is ready to receive the licenses.

## 3.2 Installing the Licenses

Before you can use your management centre in productive service, you first have to install the obtained licenses on your system. Otherwise the software will remain in demo mode and will be open to anyone to manage it.

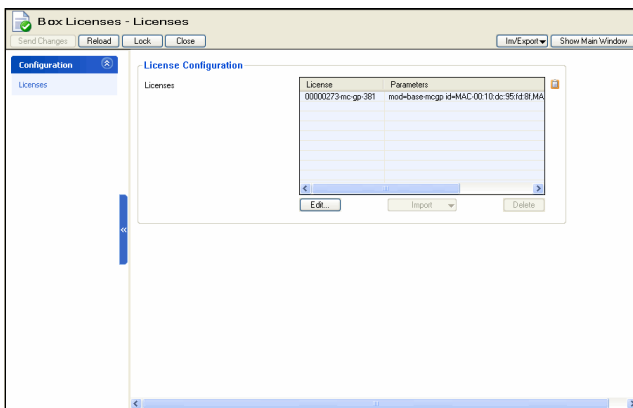
Installing licenses is done in the following steps:

### Step 1 Install the Box License

Log into the management centre box (actuate **Box** button of the phion.a Login screen). To do so, enter the box IP address of the management centre box in the **Address** field and the correct password in the **Password** field.

To install the box license, simply select the **Config** entry from the box menu and enter **Box** > **Box Licenses**.

Fig. 18-9 Box Licenses configuration



Now lock the configuration window and click the **Import** button to select the import type (either **Import from Clipboard** or **Import from File ...**).

If the license is password protected, an additional dialogue is opened where you have to enter the password.

After clicking **Send Changes** and **Activate** the box licenses are activated.

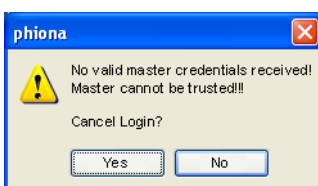
### Step 2 Install the master license also known as master identity

Login into the management centre (activate **MC** button of the phion.a Login screen).

Enter the management IP address of the management centre in the **Address** field and the correct password in the **Password** field.

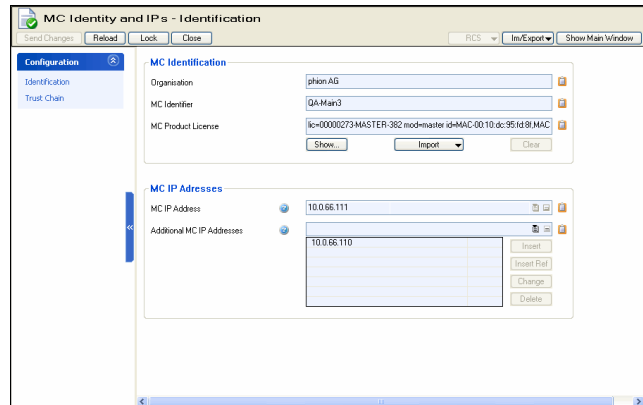
When logging into the management centre for the very first time, the message shown in figure 18-10 will appear, since the necessary MC licenses are not installed at this point. Click **NO** to continue the login procedure.

Fig. 18-10 phion.a warning when logging in without licenses



To install the master identity, simply select the **Config** entry from the box menu and enter **MC Identity** (**Multi-Range** > **Global Settings**).

Fig. 18-11 Master License configuration



Now lock the configuration window and click the **Import** button belonging to the **MC License** field and select an import type (either **Import from Clipboard** or **Import from File ...**).

If the license is password protected, an additional dialogue is opened where you have to enter the password.

After importing the license you have to perform additional setup steps to complete the Master ID configuration:

Enter a company name and edit the information of the master certificate by clicking **Edit** in the Master Certificate section of this window.

Furthermore you have to generate or import a new Master Private Key and a Master SSH Key.

After clicking **Send Changes** and **Activate** the Master ID is activated.

### Step 3 Install pool licenses

To install a pool license, simply select the **Config** entry from the box menu and enter **Pool Licenses** (**Multi-Range** > **Global Settings**).

Now lock the configuration window and click the **Import** button to select the import type (either **Import from Clipboard** or **Import from File ...**).

If the license is password protected, an additional dialogue is opened where you have to enter the password.

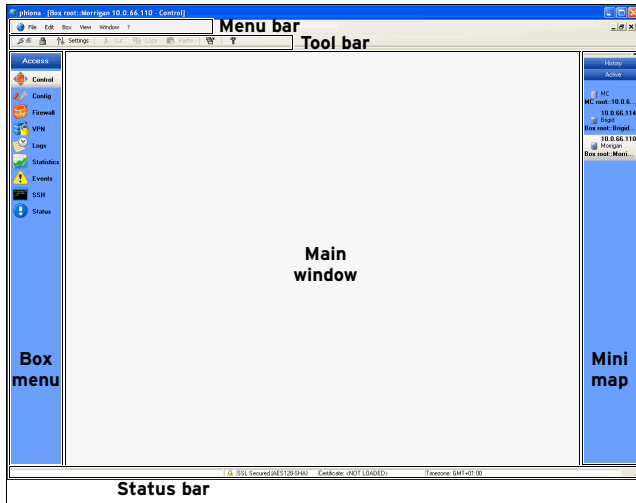
After clicking **Send Changes** and **Activate** the Master ID is activated.

## 4. MC User Interface

### 4.1 General

When logging into a management centre (by using the **MC** tab of the phion.a login screen), you will notice that the user interface slightly differs from the one of a netfence gateway (**Getting Started** - 3.2 User Interface, page 17).

Fig. 18-12 MC user interface - Overview



As it can be seen in figure 18-12, the differences are in the Menu bar and in the Box menu. However, the options that are available via these menus have the same effect.

- **Control** - see 5. MC Control Centre, page 396
- **Config** - see 6. MC Configuration Service, page 410
- **Database** - see 7. MC Database, page 431
- **Statistics** - see 9. MC Statistics, page 436
- **Event** - see 10. MC Eventing, page 443
- **PKI** - see 13. MC PKI, page 459

### 4.2 Standard Context Menu


Right-clicking in any tab of the control centre generally opens a context menu with the following entries:

- **Search for Text**  
Through this entry a window is started to define a search text that all entries of this certain view are searched for.  
The buttons **Previous** and **Next** allow you to navigate between the found entries. Clicking the button **Close** closes the dialogue.
- **Export List to Clipboard**  
Via this entry all entries of the current list are copied to clipboard.
- **Export Selected to Clipboard**  
This command copies only the selected entries to clipboard.
- **Print List**  
Prints all entries of the current view.
- **Print Preview List**  
This entry starts a print preview from where the print process can be started.
- **Print Selected List**  
This entry prints only the selected entries.
- **Print Preview Selected List**  
This entry starts a print preview from where the print process can be started.

**Note:**

If another context menu is displayed, either additionally or exclusively, it will be described in the corresponding section of this Administration Guidance.

## 5. MC Control Centre

The MC Control Centre, amongst other things, provides real-time information about all netfence gateways the management centre administers. To access it, click  **Control** in the box menu.

The following tabs are available for operational purposes:

- Status Map Tab, see 5.2 Status Map Tab, page 397
- Favourites Tab, see 5.3 Favourites Tab, page 398
- Configuration Updates Tab, see 5.4 Configuration Updates Tab, page 398
- Sessions Tab, see 5.6 Sessions Tab, page 400
- Floating Licenses Tab, see 5.7 Floating Licenses Tab, page 400
- Statistics Collection Tab, see 5.8 Statistics Collection Tab, page 401
- Box Execution Tab, see 5.9 Box Execution Tab, page 401
- Software Update Tab, see 5.11 Software Update Tab, page 405
- Update Tasks Tab, see 5.12 Update Tasks Tab, page 408

### 5.1 General Characteristics of the Graphical Interface

Especially for management centres administering a huge number of boxes, it is desirable that data sets can be arranged in such a way that the most wanted information catches the eye. Giving consideration to these needs, the MC Control Centre incorporates several sortation mechanisms.

To simplify matters, the main characteristics regarding arrangement and ordering of data in the various tabs, will be described together in this chapter. Characteristics exceeding the description in this place are positioned in the respective chapter itself.

#### 5.1.1 Title Bar(s)

##### ➤ Changing the column sequence

Information situated in the main window of each operational tab is captioned with a title bar. The data sets themselves are arranged in columns. The column sequence may be adjusted to personal needs either by using the standard context menu (see 4.2 Standard Context Menu, page 395) or by dragging and dropping the respective column to another place.

##### ➤ Ordering data sets

Data sets may be arranged ascending or descending respectively by clicking into the column labelling of a title bar. The information may not only be sorted alphabetically, but also with regard to a specific status.

#### 5.1.2 Context Menu Entries

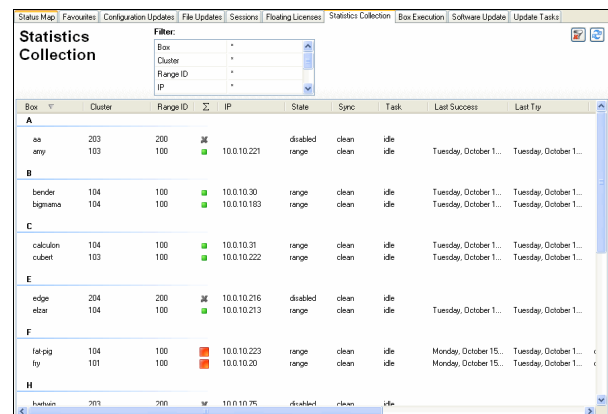
- Right-clicking into any configuration area without selected item, makes the standard context menu available through the menu item **Tools** (see 4.2 Standard Context Menu, page 395).

- A menu item **Arrange Icons By** is included in every operational tab. This menu item always contains the column headings of each specific section as sub-items and allows ordering data sets by checking the corresponding label.

In some places the **Arrange Icons By** sub-menu contains further parameters allowing more differentiated ordering (for example Configuration Updates tab, see 5.4.3.1 Context Menu, page 399).

The **Arrange Icons By** menu sometimes contains an additional value **Show in Groups** that allows switching between two views, the classical view, a continuous list, or a list combining groups of elements.

**Fig. 18-13** Group view of elements in the Statistics Collection tab, sorted alphabetically by box name




Box	Cluster	Range ID	IP	State	Sync	Task	Last Success	Last Try
<b>A</b>								
es	203	200	10.0.10.221	disabled	clean	idle	Tuesday, October 1...	Tuesday, October 1...
any	103	100	10.0.10.183	range	clean	idle	Tuesday, October 1...	Tuesday, October 1...
<b>B</b>								
bender	104	100	10.0.10.30	range	clean	idle	Tuesday, October 1...	Tuesday, October 1...
bigname	104	100	10.0.10.183	range	clean	idle	Tuesday, October 1...	Tuesday, October 1...
<b>C</b>								
calculum	104	100	10.0.10.31	range	clean	idle	Tuesday, October 1...	Tuesday, October 1...
cubet	103	100	10.0.10.222	range	clean	idle	Tuesday, October 1...	Tuesday, October 1...
<b>E</b>								
edge	204	200	10.0.10.216	disabled	clean	idle	Tuesday, October 1...	Tuesday, October 1...
elbar	104	100	10.0.10.213	range	clean	idle	Tuesday, October 1...	Tuesday, October 1...
<b>F</b>								
fatpig	104	100	10.0.10.223	range	clean	idle	Monday, October 15...	Tuesday, October 1...
fly	101	100	10.0.10.20	range	clean	idle	Monday, October 15...	Tuesday, October 1...
<b>H</b>								
harden	201	200	10.0.10.76	disabled	clean	idle	Tuesday, October 1...	Tuesday, October 1...

- Some operational tabs provide **"action" bars** with buttons meant to execute specific actions (for example Configuration tab, see 5.4.2 "Action" Bars, page 399). If such action bars are present, their buttons are included into the context menu as well.

- If present, the information displayed in a tab can generally be refreshed by using the menu items **Refresh**, **Update List** or **Update Lists**.

#### 5.1.3 Filter Settings

Some tabs are equipped with the option of setting filters to narrow down the view. Filters may be applied to each available column. By default, all columns are marked with an asterisk (\*), which stands for a character string of any length. Click the **Enter** key or click the  **Update List** button to refresh the view after having defined a filter. As soon as a filter applies the filtered value is displayed highlighted in yellow and the filter is flagged with an

exclamation point. Click the **Reset** button to remove filter settings.

Fig. 18-14 Floating Licenses tab showing licenses supplied for all boxes

License	Box	Cluster	Run...	Last (days)	Success (days)	Gra
00000273-NF-100-182						
00000273-NF-100-182...	Bart	HQ	4	25 h	25 h	15
00000273-NF-100-182...	Blinky	Border	1	26 h	26 h	15
00000273-NF-100-182...	Grampa	marlin	5	3 d	3 d	15
00000273-NF-100-182...	Krusty	GLE	10	25 h	25 h	15
00000273-NF-100-182...	LISA	GLE	10	25 h	25 h	15
00000273-NF-100-182...	Lenny	Bernhard	8	3 d	3 d	15
00000273-NF-100-182...	Maggie	Border	2	25 h	25 h	15
00000273-NF-100-182...	Ned	Branch	5	3 d	3 d	15
00000273-NF-100-182...	Nelson	Remote	1	4 d	4 d	15
00000273-NF-100-182...	Otto	Branch	4	25 h	25 h	15
00000273-NF-100-182...	Patty	Bernhard	8	3 d	3 d	15
00000273-NF-100-182...	Ralph	Branch	2	25 h	25 h	15
00000273-NF-100-182...	b-laddie	c-holger	9	25 h	25 h	15
00000273-NF-100-182...	b-milhouse	c-holger	9	25 h	25 h	15
00000273-NF-100-182...	b-stefan	c-stefan	6	3 d	3 d	15
00000273-NF-100-182...	barney	c-stefan	6	27 h	5 d	15

Fig. 18-15 Floating Licenses tab only showing licenses supplied for boxes in cluster GLE

License	Box	Cluster	Run...	Last (days)	Success (days)	Gra
00000273-NF-100-182						
00000273-NF-100-182...	Krusty	GLE	10	25 h	25 h	15
00000273-NF-100-182...	LISA	GLE	10	25 h	25 h	15

A further filter option is positioned in the Configuration Updates Tab (see 5.4 Configuration Updates Tab, page 398).

## 5.2 Status Map Tab

The Status Map summarises status information of all systems administered by the MC. It divides systems into the hierarchical structure range, cluster and box. Clicking a range entry uncovers all clusters belonging to the respective range. Clicking a cluster entry uncovers all boxes belonging to the respective cluster.

Fig. 18-16 Status Map tab

Range section

Cluster section

Box section

Coloured icons depict the general state a structural entity is in. Colour coding is triggered by the severity IDs of events that have been generated on the boxes (**Eventing** -

2.1.2 Severity Tab, page 307). Colour coding implies the following:

Table 18-4 Colour coding of status icons

Icon	Description
	The system is in normal state. Only informational and notice events have been generated.
	Warnings have been generated. A check is recommended.
	Security events and errors have been generated. A check is mandatory.
	A server has been disabled.
	The system is unavailable.

The status summary in each case refers to specific system entities, which are depicted by icons in the title bars of each section. The following icons are available:

Table 18-5 Icons used in the title bars of range, cluster and box section

Icon	Description
	Disk usage ( <b>Control Centre</b> - 2.4 Resources Tab, page 36)
	Status of the processes ( <b>Control Centre</b> - 2.3 Processes Tab, page 36)
	Status of the operative-relevant event monitoring ( <b>Eventing</b> - 2.1.2 Severity Tab, page 307)
	Status of the security-relevant event monitoring ( <b>Eventing</b> - 2.1.2 Severity Tab, page 307)
	Status of the servers ( <b>Control Centre</b> - 2.1 Server Tab, page 29)
	Status of the network ( <b>Control Centre</b> - 2.2 Network Tab, page 30)
	Validity of certificates/licenses ( <b>Control Centre</b> - 2.5 Licenses Tab, page 37)
	Displays status of the box ( <b>Control Centre</b> - 2.6 Box Tab, page 38)

### 5.2.1 Context Menus

#### 5.2.1.1 Context Menu of Range/Cluster Section

For a description of the range and cluster section context menu, please see 5.1.2 Context Menu Entries, page 396.

#### 5.2.1.2 Context Menu of Box Section

For a general description of the box section context menu, please see 5.1.2 Context Menu Entries, page 396.

Furthermore, in this place right-clicking a selected box makes further menu items available allowing you to jump directly to certain areas within the selected netfence gateway.

Fig. 18-17 Box section context menu

- Launch Firewall Status for 10.0.8.113
- Launch VPN Status for 10.0.8.113
- Launch SSH for 10.0.8.113
- Launch Control for 10.0.8.113
- Launch Log for 10.0.8.113
- Launch Statistics for 10.0.8.113
- Launch Event Monitor for 10.0.8.113
- Alternative Login for 10.0.8.113...
- Add to Favourites
- Refresh
- Views
- Arrange Icons By
- Tools

The following areas are thus straightforwardly accessible from the Status Map:

- Firewall Status
- VPN status
- SSH session
- Control
- Log
- Statistics
- Event Monitor

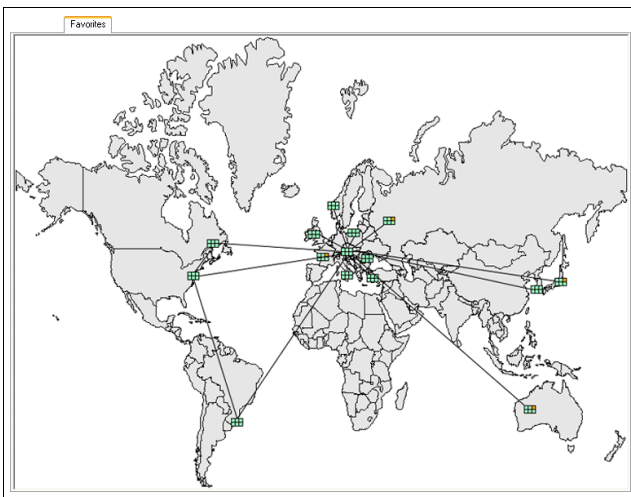
Yet another context menu entry offers the possibility to add the selected netfence gateway to the Favourites tab (menu entry **Add to Favourites**, see 5.3 Favourites Tab, page 398).

## 5.3 Favourites Tab

The Favourites tab aims at providing fast access to frequently needed netfence gateways. It contains those gateways, which have been declared as favourites in the Status Map tab (see 5.2.1.2 Context Menu of Box Section, page 397).

The used icons and colour codes are identical with the ones used in the Status Map (see 5.2 Status Map Tab, page 397).

Fig. 18-18 Example for a Favourites tab with wallpaper and small icons



### 5.3.1 Context Menus

#### 5.3.1.1 Context Menu without selected icon

Right-clicking in the **Favourites** tab without having an icon selected, opens the general context menu providing the following entries:

- **Small/Large icons**  
This entry allows changing the icon size from large (default) to small and vice versa.
- **Zoom in 10 %**  
If a bitmap is loaded as background (via entry **Choose Bitmap ...**), this entry is available and allows zooming into the graphic in 10 % steps. As soon as such a

zoom-in step is taken, the entries **Zoom out** and **Zoom 10 %** are available in order to reset the zoom level.

- **Choose Bitmap ...**

This entry enables you to load a bitmap file as wallpaper of the Favourites tab (for example a world map). This way the (for example geographical) location of netfence gateways can be depicted.

- **Remove Bitmap**

This entry is only available as long as a bitmap is loaded and allows removal of this wallpaper.

- **Export/Import Map Positions ...**

These entries allow you to export/import the positions of the icons. That means you can create a standard favourites view and send it to other administrators.

#### 5.3.1.2 Context Menu with selected icon

This menu provides about the same entries as described in 5.2.1.2 Context Menu of Box Section, page 397.

Two further menu items exist in this place:

- **Open MC Configuration**

Selecting this item effects a direct jump to the box configuration area in the configuration tree of the MC.

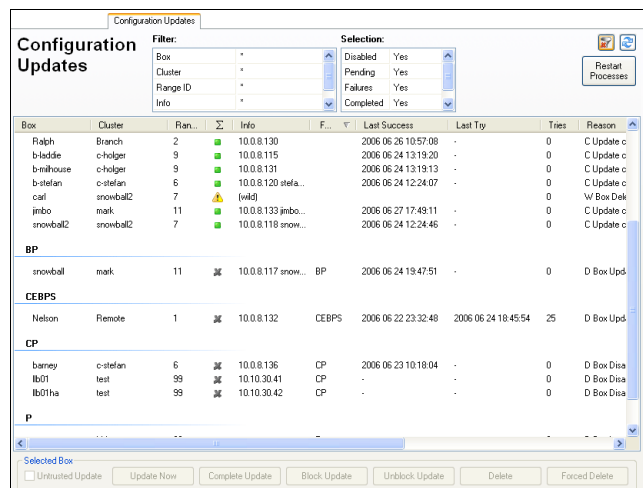
- **Remove from Favourites**

This item removes the selected netfence gateway from the Favourites tab.

## 5.4 Configuration Updates Tab

To become active, box configuration changes done on the MC have to be sent to the netfence gateway they are meant for. This is done through the **Configuration Updates** tab. This tab gives an update status overview of all available netfence gateways.

Fig. 18-19 Configuration Updates tab



Box	Cluster	Plan	Σ	Info	F...	Last Success	Last Try	Tries	Reason
flugh	branch	2	10.0.8.130			2006-06-26 10:57:08	-	0	C Update c
bradde	c-holger	9	10.0.8.115			2006-06-24 13:19:20	-	0	C Update c
b-milhouse	c-holger	9	10.0.8.131			2006-06-24 13:19:13	-	0	C Update c
b-stefan	c-stefan	6	10.0.8.120 stef...			2006-06-24 12:24:07	-	0	C Update c
carl	snowball2	7	10.0.8.133	[wld]				0	W Box Del
imbo	mark	11	10.0.8.133 imbo...			2006-06-27 17:48:11	-	0	C Update c
snowball2	snowball2	7	10.0.8.118 snow...			2006-06-24 12:24:46	-	0	C Update c
<b>BP</b>									
snowball	mark	11	10.0.8.117 snow...	BP		2006-06-24 19:47:51	-	0	D Box Upd
<b>CEBPS</b>									
Nelson	Remote	1	10.0.8.132	CEBPS		2006-06-22 23:32:48	2006-06-24 18:45:54	25	D Box Upd
<b>CP</b>									
barney	c-stefan	6	10.0.8.136	CP		2006-06-23 10:18:04	-	0	D Box Disa
lb01	test	99	10.10.30.41	CP		-	-	0	D Box Disa
lb01ha	test	99	10.10.30.42	CP		-	-	0	D Box Disa
<b>P</b>									

As shown in figure 18-19, the display is built up of an update status listing of all netfence gateways managed by the management centre in the main window, and of two "action" bars on top and on bottom of it respectively.

The current status is indicated by an icon in the **Σ (Box Icon)** column and by characters in the **Flags** column (see



5.4.3 Listing, Box / Cluster / Range ID columns and Flags column, page 399).

### 5.4.1 Filter Settings

➤ **Selection** (*Disabled/ Pending/ Failed/ Completed/ Wild*)  
 By default all filters except "**Disabled**" are set to **yes**. Setting a filter to **no** excludes the corresponding boxes from the view in the main window's listing. As soon as a filter applies the filtered value is displayed highlighted in yellow and the filter is flagged with an exclamation point. Click the **Reset** button to remove filter settings.

### 5.4.2 "Action" Bars

The items in the upper "action" bar are applicable to all existing boxes in the main window's listing.

➤ Clicking **Restart Processes** restarts the update processes manually.

The items in the lower "action" bar are applicable to all selected boxes in the main window's listing. They have the following functions:

➤ **Untrusted Update** checkbox enables the update of boxes that are not known to the management centre. Untrusted updates can as well be used on boxes, in case problems with authentication keys arise.

**Attention:**  
 Untrusted updates are very hazardous, since they work without strong authentication.

The **Untrusted Update** option only works on boxes that accept non-authenticated connections. On a netfence gateway, such a situation could arise after disaster recovery using an old .par file or after installation from scratch.

- **Update Now** triggers immediate box update execution.
- **Complete Update** triggers sending of the entire box configuration to the box and not only of the modified part of it.
- **Block Update** disables the possibility to perform a box update.
- **Unblock Update** enables scheduling of updates.
- **Delete** updates which can no longer be applied, that means updates allotted to boxes, which have been removed from the MCs configuration tree and have thus been marked as "wild".
- **Force Delete** deletes configuration updates of active boxes.

### 5.4.3 Listing

The listing in the main window, displays the configuration status of all available boxes administered by the management centre.

The listing is divided into the following columns:

➤ **Box / Cluster / Range ID** columns  
 These data sets describe the membership of the netfence gateway, that means its name and the names of cluster and range it belongs to.

➤  $\Sigma$  (**Box Icon**) column  
 A status icon follows the box labelling. Status icons have the following signification:

**Table 18-6** Icons used in the Configuration Updates tab

Icon	Description
	Box updates have been disabled.
	The box is in state pending, that means an update is actively performed.
	At least the last update, possibly even multiple updates have failed on this box.
	The update process has completed successfully.
	Updates no longer apply, because the box has been deleted from MCs configuration tree. The update status has been set to <i>wild</i> . Wild updates can be deleted from the listing with the <b>Delete</b> button in the "Action" bar.

➤ **Info** column  
 This column displays the IP address and name of the netfence gateway. The information (**wild**) flags update settings of nonexistent boxes.

➤ **Flags** column  
 The update status can be verified in the Flags column. The following flags exist:

**Table 18-7** Update Status flags overview

Flag	Description	Comment
<b>C</b>	Complete Update	A full update with the complete configuration has been applied.
<b>E</b>	Update Error	Last update was not successful.
<b>F</b>	Force Update	The last update has been forced therewith overriding the internal scheduler.
<b>U</b>	Untrusted Update	Box and MC have not exchanged authentication data, and thus have not approved trustworthiness.
<b>T</b>	Update Terminated	Update has terminated.
<b>B</b>	Update Blocked	Updates are blocked.
<b>P</b>	Update Pending	PAR file is ready to be sent.
<b>S</b>	Update Scheduled	Update has been scheduled.
<b>A</b>	Update Active	Update process is active.

➤ **Last Success** column  
 This column informs about date and time of the last successful configuration update (the used syntax is yyyy mm dd hh:mm:ss).

➤ **Last Try** column  
 This column informs about date and time of the last attempt to update a configuration (the used syntax is yyyy mm dd hh:mm:ss).

➤ **Tries** column  
 Here the number of attempts to update the configuration of a netfence gateway is displayed.

➤ **Reason** column  
 Here the status message is shown (for example displaying the reason for a failed update).

#### 5.4.3.1 Context Menu

For a general description of the context menu, please see 5.1.2 Context Menu Entries, page 396.

## 5.5 File Updates Tab

### Note:

See documentation **netfence entegra**.

## 5.6 Sessions Tab

The Sessions tab lists open supervising sessions on the boxes it administers. The data displayed in this place is similar to the information shown in the Sessions tab available on each box itself (**Control Centre - 2.7 Sessions Tab**, page 40).

### Note:

The Sessions tab does not show configuration sessions, which for example are produced by locking configuration nodes, ... To find out about active configuration sessions use the **Sessions ...** button in the **Config** section.









The following button is available in the upper "action" bar:

#### ➤ Kill Session button

Clicking this button terminates the selected session.

The listing is divided into the following columns:

**Table 18-8** Session types overview

Column	Description
<b>Box</b>	This is the name of the netfence gateway.
<b>Cluster</b>	This is the name of the cluster the box resides in.
<b>Range ID</b>	This is the name of the range cluster and box belong to.
<b>Service Icon</b>	The icons describe the service responsible for the session: <ul style="list-style-type: none"> <li> Firewall control session (Service <code>firewall_</code>)</li> <li> Login session</li> <li> VPN session (Service <code>vpnserver_*vpn</code>)</li> <li> Log viewer session (Service <code>box_logd</code>)</li> <li> Statistics viewer session (Service <code>box_qstated</code>)</li> <li> Box control session (Service <code>box_control</code>)</li> <li> phion.a session (Service <code>phiona</code>)</li> <li> indicates a sync operation</li> </ul>
<b>IP</b>	This is the IP address of the netfence gateway.
<b>Info</b>	This is the optional box description as inserted into the Description field of the <b>Box Config</b> file.
<b>Service</b>	This is the name of the service that has been accessed.
<b>Peer</b>	This is the IP address from where the session was started.
<b>Admin</b>	This is the name of the administrative account that has logged in.
<b>Start</b>	This is the period that has passed since the session has started.
<b>PID</b>	This is the internal, unique <b>Process ID</b> .

Double-clicking an entry opens a detail window summarising all available information regarding the specific session.

### 5.6.1 Context Menu

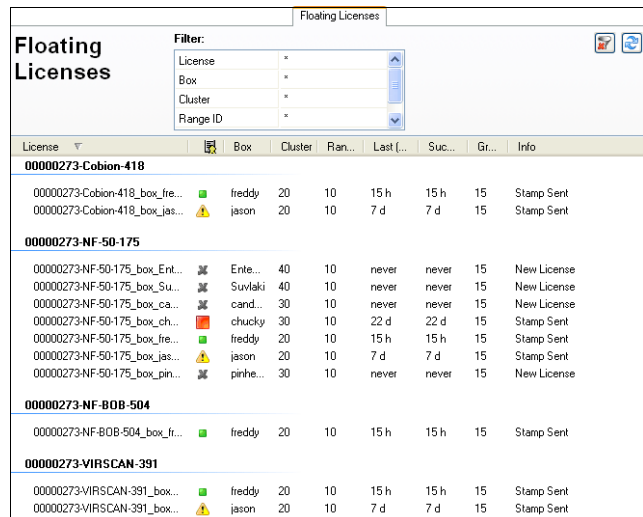
For a general description of the context menu, please see 5.1.2 Context Menu Entries, page 396.

## 5.7 Floating Licenses Tab

The **Floating Licenses** tab displays a listing of all licenses it supplies for its MC-administered boxes.

Double-click an entry to open a detail window summarising all available information regarding the specific license.





**Fig. 18-20** Floating Licenses tab



License	Box	Cluster	Ran..	Last [..	Suc...	Gr..	Info
<b>00000273-Cobion-418</b>							
00000273-Cobion-418_box_fre...	freddy	20	10	15 h	15 h	15	Stamp Sent
00000273-Cobion-418_box_jas...	jason	20	10	7 d	7 d	15	Stamp Sent
<b>00000273-NF-50-175</b>							
00000273-NF-50-175_box_Ent...	Erle...	40	10	never	never	15	New License
00000273-NF-50-175_box_Su...	Suvlaki	40	10	never	never	15	New License
00000273-NF-50-175_box_ca...	cand...	30	10	never	never	15	New License
00000273-NF-50-175_box_ch...	chucky	30	10	22 d	22 d	15	Stamp Sent
00000273-NF-50-175_box_fre...	freddy	20	10	15 h	15 h	15	Stamp Sent
00000273-NF-50-175_box_jas...	jason	20	10	7 d	7 d	15	Stamp Sent
00000273-NF-50-175_box_pin...	pinthe...	30	10	never	never	15	New License
<b>00000273-NF-808-504</b>							
00000273-NF-808-504_box_fr...	freddy	20	10	15 h	15 h	15	Stamp Sent
<b>00000273-VIRSCAN-391</b>							
00000273-VIRSCAN-391_box...	freddy	20	10	15 h	15 h	15	Stamp Sent
00000273-VIRSCAN-391_box...	jason	20	10	7 d	7 d	15	Stamp Sent

The listing is divided into the following columns:

**Table 18-9** Data listed in the Floating Licenses tab

Column	Description
<b>License</b>	This is the name of the pool license supplied by the MC.
<b>License Icon</b>	The license icons indicate the status of a license with regard to the last successful license verification request attempted by a box. They depict the following conditions: <ul style="list-style-type: none"> <li> Since the last successful verification request less than half the grace period has passed.</li> <li> Since the last successful verification request at least half the grace period has passed.</li> <li> Since the last successful verification request the grace period has expired. The box is either down or has lost connection to the MC. The "inactive" icon also comes into effect, when a license verification has been requested by a box, though the license is not available in the license pool on the MC. This situation might arise when a license has been imported into the box using Emergency Override.</li> <li> The MC supplies a new license that has not yet been requested by the box, for example because less than a quarter of the grace period has passed and the box has not yet had need for license verification.</li> </ul>
<b>Box</b>	This is the name of the netfence gateway.
<b>Cluster</b>	This is the name of the cluster the box resides in.
<b>Range ID</b>	This is the name of the range cluster and box belong to.
<b>Last</b>	This is the time that has passed since license verification has last been requested by the box. The following time indicators apply: <b>s</b> =seconds, <b>h</b> =hours, <b>m</b> =minutes, <b>d</b> =days, <b>never</b> . The <b>Last</b> column does not include any statement, if the verification request has been successful.
<b>Success</b>	This is the time that has passed since license verification has successfully been requested by the box. The following time indicators apply: <b>s</b> =seconds, <b>h</b> =hours, <b>m</b> =minutes, <b>d</b> =days, <b>never</b> . Successful license verification implies that the box has requested a license that has been assigned to it on the MC and thus the MC has answered the request by sending a stamp. The <b>Success</b> column does not include any statement though, if the license is actually identified as valid license on the MC-administered box itself. To review a summary of the actual license status on all boxes the MC administers, have a look at the <b>Status Map</b> tab instead (see 5.2 Status Map Tab).

**Table 18-9** Data listed in the Floating Licenses tab

Column	Description
<b>Grace</b>	This is the grace period assigned to the license.
<b>Info</b>	The Info column describes license state conditions. Amongst others, the following messages may be displayed: <ul style="list-style-type: none"> <li>➤ <b>Stamp Sent</b> The MC has obeyed the license verification request and has answered by sending a stamp.</li> <li>➤ <b>New License</b> A new license is available but has not yet been requested by a box for delivery.</li> <li>➤ <b>License not found</b> A license has been requested that does not reside in the license pool on the MC.</li> </ul>

**Note:**

To understand the context between license status and system behaviour see **Licensing - 4. System Behaviour** without or with Invalid Licences, page 503.

### 5.7.1 Context Menu

For a general description of the context menu, please see 5.1.2 Context Menu Entries, page 396.

## 5.8 Statistics Collection Tab

This tab provides information about collected statistics. Double-clicking an entry opens a detail window summarising all available information regarding the statistics collection of the specific box.

The listing is divided into the following columns:

**Table 18-10** Data listed in the Stat Collect tab

Column	Description
<b>Σ (Box Icon)</b>	This column shows the status of statistics collection based on the reason which has provoked this status. The following icons depict the following states: <ul style="list-style-type: none"> <li>■ Statistics collection works flawlessly.</li> <li>⚠ Statistics collection has been aborted.</li> <li>■ Statistics collection has been disabled.</li> </ul>
<b>Box</b>	This is the name of the netfence gateway.
<b>Cluster</b>	This is the name of the cluster the box resides in.
<b>Range ID</b>	This is the name of the range cluster and box belong to.
<b>IP</b>	This is the IP address of the netfence gateway.
<b>State</b>	Shows whether the statistics transfer configuration is based on range settings (range) or cluster settings (cluster). If no statistics transfer configuration is defined, disabled is shown.
<b>Sync</b>	Displays the status of the box synchronisation: <ul style="list-style-type: none"> <li>➤ <b>clean</b> - The synchronisation procedure has been executed correctly.</li> <li>➤ <b>dirty</b> - The synchronisation procedure has failed or is still in progress.</li> <li>➤ <b>unknown</b> - The synchronisation status cannot be determined.</li> </ul>
<b>Task</b>	Shows the currently running process (for example unknown, idle).
<b>Last Success</b>	This column informs about date and time of the last successful synchronisation (the used syntax is yyyy mm dd hh:mm:ss).
<b>Last Try</b>	This column informs about date and time of the last synchronisation try (used syntax is yyyy mm dd hh:mm:ss).
<b>Reason</b>	This column displays the status and/or error messages.

### 5.8.1 Context Menu

For a general description of the context menu, please see 5.1.2 Context Menu Entries, page 396.

## 5.9 Box Execution Tab

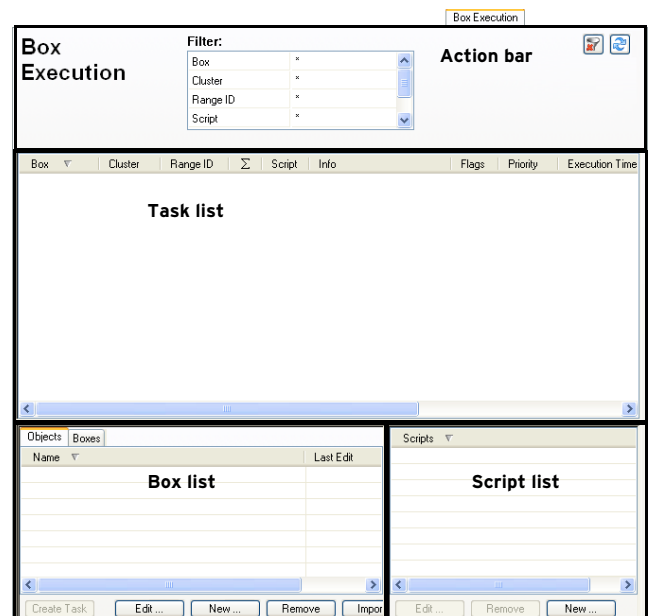
The management centre control facility allows **remote execution** of scripts and programs on selected netfence gateways. This feature can be used to execute nonrecurring tasks like removal of unwanted files or termination of processes ... on several boxes simultaneously in a single administrative step. It is thus not required to log on each netfence gateway separately.

To this end a collection of scripts is maintained at the management centre. These scripts can be edited, added and removed by the administrator. By selecting a particular script and a netfence gateway, execution of the script can be triggered. During execution all output of the script is directed to a box log file which is held at the MC and can be reviewed by the administrator after execution. Consult these files for verbose output or error logging of the script.

As shown in figure 18-21, the display is divided into four areas:

- An Action bar on top of the main window
- Task list, see 5.9.1 Task List, page 402
- Box list, see 5.9.3 Box List, page 402
- Script list, see 5.9.2 Script List, page 402

**Fig. 18-21** Box Execution tab



## 5.9.1 Task List

This list displays the status of tasks. The listing is divided into the following columns:

**Table 18-11** Data listed in the Box Execution tab

Column	Description
$\Sigma$ (Box Icon)	This column depicts the status of an executed task.
<b>Box</b>	This is the name of the netfence gateway a task has been created for.
<b>Cluster</b>	This is the name of the cluster the box resides in.
<b>Range ID</b>	This is the name of the range cluster and box belong to.
<b>Script</b>	This is the name of the script that is currently executed.
<b>Info</b>	This column lists additional information such as IP address and short name.
<b>Flags</b>	Flags depict the current task state. The following states are available: <ul style="list-style-type: none"> <li>➤ <b>F</b> - SSH failed (SSH-network connection or login failed)</li> <li>➤ <b>G</b> - Script failed (script returned a non-zero value)</li> <li>➤ <b>D</b> - Deleted (Box was removed from the MC)</li> <li>➤ <b>U</b> - Untrusted (Peer authentication check is disabled)</li> </ul>
<b>Priority</b>	This is the assigned task priority. The following priorities are available: <ul style="list-style-type: none"> <li>➤ <b>0</b> - High priority</li> <li>➤ <b>1</b> - Normal priority</li> <li>➤ <b>2</b> - Low priority</li> </ul>
<b>Execution Time</b>	This is the time the task is currently running.
<b>First Attempt</b>	This column informs about date and time when the first execution attempt was started (used syntax is <code>yyyy mm dd hh:mm:ss</code> ).
<b>Last Try</b>	This column informs about date and time when the last execution attempt was started (used syntax is <code>yyyy mm dd hh:mm:ss</code> ).
<b>Tries</b>	This is the number of execution tries.
<b>Reason</b>	This is the failure reason in case the last execution try has failed.

### 5.9.1.1 Context Menu

For a general description of the context menu, see 5.1.2 Context Menu Entries, page 396.

Additionally, the following further menu items exist in the **Task List** window:

- **Reschedule**  
If remote execution fails (box is not reachable over the network, script fails or box is untrusted) a task can be rescheduled. When doing so, time schedule, priority settings and trust level can be re-chosen.
- **Delete Task**  
Removes the selected tasks and terminates any running processes if necessary.

## 5.9.2 Script List

In this place, scripts provided for execution on boxes, can be created, modified and deleted. Use the buttons from the action menu to perform the following operations:

- **New ...**  
Click this button to create a new script. Choose a name for the script and enter a sequence of bash commands to be executed.
- **Edit ...** button  
Select a script and click this button to modify it.

- **Remove** button  
Discards a script stored on the management centre.

### Note:

A script, which can be selected together with a box or a box group object has to exist before a task can be created.

## 5.9.3 Box List

In the box list boxes or groups of boxes can be selected for task execution. Two tabs with different functions are available to do so.

### 5.9.3.1 Objects Tab

In this tab, multiple boxes can be combined to form group objects. The so-called **management centre Objects** are a permanently grouped selection of boxes. They are intended to apply the administrator with quick task creation opportunity.

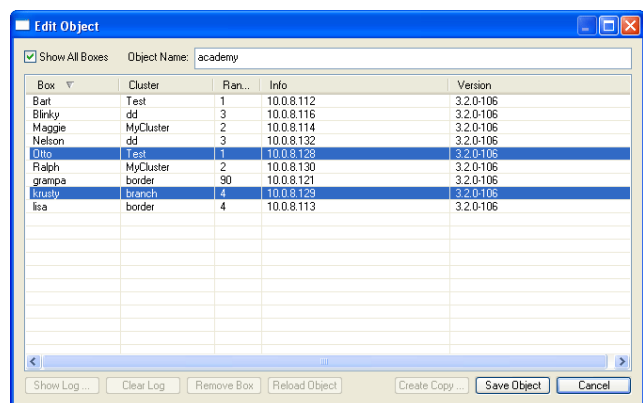
management centre Objects are saved to the Microsoft Windows System Registry on the client PC. They can be exchanged between multiple client PCs by exporting and then again importing them.

### Note:

management centre Objects created in the Box Execution tab may be used in the Software Updates tab as well and vice versa.

Click the **New ...** button in the action menu of the Objects tab in the box list to create a new management centre Object. This opens a new window enabling box selection.

**Fig. 18-22** Box List - Edit Object



**Fig. 18-23** Creating a box group object

Enter a name for the new object in the **Object Name** field. Select all desired boxes by simultaneously pressing the Shift/CTRL key and clicking a box. Then, click the **Save Object** button to save the object.

When reopening the object after it has been saved, only the selected boxes are displayed in the configuration window.

Select the **Show All Boxes** checkbox to display a view showing all available boxes. The boxes belonging to a saved object are shown highlighted.

The following buttons in the **Edit Object** window allow further actions:

**Note:**

If buttons are activated for use or not depends on the selected view (checkbox **Show All Boxes** selected or not) and if the object has already been saved.

- **Show Log ...**  
Displays a view of the box log file containing entries about the lastly executed task. Box log files are stored on the MC. Their view can as well be triggered by double-clicking a box entry in the list.
- **Clear Log**  
Clears a box log file's contents. This should be done best before executing a new task.
- **Remove Box**  
Removes the box from the saved object.
- **Reload Object**  
Refreshes the view to display boxes saved in the object only.
- **Create Copy ...**  
Creates a copy of an already saved management centre Object.

### 5.9.3.2 Boxes Tab

The Boxes tab displays a listing of all existing boxes on the management centre. A selected box is displayed highlighted. Multiple boxes can be selected by simultaneous pressing of the **Shift/CTRL** key and clicking on a box.

The following detail information is covered in the box list:

- **Box / Cluster / Range ID** columns  
These data sets describe the membership of the netfence gateway, that means its name and the names of cluster and range it belongs to.
- **Info** column  
This column displays additional box information (IP address and short name).
- **Version** column  
This is the version number of the netfence gateway installed on the box.

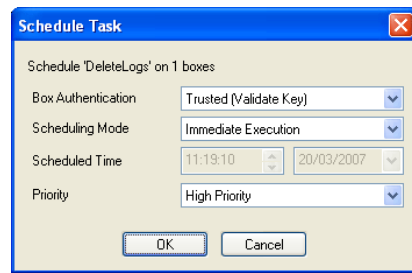
### 5.9.3.3 "Action" Bars

The following action menu applies for both tabs in the box list:

- **Create Task** button  
The **Create Task** button becomes active when a Box/Object/Script combination is chosen from the Scripts and Box lists.  
Task creation opens the Schedule Task window allowing for detailed specification when and how the task should

be executed. The following configuration values are made available:

**Fig. 18-24** Schedule Task window



**List 18-2** Schedule Task configuration

Parameter	Description
<b>Box Authentication</b>	The following two modes are available for selection: ➤ <b>Trusted (Validate Key)</b> ➤ <b>Untrusted (Ignore Key)</b> The untrusted mode enables the update of boxes that are not known to the management centre. Untrusted updates can as well be used on boxes, in case problems with authentication keys arise. Otherwise, trusted mode should always be used.
<b>Scheduling Mode</b>	By default, tasks are scheduled for <b>Immediate Execution</b> . The option <b>Delayed Execution</b> activates the parameter <b>Scheduled Time</b> below, where task execution time can be configured in detail.
<b>Scheduled Time</b>	These two fields take a scheduling time for task execution.
<b>Priority</b>	When multiple tasks are configured for execution, the priority setting determines the execution succession. The setting may be chosen from <b>Low</b> over <b>Normal</b> to <b>High Priority</b> .

The following action menu only applies for the **Boxes** tab:

- **Show Log** button  
Displays a view of the box log file containing entries about the lastly executed task. Box log files are stored on the MC. Their view can as well be triggered by double-clicking a box entry in the list.
- **Clear Log** button  
Clears the log files of all selected boxes. This should be done best before executing a new task.

The following action menu only applies for the **Objects** tab:

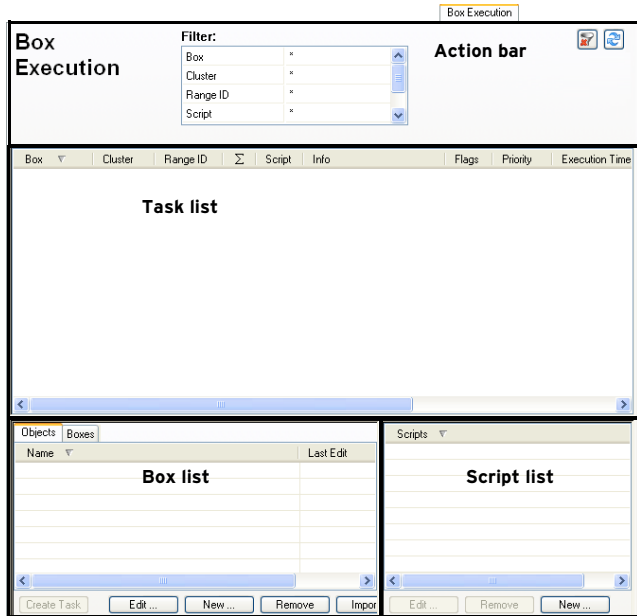
- **Edit** button  
Clicking this button allows editing a selected object.
- **New** button  
Creates a new object.
- **Remove** button  
Removes the selected object
- **Import** button  
Imports a management centre Object into the Microsoft Windows System registry.
- **Export** button  
Exports a management centre Object from the Microsoft Windows System registry. Box group objects are saved to management centre Object (\*.mco) files.



### 5.9.4 Example

For easier understanding of the procedure when taking actions via the **Box Execution** tab, have a look at the following example: The aim is to cleanup the /tmp directory on all netfence gateways.

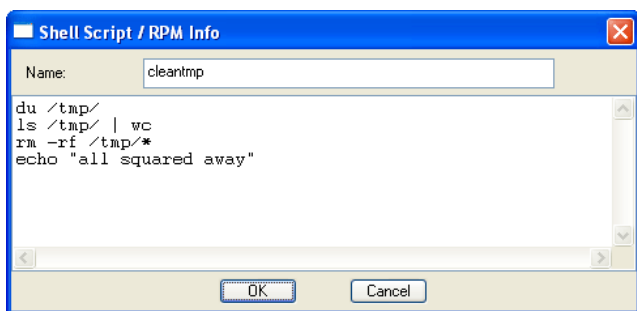
Fig. 18-25 Box Execution tab



#### Step 1 Create a new script

Click the **New** button in the Script list window, enter `cleantmp` as script name and insert the command sequence shown in figure 18-26.

Fig. 18-26 Shell Script



#### Step 2 Select the boxes and the cleantmp script

Select all boxes on the **Boxes** tab in the Box list window and the `cleantmp` script in the Script list window simultaneously.

#### Step 3 Create the tasks

Click the **Create Task** button in the Box list window.

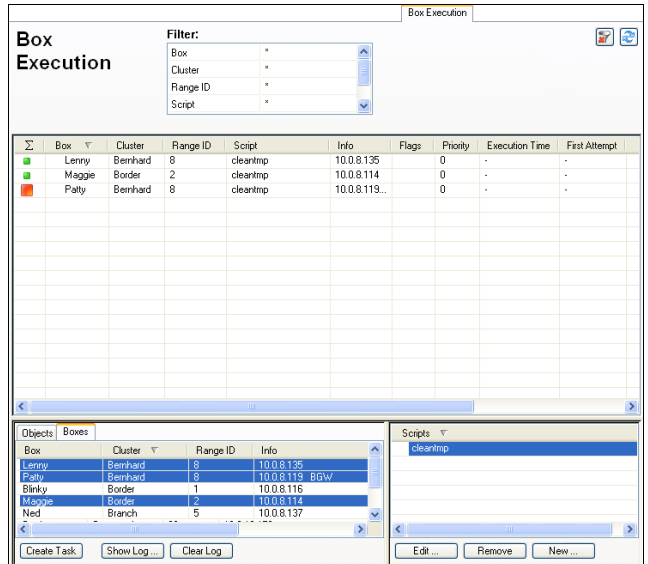
#### Step 4 Schedule the tasks

Schedule the tasks for **Immediate Execution** in the Schedule Task window.

#### Step 5 Watch the task list

The newly created tasks appear as entries with a green indicator (figure 18-27) and disappear as soon as the task is finished.

Fig. 18-27 Box Exec with tasks running

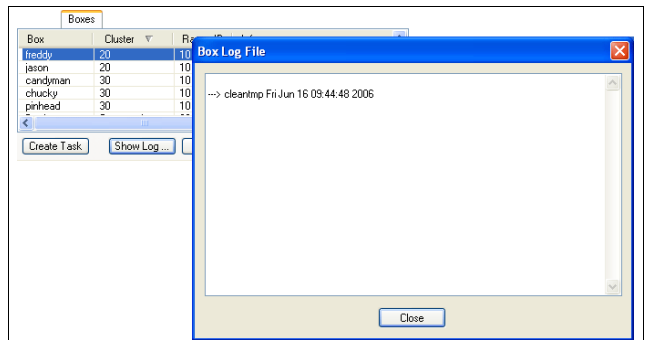


If a task fails the according entry remains in the task list and is shown with a red indicator. Have a look at the **Reason** column for an explanation of the failure.

#### Step 6 Review the log files

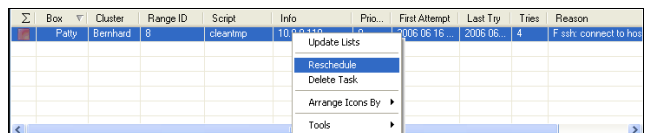
Double-click the specific netfence gateways to view the log files and check if the desired actions have been taken.

Fig. 18-28 Box log file view



#### Step 7 Reschedule or delete failed tasks

Fig. 18-29 Rescheduling of a failed task





### 5.9.5 Popular Scripts

Table 18-12 Popular Scripts

Name	Content	Function
wipeevent	rm -f /var/phion/event/evendb	clears all events from the selected netfence gateway(s) at once
relcheck	/etc/phion/bin/phionRelCheck	performs a release check on freshly installed netfence gateways
redbutton	/opt/phion/bin/phionctrl shutdown	initiates an emergency stop on the selected netfence gateway(s)

### 5.10 Scanner Versions Tab

The management centre provides a quick overview of active content scanner versions, especially in distributed environments.

The tab **Scanner Versions** gives details of the currently active Antivirus engine, Antivirus patterns or the ISS Webfilter Database (if a local Webfilter DB is configured). Of course date and time of the last successful update are available.

Table 18-13 Data listed in the columns of the Scanner Versions tab

Column	Description
<b>Box</b>	The name of the MC-administered box.
<b>Cluster</b>	The name of the cluster the box resides in.
<b>Range ID</b>	The range that the cluster and the box belong to.
<b>Server</b>	The virtual server on the box.
<b>Service</b>	The assigned service on the box.
<b>Product Version</b>	The product version communicated by the box.
<b>Engine Version</b>	The engine version communicated by the box.
<b>Packlib Version</b>	The packlib version communicated by the box.
<b>Pattern Version</b>	The antivirus pattern version communicated by the box.
<b>Last Update</b>	Date and time of the last update.

### 5.11 Software Update Tab

The Software Update tab is intended for execution of software updates on managed boxes. It is especially designed for administration of a huge number of netfence gateways with different release versions.

The handling of remote software updates is very similar to the remote execution facility described under 5.9 Box Execution Tab, page 401.

**Note:**

Valid software packages are RPM files for release updates and service packs (SP) and zipped tar files (\*.tgz archives) for software hot fixes.

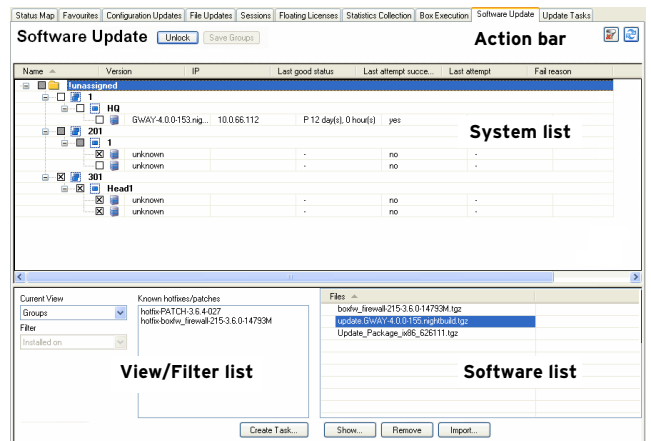
**Attention:**

Only use RPMs provided by phion. If you are for some reason forced to install an arbitrary RPM, you yourself have to make sure that the installed software is compatible with the phion components present. Hotfixes are zipped TAR files which include the package data and a script called "doit". The activation procedure simply unpacks the TAR file in a temporary directory and then calls the "doit" script within this directory. The script then copies the package file to the proper location. You can create your own hotfixes and use them to distribute files among your boxes.

The display of the Software Update tab is divided into four areas (figure 18-30):

- Action bar
- System List, see 5.11.1 System List, page 405
- View/Filter List, see 5.11.2 View/Filter List, page 407
- Software List, see 5.11.3 Software List, page 408

Fig. 18-30 Software Update tab - Groups view



#### 5.11.1 System List

In the system list, administrative entities may be arranged in views corresponding to the structure of the management centre configuration tree. Views are triggered by appropriate selection in the **Current View** list within the View/Filter list (see View/Filter List below).

Each view includes detailed information about every system the management centre administers. The detail information is arranged in the following columns. Note that not all columns are available in every view.

Table 18-14 Data listed in the system list of the Software Update tab

Column	Description
<b>Name</b>	This is the name of the MC-administered box.
<b>Cluster</b>	This is the name of the cluster the box resides in.
<b>Range</b>	This is the name of the range that the cluster and the box belong to.
<b>Group</b>	This is the name of the group the box has been assigned to.
<b>Version</b>	This is the software version installed on the box.
<b>IP</b>	This is the management IP address of the box.
<b>Last good status</b>	This is the time that has passed since the MC has fetched status information from a box successfully. netfence gateways 3.4.4 and later, and 3.6.1 and later propagate status information to the MC actively. Information that has been "pushed" to the MC by these systems is flagged with <b>P</b> in the column listing.

**Table 18-14** Data listed in the system list of the Software Update tab

Column	Description
<b>Last attempt successful</b>	This column indicates, if the last attempt to fetch status information from a box has been successful ( <b>yes/no</b> ).
<b>Last attempt</b>	If the last attempt to fetch status information from a box has been unsuccessful, this column indicates the time that has passed since then.
<b>Fail reason</b>	This column lists the reason for status information update failure.

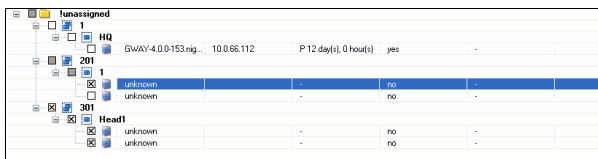
### 5.11.1.1 Views

**Note:**  
An Administrator only sees ranges, clusters, and boxes of his scope.

In the System list, MC-administered boxes may be arranged in one of the following views:

➤ **Groups**

**Fig. 18-31** Software Update tab - Groups view



The Groups view allows defining administrative groups of boxes, in order to facilitate installation of updates on boxes with similar configurations.

To access this view, select **Groups** in the **Current View** list withing the **View/Filter list**.

**Note:**  
Only a root Administrator is allowed to edit groups (create, delete& rename group).

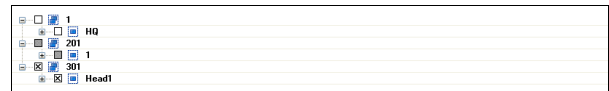
- To create a group:
  - Click the **Lock** button in the Action bar.
  - Right-click any item in the System list, select **Create Group** from the context menu and specify a group name (characters: <space> ' " and | are not allowed for group names - these characters will be replaced by an underdash (\_)).
  - Click the **Save Groups** button in the Action bar.
- To delete a group:
  - Click the **Lock** button in the Action bar.
  - Select the group in the System list, right-click and select **Remove** from the context menu. Note that the preconfigured group element **!unassigned** may not be deleted. When a group is deleted, boxes assigned to it are automatically moved to the group **!unassigned**.
  - Click the **Save Groups** button in the Action bar.
- To assign a box to a group:
  - Click the **Lock** button in the Action bar.
  - Click a box, drag it to the group it should be assigned to and drop it.
  - Click the **Save Groups** button in the Action bar.

**Note:**  
Boxes may only be assigned to **one** group.

**Note:**  
Everybody can see all groups und move his ranges, clusters, and boxes into any group.

➤ **Ranges**

**Fig. 18-32** Software Update tab - Ranges view



In the **Ranges** view, boxes are arranged in a tree structure as known from the configuration tree in the **Config** section of phion.a.

➤ **Boxes**

**Fig. 18-33** Software Update tab - Boxes view

Group	Box Name	ID	Status	Version	Last Update	Fail Reason
unassigned	Head1	1	unassigned	GWAY-4.0.0-153.nig...	10.0.66.112	P 12 day(s), 1 hour
201	box1	201	unassigned	unknown	-	-
301	box1	301	unassigned	unknown	-	-
201	box2	201	unassigned	unknown	-	-
301	box2	301	unassigned	unknown	-	-

In the **Boxes** view, boxes are arranged ordered alphabetically by their name.

➤ **Versions**

**Fig. 18-34** Software Update tab - Versions view

Group	Box Name	ID	Status	Version	Last Update	Fail Reason
unassigned	Head1	1	unassigned	GWAY-4.0.0-153.nightbuild	10.0.66.112	P 12 day(s), 1 hour
201	b. 1	201	unassigned	unknown	-	no
301	b. Head1	301	unassigned	unknown	-	no
201	b. 1	201	unassigned	unknown	-	no
301	b. Head1	301	unassigned	unknown	-	no


In the **Versions** view, boxes are summarised by the netfence software version they are currently installed with. Boxes that are unavailable, are assigned to the the version item **unknown**.

### 5.11.1.2 Context Menu

The context menus available in the System list are dependant on the view that has been defined in the View/Filter list.

In all views, right-clicking a box makes the following entries available:

➤ **Trigger reload**

Click here to trigger the MC to fetch current status information from a box. Then click the  **Update List** button to reload the view in phion.a.

**Note:**  
Allow a few seconds before reloading the phion.a view.

**Note:**  
Status information for boxes pushing content actively (flagged with **P** in the listing) is always reloaded, when **Trigger Reload** is executed on any system.

➤ **Check all**

Click here to select all systems displayed in the listing. For selected systems update tasks may be created (see 5.12.1 Example, page 408).

➤ **Uncheck all**

Click here to unselect all systems.

➤ **Collapse all**

Click here to collapse the complete configuration tree.

➤ **Expand all**

Click here to expand the complete configuration tree.

In the **Groups** view, the following additional entries are available:

**Note:**

To enable group-related context menu items, lock the View/Filter list area by clicking the **Lock** button.

➤ **Create Group**

Click here to create a new organisational group.

➤ **Rename**

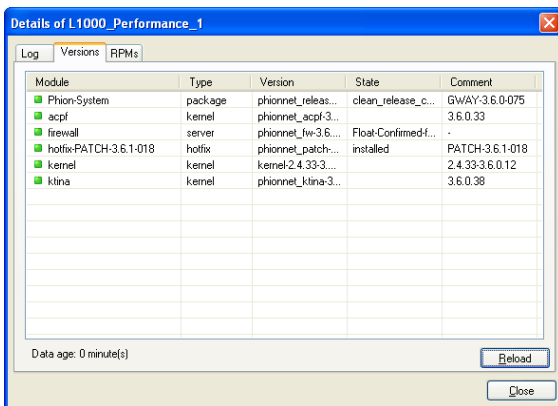
Select a group and click here to rename it. Note that the preconfigured group element **!unassigned** may not be renamed.

➤ **Remove**

Select a group and click here to delete it. Note that the preconfigured group element **!unassigned** may not be deleted. When a group is deleted, boxes assigned to it are automatically moved to the group **!unassigned**.

### 5.11.1.3 Viewing Box Details

Fig. 18-35 Box Details window



To view detailed box information, double-click a box in the System list. This opens the **Details** window including the following information:

➤ **Log** tab

This tab contains the log messages related to the last software update execution. Information may be reloaded from the MC by clicking the **Reload** button or cleared from the window by clicking the **Clear** button. Note that log entries are not cleared from the logfiles on the box itself.

➤ **Versions** tab

This tab lists important modules installed on the box and their corresponding version numbers.

➤ **RPMs** tab

This tab lists all RPMs installed on the box and indicates their status.

### 5.11.2 View/Filter List

Filtering options available in this section allow defining specific views in order to easily recognise systems with identical software versions. Based on this, boxes may then be selected and scheduled for update concurrently.

The following filtering options are available:

➤ **Current View**

Options available in this list are described in detail in 5.11.1.1 Views, page 406.

➤ **Filter / Known hotfixes/patches**

Combination of these filtering options allows including or excluding boxes in or from the view respectively. The Known hotfixes/patches field lists all patches that have already been installed on an arbitrary number of boxes and have been recognised by the MC.

**Note:**

Only hotfixes (all) and patches 3.6.x will be shown. (Since 4.0 patches are of type releases/packages). To change this ...

➤ Set the **Current View** to **Versions**

This will show the MC-managed boxes in sections with their current software version.

To define a filter based on a system's software version proceed as follows :

➤ Click the **Lock** button in the View/Filter list.

➤ Select an update listed in the Known hotfixes/patches field.

➤ Select **Installed on** in the **Filter** list to include boxes that have been installed with the patch into the view in the System list, or ...

➤ Select **NOT installed on** in the Filter list to exclude these boxes from the view.

➤ Click the **Reset** button to remove filter settings.

### 5.11.3 Software List

Into the **Software** list update packages that should be installed on MC-administered boxes have to be imported. From there they can then be selected in order to create corresponding update tasks for execution. Current update packages may be downloaded from the phion support homepage.

The following buttons are available in the action bar in order to execute one of the following operations:

- **Import ...** button  
Allows importing a software package into the MC.
- **Show ...** button  
Displays software package specific information. This information may be displayed as well by double-clicking a selected software package.
- **Remove** button  
Deletes an uploaded software package from the MC.

#### Note:

Uploaded software packages are stored in `/opt/phion/rangetree/exec/rpms` on the management centre. The partition this folder resides in, is 2 GB in size. To prevent the MC running out of disk space, make sure to delete outdated update packages from the software list regularly.

## 5.12 Update Tasks Tab

Update tasks that are created in the Software Update tab are not executed immediately but instead are added to the listing in the Update Tasks tab. This list displays the status of tasks.

The listing is divided into the following columns:

**Table 18-15** Data listed in the task list of the Software Update tab

Column	Description
<b>Box</b>	This is the name of the netfence gateway.
<b>Cluster</b>	This is the name of the cluster the box resides in.
<b>Range ID</b>	This is the name of the range cluster and box belong to.
<b>Σ (Box Icon)</b>	This column depicts the status of an executed task. <ul style="list-style-type: none"> <li>■ The task is executed successfully.</li> <li>■ Task execution has failed.</li> </ul>
<b>RPM</b>	This is the name of the RPM that is currently executed.
<b>Info</b>	This column lists additional information such as IP address and short name.
<b>Status</b>	This is the assigned task status. <ul style="list-style-type: none"> <li>➤ <b>0 Pending Copy</b></li> <li>➤ <b>1 Failed Copy</b></li> <li>➤ <b>2 Completed Copy</b> (ready for activation)</li> </ul>
<b>Time</b>	This column informs about date and time when the update was started (the used syntax is <code>yyyy mm dd hh:mm:ss</code> ).
<b>Reason</b>	This is the failure reason in case the last execution try has failed.

Consider the example below to understand the context between task creation in the Software Update tab and task execution in the Update Tasks tab.

### 5.12.1 Example

The example below describes how to create a software update task in the Software Update tab and add it to the **Update Tasks** tab.

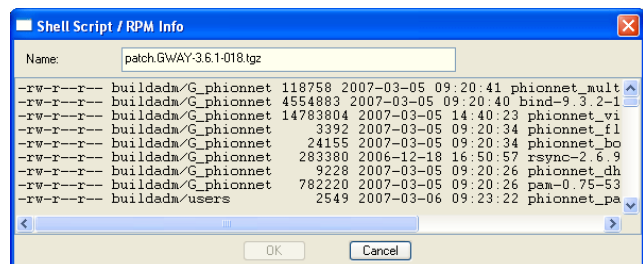
#### Step 1 Import a package

Click the **Import** button in the Software list window, select a package and click open to import it into the MC.

#### Step 2 Check the package content

Double-click the imported package in the package selection list and make sure that it contains the desired software.

**Fig. 18-36** RPM information window



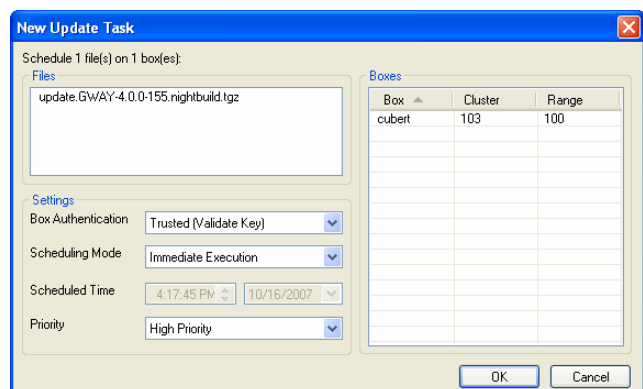
#### Step 3 Create the update tasks

In the Software list select the package, and in the System list check the netfence gateway(s) that should be updated with the imported package. Then click the **Create Task** button in the View/Filter list window.

#### Step 4 Schedule the tasks

Schedule the tasks for **Immediate Execution** in the Schedule Task window.

**Fig. 18-37** Scheduling a new task



#### Step 5 Watch the task list

For each created task an entry is added to the **Update Tasks** tab.

Tasks are added with a green indicator and disappear as soon as they have been executed.

#### Step 6 Check the package transfer

Check the update task list for the status of the package transfer and wait until the task is in the **Copy Completed** state.

#### Note:

This may take some time.

**Step 7 Activate the package**

Access the **Update Tasks** tab, select the task and then select **Perform Update** from the context menu. Wait until the update task entry disappears from the list.

**Step 8 Review the log files**

In the **Software Update** tab, double-click the specific netfence gateway to view the log files and check if the desired actions have been taken.

**Step 9 Review the log files on the updated box**

Log in to the box log facility and review the update log files for the installed package type (📄 **Logs** > 📦 **Box** > 📁 **Release**).

**Step 10 Reschedule or delete failed tasks**

Fig. 18-38 Rescheduling of a failed task

Σ	Box	Cluster	Range ID	RPM	Info	Status	Time	F
	Su...	40	10	update.GWAY-3...	Update Lists	2: Completed Copy	09 Aug...	U
					Perform Update			
					Delete Update			
					Arrange Icons By ▶			
					Tools ▶			

## 6. MC Configuration Service

### 6.1 General


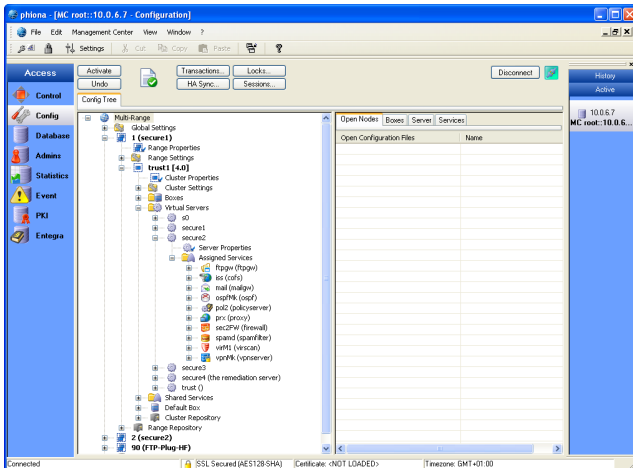
The Configuration Service of the management centre is accessible through the box menu item  **Config**. It allows remote configuration of the MC and of the netfence gateways the MC administers.

Fig. 18-39 management centre (MC) - Configuration Service



The main window consists of two frames. The left one shows the configuration tree, the right one shows in tabs:

- **Open Nodes**  
access to all opened configuration files
- **Boxes**  
access to the boxes configuration files.
- **Server**  
access to the virtual server configuration files
- **Services**  
access to the assigned services configuration files

#### Note:

If there is no right frame on your screen open it with your mouse from the right side of the main window.

To switch from the MC to a box right-click the desired box and choose **Launch Control for Box...** from the context menu.

Fig. 18-40 MC Config main window - launch control for box

Open Nodes	Boxes	Server	Services
Box	Cluster	Range	Box IP
DHCP-server (für int...	trust1	1	10.0.6.44
borderFirewall1 (M1...	trust1	1	10.0.6.13
borderFirewall2 (M50)	trust1	1	10.0.6.38
polsrv1-backup (/pha...	trust1	1	10.0.6.130
polsrv1 (th...	Launch Control for Box...	1	10.0.6.40
polsrv2 (cc...	Refresh	2	172.22.0.160
remsrv1 (t...	Tools	1	10.0.6.42
s10 ()		2	10.0.6.21
s20-ethernet (uses ...	trust2	2	10.0.6.28
s20-remote (uses tr...	trust1	1	10.0.6.28

Three administration entities are available:

- **Range**
- **Cluster**

#### Attention:

phion management centre 4.2 does not provide support for managing netfence 3.2 clusters. All clusters must be migrated to version 3.4 or higher before updating the MC to netfence 4.2 (see 6.9.3.1 Migrating a Cluster, page 422)

- **Box**



#### Note:

The `<boxname>_<clustername>_<rangeID>` arrangement may contain a **maximum of 16 characters**. Use as short names as possible for ranges, clusters and boxes.

## 6.2 Multi-Range

The configuration node  **Multi-Range** represents the highest level within the management centre configuration tree hierarchy. It contains all available ranges, clusters and boxes that are managed by the management centre.

### 6.2.1 Context Menu of Multi-Range

To access the Multi-Range context menu, right-click the configuration node  **Multi-Range**. The context menu makes the following MC-specific items available beside the standard entries known from the single box configuration (configuration tree item  **Box**, see **Configuration Service** - 2.2.1.1 Box Context Menu, page 51):

- **Create Range ...**

Clicking this entry allows creating a new range (see 6.4.1 Creating a New Range, page 416).

#### Note:

Immediately click **Send Changes > Activate** after having introduced a new range.



- **Toggle Permission View**

Clicking this entry displays the configurable read (r) and write (w) permissions for each entry of the configuration tree. For information on how to configure permission settings, refer to 6.7 Defining Node Properties, page 420.

- **Toggle Release View**

Clicking this entry displays the release version numbers of all boxes, servers and services included in the Multi-Range configuration. For details on netfence multi-release features, see 6.9 Multiple Releases, page 421.

- **Restrict View to Range, Restrict View to Cluster**

These entries become available with either selection of  **Range** or  **Cluster** node. Clicking the respective



entry, restricts the view to the selected range or cluster accordingly.

➤ **Show Full tree**

This entry becomes available when the configuration tree view is restricted to either range or cluster view (see above). Clicking it expands the configuration tree view to display of all ranges and clusters.

➤ **Migrate Clusters, Migrate Ranges, Migrate Complete Tree**

For a description of these context menu entries, refer to 6.9 Multiple Releases, page 421.

## 6.3 Global Settings

Global Settings are applicable for all ranges, clusters and boxes that the management centre administers. The following settings are available for configuration:

- Eventing
- Global Firewall Objects
- Pool Licenses, page 411
- MC Identity, page 412
- MC Parameters, page 413
- MC Access Notification, page 413
- Administrative Roles, page 414
- Statistics Cook Settings, page 415
- VPN GTI Editor (Global), page 415
- Box VIP Network Ranges, page 415

### 6.3.1 Global Settings - Eventing

Global eventing settings are effective for all events that MC-administered boxes propagate to the management centre. Global settings may be overridden by Range- or Cluster-specific event settings (see 6.4.2.2 Range-specific Event Settings, page 417, and 6.5.2.2 Cluster-specific Event Settings, page 419).

To access global eventing settings, select ⚠ **Eventing** in the configuration tree (accessible through 🛠 **Config** > 🌐 **Multi-Range** > 📁 **Global Settings**).

The configuration procedure of global eventing settings is identical to the procedure on single boxes. For details, see **Eventing** - 2. Event Configuration, page 306.

### 6.3.2 Global Settings - Global Firewall Objects

Global firewall objects are available to all firewall services that the management centre administers. Making use of global firewall objects in rule sets aims at ensuring implementation of consistent security policies.

To access the global firewall objects configuration area, select 📁 **Global Firewall Objects** in the configuration tree (accessible through 🛠 **Config** > 🌐 **Multi-Range** > 📁 **Global Settings**).

The following firewall objects may be defined globally:

- **Networks**
- **Services**
- **User Groups**
- **Content Filter**

**Note:**

In case global Firewall objects are renamed this change has to be confirmed directly with **Send Changes** > **Activate** before editing further Firewall objects.

The configuration procedure of global objects is identical to the procedure on single boxes. For details, see **Firewall** - 2.2 Rule Set Configuration, page 132.

#### 6.3.2.1 Global GTI Objects

When tunnel endpoints are created in the **VPN GTI Editor (Global)**, corresponding dynamic network objects are created at the same time (**phion management centre** - 15. VPN GTI, page 464). These objects are named `<servername>_<clustername>_<rangeID>` with a prefixed **GTI-Server** accordingly. Global GTI Objects are inherited as references by Local and Forwarding Firewall rule sets of each Firewall service related to the tunnel endpoint and may be used for rule specification. Every time a new tunnel endpoint is inserted into the Global VPN GTI Editor, the GTI Objects should be reloaded in the **Global Firewall Objects** window in order to become available in the configuration dialogues (**Firewall** - 2.2.3 Rules Configuration, page 135, parameter **Reload GTI Objects**).

**Note:**

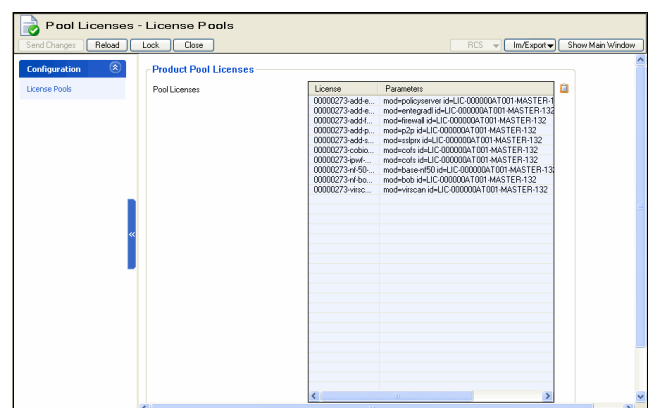
As Global GTI Objects are created dynamically, they cannot be renamed or modified.

### 6.3.3 Global Settings - Pool Licenses

management centre licenses are attached to the hardware of the machine the management centre is running on. They enable the administrator to generate and activate the Main Identity of the management centre. This Main Identity will be used for all further communication between the MC and the netfence gateways.

To access the pool licenses configuration area, select 📁 **Pool Licenses** in the configuration tree (accessible through 🛠 **Config** > 🌐 **Multi-Range** > 📁 **Global Settings**).

Fig. 18-41 Pool Licenses - user interface



In the Pool Licenses configuration area, a listing of all installed licenses is displayed.

Right-clicking the licenses list makes the standard context menu available (see 4.2 Standard Context Menu, page 395).

The following buttons are available for license administration:

- **Edit ...**  
To view full license information in the license's Certificate View window, select a license and click the **Edit** button (or double-click a selected license).
- **Import** menu  
To install a new license, click **Import** and then click **Import from Clipboard** or **Import from File**.  
To export license information, select a license, click **Import** and then click **Export to Clipboard** or **Export to File**.  
To add an optional license description to the list, select a license, click **Import** and then click **Add Comment**.
- **Delete**  
To delete one or multiple licenses, select the license(s) and click **Delete**. To select multiple licenses, click the **CTRL** and/or **SHIFT** key and click the respective license in the listing.

## 6.3.4 Global Settings - MC Identity





The MC Identity configuration area allows configuring various MC-related settings (for example MC IP address(es), private keys, ...).

### Note:

Make sure to configure the MC Identity section correctly before introducing boxes on the management centre. If not configured correctly, the boxes will not receive a valid box certificate and will not be able to establish a trust relationship to the MC.

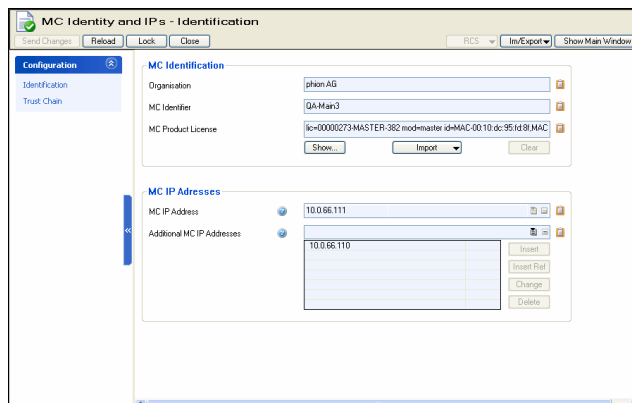
### Note:

Make sure to specify both, the server and the box IP in the MC Identity settings of the management centre (see **MC IP Address** and **Additional MC IP Addresses**).

To access the MC Identity configuration area, select  **MC Identity** in the configuration tree (accessible through  **Config** >  **Multi-Range** >  **Global Settings**).

### 6.3.4.1 Identification

Fig. 18-42 MC Identity - Identification



The **Identification** view makes the following configuration items available:

List 18-3 MC Identity - Identification - section MC Identification

Parameter	Description
<b>Organisation</b>	Into this field, insert the name of the company.
<b>MC Identifier</b>	Information displayed in this read-only field is extracted from the MC (Master) license.
<b>MC Product License</b>	Into this field, import the Master License file that has been issued by phion. <ul style="list-style-type: none"> <li>➤ To import the license file, click <b>Import</b> and select <b>Import from Clipboard</b> or <b>Import from File</b>.</li> <li>➤ To view the imported license in the Certificate View window, click <b>Show</b>.</li> <li>➤ To delete the currently installed master license, click <b>Clear</b>.</li> </ul>

List 18-4 MC Identity - Identification - section MC IP Addresses

Parameter	Description
<b>MC IP Address</b>	Into this field, insert the IP address that should be used for connections between MC and MC-administered boxes.
<b>Additional MC IP Addresses</b>	Into this field, insert the IP address(es) that should be used for logins to the MC on box level.

### 6.3.4.2 Trust Chain

List 18-5 MC Identity - Trust Chain Configuration - section Trust Chain Configuration

Parameter	Description
<b>MC Certificate</b>	The <b>MC Certificate</b> is the Main Identity of the management centre. It is signed by the license key and distributed to MC-administered boxes for authentication purposes, thus ensuring trustable communication.  To insert appropriate company information into the certificate click <b>Edit</b> . To view certificate information click <b>Show</b> . Note that the certificate's public hash (displayed to the right) changes when a new <b>MC Private Key</b> is generated (see below).  <b>Note:</b> Certificate installation procedure on management centres is described in detail in 3.2 Installing the Licenses, page 394.
<b>MC SSL Certificate</b>	In contrast to the <b>MC Certificate</b> (see above), the MC SSL Certificate not signed by the license key but self-signed instead. The SSL certificate automatically changes when the MC Certificate changes. It is sent out to all managed boxes in a hidden <i>conf</i> file (masterpub.conf). The MC SSL Certificate is required for SSL-compatible peer authentication between a box transmitting data and the MC Log Service in context with SSL based log file streaming.

List 18-5 MC Identity - Trust Chain Configuration - section Trust Chain Configuration

Parameter	Description
<b>MC Private Key</b>	<p>Here the MCs private key is handled. The button <b>New Key</b> generates a new private key and hash (displayed to the right).</p> <p>The menu <b>Ex/Import</b> offers the following options:</p> <ul style="list-style-type: none"> <li>➤ <b>Export to Clipboard/ File ...</b> Exports the master private key to the clipboard or to a file.</li> <li>➤ <b>Export to Clipboard/ File ... (password protected)</b> Exports the master private key to the clipboard or to a file. However, it is necessary to define and confirm a password that has to be entered, when importing the key.</li> <li>➤ <b>Export Public to Clipboard/ File ...</b> Exports the public key to the clipboard or to a file.</li> <li>➤ <b>Import from Clipboard/ File ...</b> Imports the master private key from the clipboard or from a file.</li> </ul>
<b>Preceding Private Key #1, #2, #3</b>	<p>In this section former private keys are stored as soon as a new <b>MC Private Key</b> is generated.</p> <p>The menu <b>Ex/Import</b> offers the following options:</p> <ul style="list-style-type: none"> <li>➤ <b>Import from Clipboard/ File ...</b> Imports the old private key from the clipboard or from a file.</li> </ul>

List 18-6 MC Identity - Trust Chain Configuration - section MC SSH Access Keys

Parameter	Description
<b>MC SSH Key</b>	<p>Here the MCs SSH key is handled. The button <b>New Key</b> generates a new SSH key and hash (displayed to the right).</p> <p>The menu <b>Ex/Import</b> offers the following options:</p> <ul style="list-style-type: none"> <li>➤ <b>Export to Clipboard/ File ...</b> Exports the master SSH key to the clipboard or to a file.</li> <li>➤ <b>Export to Clipboard/ File ... (password protected)</b> Exports the master SSH key to the clipboard or to a file. However, it is necessary to define and confirm a password that has to be entered, when importing the key.</li> <li>➤ <b>Export Public to Clipboard/ File ...</b> Exports the public key to the clipboard or to a file.</li> <li>➤ <b>Import from Clipboard/ File ...</b> Imports the master SSH key from the clipboard or from a file.</li> </ul>
<b>Preceding MC SSH Key</b>	<p>In this section former SSH keys are stored as soon as a new <b>MC SSH Key</b> is generated.</p> <p>The menu <b>Ex/Import</b> offers the following options:</p> <ul style="list-style-type: none"> <li>➤ <b>Export to Clipboard/ File ...</b> Exports the old SSH key to the clipboard or to a file.</li> <li>➤ <b>Export to Clipboard/ File ... (password protected)</b> Exports the old SSH key to the clipboard or to a file. However, it is necessary to define and confirm a password that has to be entered, when importing the key.</li> <li>➤ <b>Export Public to Clipboard/ File ...</b> Exports the public key to the clipboard or to a file.</li> <li>➤ <b>Import from Clipboard/ File ...</b> Imports the old SSH key from the clipboard or from a file.</li> </ul>

### 6.3.5 Global Settings - MC Parameters

These parameters describe the behaviour of the management centre

- within the status map ( **Control** > **Status Map**)
- when running a configuration update ( **Control** > **Configuration Updates**)
- when running remote execution

To access the MC Parameters configuration area, select **MC Parameters** in the configuration tree (accessible through **Config** > **Multi-Range** > **Global Settings**).

#### 6.3.5.1 Operational Setup

List 18-7 MC Parameters - Operational Setup - section Status Map Setup

Parameter	Description
<b>Total Poll Time</b>	Defines the refresh rate of the status map in seconds.
<b>Box Reachable Statistics</b>	Set to <b>yes</b> to create statistics about the reachability of the included boxes (default: <b>no</b> ).
<b>Trace Unreachable Boxes</b>	Set to <b>yes</b> to trace unreachable boxes (default: <b>no</b> ).
<b>External Boxes</b>	<p>Via this section it is possible to integrate external boxes that are not managed by this management centre into the status map.</p> <p><b>Note:</b> Insert the MC box IP to embed the MC itself into the status map.</p>

List 18-8 MC Parameters - Operational Setup - section Configuration Update Setup

Parameter	Description
<b>Max. Update Processes</b>	This parameter defines the maximum number of simultaneous configuration updates.
<b>HA Sync Timeout</b>	Default 120 seconds. In case of HA synchronization problems increase this timeout.

List 18-9 MC Parameters - Operational Setup - section Remote Execution Setup

Parameter	Description
<b>Max. Exec Processes</b>	This parameter defines the maximum number of simultaneous sessions.

List 18-10 MC Parameters - Operational Setup - section VPN World Setup

Parameter	Description
<b>Poll Box VPN Status</b>	Choose <b>yes</b> when you are using VPN world. The MC will collect all relevant data that is necessary to be displayed in VPN world.

#### 6.3.5.2 RCS Setup

For a description of the **Revision Control System (RCS)**, refer to 17. MC RCS, page 473.

### 6.3.6 Global Settings - MC Access Notification

By means of the parameters available in this tab, the notification types, which are induced by specific actions, can be configured.

The user interface allows configuring the so-called Service Defaults that apply when no special notifications are set/required. The sections **Type 1 Admin**, **Type 2 Admin**, and **Type 3 Admin** allow defining notification settings for 3 types of administrators (configurable in **Admins**, see 8.3.1 Creating a New Admin Profile, Login Event menu, page 435).

In order to enter the access notification window, simply select the entry **MC Access Notification** from the configuration tree ( **Multi-Range** > **Global Settings**).

Currently used types are:

- **Silent** (no event)
- **Notice**

➤ **Warning**

➤ **Alert**

The latter three may be used to modify the severity of a context dependent event type. A listing of generated events can be found in **System Information** - 5. List of Default Events, page 516.

### 6.3.6.1 phiona Authentication Success / phiona Authentication Failure

The following objects are available for configuration:

➤ **Configuration Centre (Success) / Configuration Centre (Failure)**

Login to MC Config

➤ **Central Event (Success) / Central Event (Failure)**

Login to MC Event

➤ **Central Statistics (Success) / Central Statistics (Failure)**

Login to MC Statistics

➤ **Central PKI (Success) / Central PKI (Failure)**

Login to MC PKI

## 6.3.7 Global Settings - Administrative Roles

These global settings define the restrictions for administrative roles. They are needed when a new administrator is introduced (see 8.3.1 Creating a New Admin Profile, Roles, page 435).

To access the Administrative Roles configuration area, select **Administrative Roles** in the configuration tree (accessible through **Config** > **Multi-Range** > **Global Settings**).

The user interface consists of a listing displaying already existing profiles (columns display the corresponding settings) and three buttons for interaction.

➤ **Edit ...** button

This button opens the configuration dialogue with the settings of the selected role.

➤ **Delete** button

The button removes the selected role from the listing.

➤ **Insert ...** button

This button allows creating a new administrative role. The first window opened requires the defining role number. After confirming the number by clicking the **OK** button the role configuration dialogue is opened providing the following settings:

List 18-11 Administrative Roles - Role Setup - Roles - section Role Name

Parameter	Description
<b>Name</b>	This parameter takes a describing name for the administrator's role.

**Note:**

The checkboxes in this following section define whether the corresponding module can be accessed by the administrator (checkbox selected). When selected the permissions can be set in detail by clicking the **Edit ...** or **Set ...** buttons.

List 18-12 Administrative Roles - Role Setup - Roles - section ... Module

Parameter	Permissions
<b>MC Config Permissions</b>	Kill Sessions
	Change Permissions
	Change Events
	Show Admins
	Manage Admins
	Create/Remove Range
	Create/Remove Cluster
	Use RCS
	Create/Remove Boxes
	Create/Remove Server
	Create/Remove Service
	Create/Remove Repository
	Manage HA Sync
	Create PAR File
	Allow Config View on Box
Allow Emergency Override	
<b>MC Control Permissions</b>	Show Map
	Show Config. Updates
	Manage Config. Updates
	Show Box REXEC
	Manage Box REXEC
	Show Box Software Updates
	Manage Box Software Updates
	Manage Box File Update
<b>Access to MC PKI</b>	
<b>Control Permissions</b>	Start/Stop Server
	Block Server
	Start/Stop Service
	Block Service
	Delete Wild Route
	Activate New Configuration
	Restart Network Subsystem
	Set or Sync Box Time
	Restart Phion Subsystem
	Reboot System
	Activate Kernel Update
	Kill Sessions
	Import License
	Remove License
	View License Data
	<b>Event Permissions</b>
Stop Alarm	
Mark as Read	
Confirm Events	
Delete Events	
<b>Log Permissions</b>	Read Box Logfiles
	Delete Box Logfiles
	Read Service Logfiles
	Delete Service Logfiles
<b>Statistics Permissions</b>	Read Box Statistics
	Delete Box Statistics
	Read Service Statistics
	Delete Service Statistics
<b>DHCP Server Permissions</b>	Enable Commands
<b>Policy Service Permissions</b>	Enable Commands

**List 18-12** Administrative Roles - Role Setup - Roles - section ... Module

Parameter	Permissions
<b>MC Policy Service Permissions</b>	Enable Commands, to modify or remove entries from the status and access cache
	Block Box Sync. to disable authentication sync within a trustzone
<b>Firewall Permissions</b>	Terminate Connections
	Modify Connections
	Kill Handler Processes
	Dynamic Rule Control
	Toggle Trace
	<b>Note:</b> Selecting this parameter together with <b>View Trace Output</b> and <b>Change Settings</b> enables the admin to run <code>admin tcpdump</code> on the command line. See documentation Command Line Interface for detailed information.
	View Trace Output, see note on parameter <b>Toggle Trace</b>
	Change Settings, see note on parameter <b>Toggle Trace</b>
<b>VPN Server Permissions</b>	View Rule Set
	Manipulate Access Cache Entries
	Terminate VPN Tunnels
<b>Mail Router Permissions</b>	Disable/Enable VPN Tunnels
	View Configuration
	Enable Commands
	View Stripped Attachments
<b>Virscan Service Permissions</b>	Retrieve Stripped Attachments
	Delete Stripped Attachments
<b>Secure-Web-Proxy Permissions</b>	Allow Block Virus Pattern Update
	Allow Manual Virus Pattern Update
<b>Secure-Web-Proxy Permissions</b>	Access Cache Management, to manipulate access cache entries
	Ticket Management, to process access request tickets
	Cert. Authorities Management, - to accept/deny a root CA - to modify CRL handling
	XML Services Management, to modify settings for RSS-feeds or Webservices (allow, scan, deny, delete)

### 6.3.8 Global Settings - Statistics Cook Settings

This section globally defines the compression of statistics files that have been collected by the management centre from its MC-administered boxes. For a detailed description of configuration options see 9.3 Compression Cooking and Deletion, page 438.

### 6.3.9 Global Settings - VPN GTI Editor (Global)

Open the **Global VPN GTI Editor** to access the netfence VPN Graphical Tunnel Interface (GTI). For detailed information on this configuration section, see 15. VPN GTI, page 464.

### 6.3.10 Global Settings - Box VIP Network Ranges

Configuration of this section is necessary to introduce so-called **remote management** or **box tunnels**. A box tunnel is used to establish an encrypted communication between the management centre and the netfence

gateway if the management IP of the gateway is not directly reachable (for example routing issues).

A common example is to establish communication between a gateway at a remote location and the MC located at the headquarter where the remote site is only reachable by an internet connection.

In general the box management IP is within the network address range of the remote site.

Since it is neither recommended nor always possible to enable an external management IP, which is directly accessible from the internet (for example when the internet provider assigns a dynamic external IP), another method has to be found to establish a connection between box and MC.

Even if a VPN tunnel between remote site and headquarter is established, it is recommended to use box tunnels. If the remote site is not reachable due to a misconfiguration of the VPN tunnel or a blocked VPN service, the box tunnel will nevertheless stay established.

VIP network ranges defined in this section are enabled as Proxy ARPs on the management centre and should thus not collide with used IP addresses in this network segment.

In addition to the definition of VIP networks, the usage of a box tunnel requires configuration of the Remote Management section in the box network node.

#### Note:

Using remote management tunnels requires the introduction of an additional service '**mvpn**' on the management centre itself.

A netfence gateway that is managed through a box tunnel establishes an encrypted VPN connection to the management centre. All communication between management centre and gateway is processed through the box tunnel (TCP, port 692). Even communication between the admin workstation and the remote box is handled through the box tunnel. phion.a utilises the **Virtual IP (VIP)** that is defined in the Box - Network Configuration - Remote Management section as box address (destination address) when establishing a connection to the MC. It is thus essential that VIP network ranges be routed from the admin workstation to the MC.

#### 6.3.10.1 VIP Networks

To insert a Box VIP Network Range, select  **Box VIP Network Ranges** from the configuration tree (accessible through  **Multi-Range** >  **Global Settings**).

The user interface consists of a listing displaying already existing network ranges (columns display the corresponding settings) and three buttons for interaction:

#### ➤ **Edit** button

This button opens the configuration dialogue with the settings of the selected network range.

#### ➤ **Insert** button

This button allows creating a new network range. The first opened window requires the defining name for the network range. After confirming the name with **OK** the configuration dialogue is opened providing the following settings:

#### ➤ **Address Range Start** IP address



➤ **Address Range Netmask**

➤ **Delete** button

This button deletes the selected network range from the listing.

### 6.3.10.2 VPN Settings

List 18-13 Box VIP Network Ranges - VPN Settings

Parameter	Description
<b>Pending Session Limitation</b> [default Yes]	Session buildup is limited that once a buildup of 5 sessions is detected any further session request will be dropped until one of the already initiated sessions is completed. This feature can be turned off configuring the VPN settings parameter <b>Pending Session Limitation</b> (see list 5-3, page 207).
<b>Use Tunnels for Authentication</b> [Yes]	Normally a tunnel registers itself at the firewall causing an auth.db entry with the tunnel network and the tunnel credentials. This can be used to build firewall rule having the tunnel name or credentials as condition. This feature is rarely used (maybe not at all). Using the VPN settings parameter <b>Use Site to Site Tunnels for Authentication</b> (see list 5-3, page 207) this functionality can be turned off improving the startup speed dramatically.
<b>Prebuild Cookies on Startup</b> [No]	Normally cookie are built on demand. For many tunnel building up simultaneously it is better to have the cookie already precalculated. This causes a slower VPN service startup but a faster tunnel buildup afterwards. This feature can be turned off configuring the VPN settings parameter <b>Prebuild Cookies on Startup</b> (see list 5-3, page 207).
<b>Listen to Port 443</b> [Yes]	Defines, whether incoming VPN connections on port 443 should be accepted or not (default: <b>Yes</b> ). In some cases you might want to disable using port 443 for incoming VPN connections, for example connections arriving at port 443 should be redirected by the firewall service to another machine. Using the VPN settings parameter <b>Use port 443</b> (see list 5-3, page 207) this functionality can be turned off.

## 6.4 Range Configuration

A range is the largest configuration entity, built up of one or multiple clusters. Ranges are meant to simplify central administration of huge networks. Within ranges, global settings, spanning all existent clusters can be defined. Within clusters, in turn, global settings, spanning all existent boxes can be configured. Beyond this, specific security implementations in the **Cluster Services** allow configuration of security settings not available for regular services (see 6.11 Supplement - Configuring the Cascaded Firewall (cfirewall), page 425).

Setups with configured ranges involve the following further benefits:

➤ **Statistics**

When the MC is configured to collect statistics, the statistics data gets range classified. This amongst others allows range specific accounting.

➤ **Administrative settings**

Ranges can be allocated to administrative roles (see Range Name, page 416). This allows specific ranges only to be administered by explicitly assigned administrative roles.

### 6.4.1 Creating a New Range

Right-click **Multi-Range** and select **Create Range** from the context menu to create a new range. Enter a **Range Name** (Note: only numbers allowed) and confirm your entry by clicking the **OK** button. This opens the range configuration dialogue (later accessible via **Multi-Range** > <rangename> > **Range Properties**).

**Attention:**  
Range names may only contain numbers. Therefore, Range names are often referred to as Range IDs. Range IDs may start with Range "1". Range ID "0" is reserved for internal purposes and may not be used. When naming a range use as short names a possible because the `box_range_cluster` name is restricted to a maximum length of 16 characters.

**Note:**  
Make sure to click **Send Changes** > **Activate** after having introduced a new range. Otherwise, boxes will not receive a valid box certificate and will not be able to establish a trust relationship to the MC.

Fig. 18-43 Create Range - configuration dialogue

List 18-14 Creating a new range - section Identification

Parameter	Description
<b>Range Name</b>	This read-only field displays the range number as inserted during the creation dialogue.
<b>Description</b>	Insert a significant range description into this field.

List 18-15 Creating a new range - section Contact Info

Parameter	Description
<b>Full Name/Contact Person/Telephone Nr./Email Address</b>	To ease approaching the range administrator, these fields should be filled with appropriate contact information.

List 18-16 Creating a new range - section Specific Settings

Parameter	Description
<b>Disable Update</b>	This parameter enables/disables configuration updates for boxes from this range (default: <b>no</b> ).
<b>Collect Statistics</b>	Setting to <b>yes</b> (default) triggers the management centre to collect statistics from managed boxes within this range.



List 18-16 Creating a new range - section Specific Settings

Parameter	Description
<b>Own Cook Settings</b>	If the range requires special cook settings for statistical data, set this parameter to <b>yes</b> (default: <b>no</b> ). By doing so, the file <b>Statistics Cook Settings</b> is introduced below <b>Multi-Range</b> >  <rangename> > <b>Range Settings</b> where the custom cook settings for the range may be defined. For information concerning the parameters available in this customising file, see 9.3.2 Range Specific Settings, page 439.
<b>Own Event Settings</b>	If the range requires special event settings, set this parameter to <b>yes</b> (default: <b>no</b> ). By doing so, the file <b>Eventing</b> is introduced below <b>Multi-Range</b> >  <rangename> > <b>Range Settings</b> where the custom event settings for the range may be defined. For information concerning the parameters available in this customising file, see 10.3.3 Cluster-specific Event Settings, page 445.
<b>Own Firewall Objects</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables range-specific firewall objects. It introduces the file <b>Range Firewall Objects</b> below <b>Multi-Range</b> >  <rangename> > <b>Range Settings</b> where range-specific network objects may be defined. For information on characteristics and handling of network objects, see <b>Firewall - 2.2.4 Network Objects</b> , page 140.
<b>Own VPN GTI Editor</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables a range-specific VPN GTI Editor. It introduces the file <b>VPN GTI Editor</b> (<rangename>) below <b>Multi-Range</b> >  <rangename> > <b>Range Settings</b> . For information on the functionality of the VPN GTI Editor, see 15. VPN GTI, page 464.
<b>Own Policy Server Objects</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables range-specific policy server objects. It introduces the nodes <b>entegra Policy Objects</b> (containing files <b>Welcome Message</b> , <b>Personal Firewall Rules</b> , <b>Pictures</b> and <b>Registry Checks</b> ), as well as <b>Policy Service Trustzones</b> below <b>Multi-Range</b> >  <rangename> > <b>Range Settings</b> . For detailed information see <b>Configuration Service - Section Policy Based Routing</b> , page 69.
<b>Own Shaping Trees</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables range-specific traffic shaping settings. It introduces the file <b>Range Shaping Trees</b> below <b>Multi-Range</b> >  <rangename> > <b>Range Settings</b> . For detailed information see <b>Configuration Service - 2.2.6 Traffic Shaping</b> , page 81.
<b>Send Statistics to Reporter</b>	Setting to <b>yes</b> (default) triggers the management centre to forward statistics files collected from managed boxes within this range to a <b>netfence reporter</b> . For this to work, parameter <b>Collect Statistics</b> (see above) has to be set to <b>yes</b> as well and the <b>MC-Reporter</b> service has to be installed (see 18. MC Reporter, page 477).

## 6.4.2 Range-specific Settings

### 6.4.2.1 Range-specific Cook Settings

Take into consideration that specific cook settings are only available if the parameter **Specific Cook Settings** (see 6.4.1 Creating a New Range, parameter **Own Cook Settings**) is set to **yes**.

For information concerning the parameters available in this customising file, please have a look at 9.3.2 Range Specific Settings, page 439.

### 6.4.2.2 Range-specific Event Settings

Take into consideration that specific event settings are only available if the parameter **Specific Event Settings**

(see 6.4.1 Creating a New Range, parameter **Own Event Settings**) is set to **yes**.

For information concerning the parameters available in this customising file, please have a look at 10.3.2 Range-specific Event Settings, page 444.

## 6.5 Cluster Configuration

**Attention:**  
 phion management centre 4.2 does not provide support for managing netfence 3.2 clusters.  
 All clusters must be migrated to version 3.4 or higher before updating the MC to netfence 4.2 (see 6.9.3.1 Migrating a Cluster, page 422).

A cluster is a set of operative boxes. Within a cluster, cluster servers and cluster services may be defined:

- **Cluster server**  
 A cluster server provides similar functionality as the single box server, except for the fact that cluster services provide flexible high-availability functionality (cluster servers do not require a dedicated HA box, but the HA partner can be reconfigured while running in operational mode).  
 For information on how to create and configure a cluster server, see 6.5.1.1 Creating a Cluster Server.
- **Cluster services**  
 Cluster services are services that can run on multiple cluster servers.  
 An example for a cluster service is the cfirewall service. The **cfirewall** (Cascaded Firewall) is a cluster firewall. This means that the firewall service is running in operational mode on more than one box at the same time with the same configuration. This offers easy configuration and easy implementation for load sharing scenarios.  
 For information on how to create and configure a cluster service, see 6.5.1.2 Creating a Shared Service, page 418.

In addition to the benefits mentioned above, the other benefits are:

- **Statistics**  
 When the MC is configured to collect statistics, the statistics data gets cluster classified. This amongst others allows cluster specific accounting.
- **Administrative settings**  
 Clusters can be allocated to administrative roles.

### 6.5.1 Creating a New Cluster

Right-click **Multi-Range** > <rangename> and select **Create Cluster ...** from the context menu to create a new cluster. Insert a **Cluster Name** and confirm your entry by clicking the **OK** button. This opens the cluster configuration dialogue (later accessible via **Multi-Range**

>  <rangename> >  <clustername> >  **Cluster Properties**).

**Note:**

Immediately click **Send Changes > Activate** after having introduced a new cluster. Otherwise, boxes will not receive a valid box certificate and will not be able to establish a trust relationship to the MC.

Parameters and their settings are nearly identical to the range-specific settings described in 6.4.1 Creating a New Range, page 416. However, they only apply to the specific cluster and overrule superordinate settings.

List 18-17 Creating a new cluster - section Identification

Parameter	Description
<b>Cluster Name</b>	This read-only displays the cluster name as inserted during the creation dialogue.
<b>Description</b>	Insert a significant cluster description into this field.
<b>Software Release</b>	A cluster is the smallest entity expecting consistent software versions of all MC-administered systems it contains. Thus, when a cluster is created, the <b>Software Release</b> version has to be specified so that configuration files can be adapted accordingly. Multi-release administration is available for netfence release versions 3.4, 3.6, 4.0 and 4.2. netfence multi-release support is described in detail in 6.9 Multiple Releases, page 421.

List 18-18 Creating a new cluster - section Contact Information

Parameter	Description
<b>Full Name/Contact Person/Telephone Nr./Email Address</b>	To ease approaching the cluster administrator, these fields should be filled with appropriate contact information.

List 18-19 Creating a new cluster - section Specific Settings

Parameter	Description
<b>Disable Updates</b>	This parameter enables/disables configuration updates for boxes from this range (default: <b>no</b> ).
<b>Collect Statistics</b>	Setting to <b>yes</b> triggers the management centre to collect statistics from managed boxes within this cluster. Setting <b>like-range</b> (default) inherits the settings from the <b>Range Config</b> file (see <b>Collect Statistics</b> , page 416).
<b>Own Cook Settings</b>	If the cluster requires special cook settings for statistical data, set this parameter to <b>yes</b> (default: <b>no</b> ). By doing so the file <b>Statistics Cook Settings</b> is introduced below <b>Multi-Range &gt; &lt;rangename&gt; &gt; &lt;clustername&gt; &gt; Cluster Settings</b> where the custom cook settings for the cluster may be defined. For information concerning the parameters available in this customising file, see 9.3.3 Cluster Specific Settings, page 439.
<b>Own Event Settings</b>	If the cluster requires special event settings, set this parameter to <b>yes</b> (default: <b>no</b> ). By doing so the file <b>Eventing</b> is introduced below <b>Multi-Range &gt; &lt;rangename&gt; &gt; &lt;clustername&gt; &gt; Cluster Settings</b> where the custom event settings for the cluster may be defined. For information concerning the parameters available in this customising file, see 10.3.3 Cluster-specific Event Settings, page 445.
<b>Own Firewall Objects</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables cluster-specific firewall objects. It introduces the file <b>Cluster Firewall Objects</b> below <b>Multi-Range &gt; &lt;rangename&gt; &gt; &lt;clustername&gt; &gt; Cluster Settings</b> where cluster-specific network objects may be defined. For information on characteristics and handling of network objects refer to <b>Firewall - 2.2.4 Network Objects</b> , page 140.
<b>Own VPN GTI Editor</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables a cluster-specific VPN GTI Editor. It introduces the file <b>VPN GTI Editor (&lt;clustername&gt;)</b> below <b>Multi-Range &gt; &lt;rangename&gt; &gt; &lt;clustername&gt; &gt; Cluster Settings</b> . For information on the functionality of the VPN GTI Editor see 15. VPN GTI, page 464.

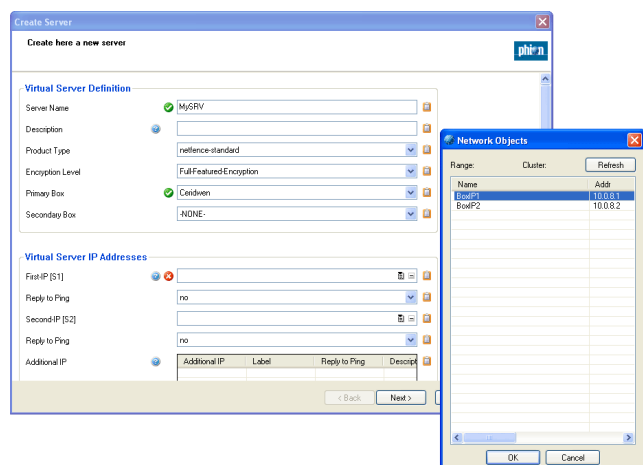
List 18-19 Creating a new cluster - section Specific Settings

Parameter	Description
<b>Own Policy Server Objects</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables cluster-specific policy server objects. It introduces the nodes <b>entegra Policy Objects</b> (containing files <b>Welcome Message</b> , <b>Personal Firewall Rules</b> , <b>Pictures</b> and <b>Registry Checks</b> ), as well as <b>Policy Service Trustzones</b> below <b>Multi-Range &gt; &lt;rangename&gt; &gt; &lt;clustername&gt; &gt; Cluster Settings</b> . For detailed information see <b>Configuration Service - Section Policy Based Routing</b> , page 69.
<b>Own Shaping Trees</b>	Setting to <b>yes</b> (default: <b>no</b> ) enables cluster-specific traffic shaping settings. It introduces the file <b>Range Shaping Trees</b> below <b>Multi-Range &gt; &lt;rangename&gt; &gt; &lt;clustername&gt; &gt; Cluster Settings</b> . For detailed information see <b>Configuration Service - 2.2.6 Traffic Shaping</b> , page 81.
<b>Send Statistics to Reporter</b>	Setting to <b>yes</b> triggers the management centre to forward statistics files collected from managed boxes within this cluster to a <b>netfence reporter</b> . For this to work, parameter <b>Collect Statistics</b> (see above) has to be set to <b>yes</b> as well and the <b>MC-Reporter</b> service has to be installed (see 18. MC Reporter, page 477). Setting <b>like-range</b> (default) inherits the settings from the <b>Range Config</b> file (see <b>Send Statistics to Reporter</b> , page 417).

### 6.5.1.1 Creating a Cluster Server

To create a cluster server, open the context menu of the configuration tree item **Virtual Servers** and select **Create Server ...**. Insert the name of the cluster server in the now opened dialogue and confirm by clicking the **OK** button, which opens the configuration dialogue. The configuration of a cluster server is identical with the configuration of a server on a netfence gateway (**Configuration Service - 3. Configuring a New Server**, page 94), except that network objects may be referenced in the Server Address fields (**Firewall - 2.2.4 Network Objects**, page 140).

Fig. 18-44 Creating a cluster server with referencing Server IP addresses to network objects



### 6.5.1.2 Creating a Shared Service

To create a shared service (also known as Cluster Service), open the context menu of the configuration tree entry **<clustername> > Shared Services**. Insert a cluster service name and confirm it by clicking the **OK** button. This opens the configuration dialogue.

The configuration of a shared service is identical to the configuration of a service on a netfence gateway

(**Configuration Service** - 4. Introducing a New Service, page 97).

However, some differences need our attention:

**List 18-20** Creating a Cluster Service - section Service Definition

Parameter	Description
<b>Software Module</b>	For a cluster service only three software modules are available: <ul style="list-style-type: none"> <li>➤ <b>DNS</b> (default), for configuration information see <b>DNS</b>, page 315</li> <li>➤ <b>Firewall</b>, for firewall configuration information see <b>Firewall</b>, page 123. For specific firewall configuration information see 6.11 Supplement - Configuring the Cascaded Firewall (cfirewall), page 425 in this chapter.</li> <li>➤ <b>SNMPd</b>, for configuration information <b>SNMP</b>, page 479</li> </ul>

**List 18-21** Creating a Cluster Service - section Admin Restrictions

Parameter	Description
<b>Administered by</b>	This parameter specifies the administrators allowed to manage the cluster. The default setting <b>all-authorized</b> permits management for each configured administrator. The second available setting is <b>restricted-set</b> . Selecting this option enables the parameter <b>Privileged Admins</b> .
<b>Privileged Admins</b>	Via this parameter the administrator explicitly allowed to manage the cluster is specified. Therefore, simply enter the phion.a login name of the corresponding administrator and click the <b>Insert ...</b> button in order to add him to the listing to the right. Via <b>Change</b> you may edit an already existing name. Select the wanted entry, modify the spelling and click <b>Change</b> in order to add the new name to the listing. By selecting an existing entry and clicking <b>Delete</b> , the admin is removed from the list and thus, after activating the changes, is no longer able to administer the cluster service.

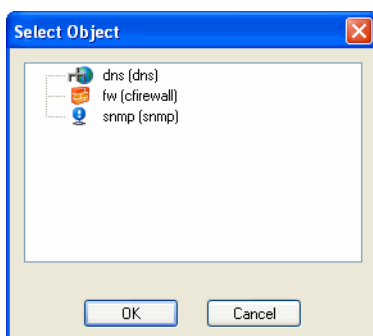
**List 18-22** Creating a Cluster Service - section Access Notification

Parameter	Description
	Beside the standard parameters <b>Service Default (Success)</b> and <b>Service Default (Failure)</b> (known from netfence gateway service configuration, see <b>Configuration Service</b> - 4. Introducing a New Service, page 97) the access notification offers success and failure parameters for each of the 3 possible admin-access-notification profiles.

### 6.5.1.3 Adding a Shared Service

Once a Shared Service has been created, it can be added to a Cluster Server. To add a Cluster Service to a Cluster Server browse to **Multi-Range** > **<rangename>** > **<clustername>** > **Virtual Servers** > **<servername>**, right-click the server node and select **Add Shared Service ...** from the context menu. A new window pops up, allowing selection of the respective service. Mark the service and click the **OK** button.

**Fig. 18-45** Adding a Cluster Service



The Cluster Service is added to the Service node below the Cluster Server. **<DNS\_servername>** (**dns**) and **<SNMPd\_servername>** (**snmp**) service nodes are created as links to the unique Cluster Service below the Cluster Service node. The same applies to the global settings of the **<cfirewall\_name>** (**cfirewall**) node. The Cascaded Firewall Specific node is the only object, which has to be configured below the **<servername>** > **Assigned Services** node directly, as settings made here apply per server and not per cluster (see 6.11.4 The Local Rules Section and The Special Rules Section, page 426).

## 6.5.2 Cluster-specific Settings

### 6.5.2.1 Cluster-specific Cook Settings

Take into consideration that specific cook settings are only available if the parameter **Specific Cook Settings** (see 6.5.1 Creating a New Cluster, page 417) is set to **yes**.

For information concerning the parameters available in this configuration file, please have a look at 9.3.3 Cluster Specific Settings, page 439.

### 6.5.2.2 Cluster-specific Event Settings

Take into consideration that specific cook settings are only available if the parameter **Specific Event Settings** (see 6.5.1 Creating a New Cluster, page 417) is set to **yes**.

For information concerning the parameters available in this configuration file, please have a look at 10.3.3 Cluster-specific Event Settings, page 445.

## 6.6 Box Configuration

The smallest configuration entity in the management centre configuration tree is the **Box**. A box is *one* operative netfence gateway.

**Note:**  
The configuration of a box in the management centre configuration tree affects only the respective box.

For configuration information have a look at **Configuration Service**, page 41.

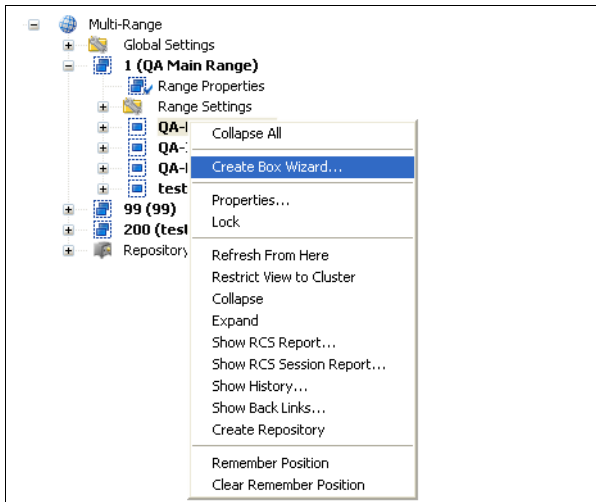
Default settings and availability of services, which can be installed and configured on each box, are determined by **OS Platform**, **Product Type** and **Appliance Model** settings (page 52) of the box. Have a look at **Getting Started** - 2.5 phion Multi-Platform Product Support, page 16 to find out about each type's typical characteristics.

## 6.6.1 Create Box Wizard

To create a new box you can right-click **Boxes** and select **Create Box...** from the context menu (see **Configuration Service - 2.2.2 Box Properties**, page 51) or you use the Create Box wizard:

- Right-click the range or the cluster where you want to introduce the new box
- Select **Create Box Wizard...** from the context menu

Fig. 18-46 Box configuration - wizard for creating a box



- **Lock** the configuration
- Click **Run (F5)**
- Follow the steps of the wizard and set all required parameters. For the description of the box parameters see **Configuration Service - 2.2 Setting up the Box**, page 49. The wizard consists of the following steps:

### Step 1 Start

### Step 2 Product Selection

### Step 3 Administrative Setup

### Step 4 DNS Setup

### Step 5 Time Setup

### Step 6 Network Interfaces

### Step 7 Network Basic

### Step 8 Network Advanced

### Step 9 Remote Access

- **xDSL**
- **DHCP**
- **ISDN**
- **UMTS**

### Step 10 Box Misc

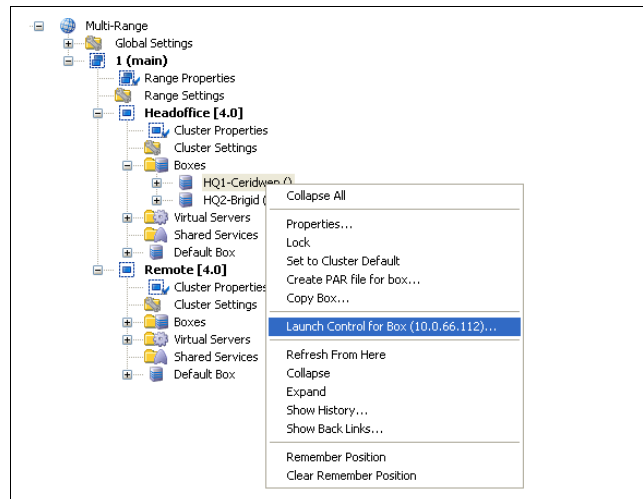
- **MSAD Authentication**
- **MSCHAP Authentication**

### Step 11 Server Assignment

## 6.6.2 Launching a Box

To switch from the MC to a box right-click the desired box and choose **Launch Control for Box (<box IP address>)** from the context menu.

Fig. 18-47 Box configuration - launch control for box



## 6.7 Defining Node Properties

For additional access restriction, the MC offers the context menu entry **Properties...** for each item of the configuration tree.

List 18-23 management centre Node Properties

Parameter	Description
<b>Name</b>	purely informational; displays name of the service's software module
<b>Description</b>	purely informational; displays a short description for the software module
<b>Created</b>	purely informational; displays date/time, admin, admin IP of service creation
<b>Last Modified</b>	purely informational; displays date/time, admin, admin IP of last modification
<b>Release</b>	netfence release version installed on the box (only netfence versions 3.4, 3.6, 4.0 and 4.2 are supported in multi-release environments).

List 18-24 management centre Node Properties - section Administrative Level

Parameter	Description
<b>Your Level</b>	purely informational; displays your administrative level.
<b>Read</b>	By entering the corresponding configuration level, the read permission is specified. <b>Note:</b> Any level lower than the set one has access. (see 8.3.1 Creating a New Admin Profile, page 433)
<b>Write</b>	By entering the corresponding configuration level, the write permission is specified. <b>Note:</b> Any level lower than the set one has access. (see 8.3.1 Creating a New Admin Profile, page 433) Click <b>Change</b> to save the new configuration.
<b>Modify Event</b>	This menu specifies the type of event notification if the corresponding file is modified. Available notification types are: <ul style="list-style-type: none"> <li>➤ <b>No Event</b> (default)</li> <li>➤ <b>Normal Event</b> (generates event <b>Config Node Change Notice</b> [2400])</li> <li>➤ <b>Notice Event</b> (generates event <b>Config Node Change Warning</b> [2401])</li> <li>➤ <b>Alert Event</b> (generates event <b>Config Node Change Alert</b> [2402])</li> </ul>



List 18-24 management centre Node Properties - section Administrative Level

Parameter	Description												
<b>History</b>	states configuration actions performed on this entity; administrator and peer IP are logged:												
	<table border="1"> <thead> <tr> <th>Entry</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>param</td> <td>when changes to the read or write level were made</td> </tr> <tr> <td>lock</td> <td>when conf entity was locked</td> </tr> <tr> <td>unlock</td> <td>when conf entity was unlocked</td> </tr> <tr> <td>change</td> <td>when conf entity was changed</td> </tr> <tr> <td>add</td> <td>when a server/service object was added to the conf tree</td> </tr> </tbody> </table>	Entry	Description	param	when changes to the read or write level were made	lock	when conf entity was locked	unlock	when conf entity was unlocked	change	when conf entity was changed	add	when a server/service object was added to the conf tree
Entry	Description												
param	when changes to the read or write level were made												
lock	when conf entity was locked												
unlock	when conf entity was unlocked												
change	when conf entity was changed												
add	when a server/service object was added to the conf tree												

## 6.8 Repositories

For increased configuration comfort, **configuration repositories** can be defined.

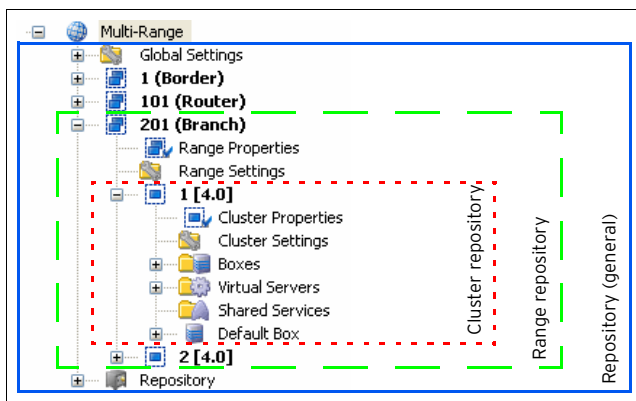
Configuration data that is used on more than one machine should be stored in a repository. This saves time and reduces configuration errors, since the information is entered only once and is then linked from the corresponding repository. Three types of repositories exist:

- **Cluster Repository**
- **Range Repository**
- **General Repository**

Cluster repositories should be used for saving cluster specific configuration data, while range repositories should contain configuration data for boxes of the whole range.

The general repository can be used for saving configuration data, which can be used on all boxes that are introduced by the management centre.

Fig. 18-48 Different types of repositories



**Note:**

Due to compatibility reasons, two nodes are structured in a different way in box repository tree than within box range tree configuration:

- **Authentication Service** is placed in **Advanced Configuration** and not in **Infrastructure Services**
- **System Settings** is placed in **Box** and not in **Advanced Configuration**

## 6.9 Multiple Releases

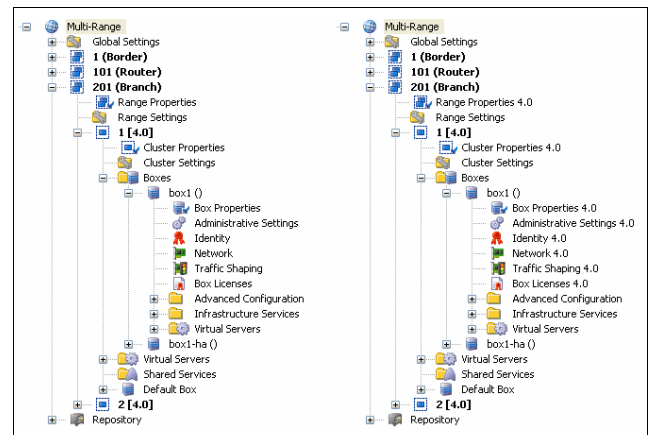
A netfence gateway management centre 4.2 is equipped with the ability to manage netfence gateways installed with release versions 3.4 and higher. Especially in huge network environments, where ad hoc migration of all systems to the recent version simultaneously cannot be accomplished, this feature enables easy and up-to-date administration.

### 6.9.1 Administering Multiple Releases

The smallest administration entity demanding uniform software versions is a cluster. When creating a new cluster (see 6.5.1 Creating a New Cluster), the software release version has to be specified. Every box that is introduced to a cluster is then expected to work with the same release version.

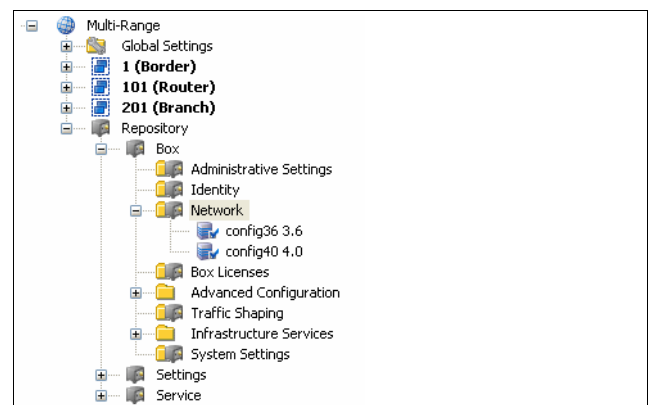
To verify the version number bound to each configuration node, select **Toggle Release View** from the context menu available through right-clicking the configuration tree entry **Multi-Range**. The release information is then displayed to the right of each configuration node.

Fig. 18-49 Configuration tree displayed in default view (left) and with toggled release view (right)



As only one repository can be created per configuration entity (global repository, range/cluster repository), repositories cannot be equipped with version numbers as whole. Thus, not the repositories themselves, but the objects created in them are assigned with version information (figure 18-50).

Fig. 18-50 Repository objects flagged with version information



Just like boxes, ranges and clusters repository objects can be migrated to a newer version (see 6.9.3.4 Migrating a Repository Object).

When administering a multi-release environment use the release view to identify system information versions easily in order to

- install correct hotfixes and updates through the Software Update Tab (see 5.11 Software Update Tab, page 405);
- prepare netfence 3.4/3.6/4.0 version gateways for update to the recent version 4.2.
- verify object version numbers in the repositories.

## 6.9.2 Updating to the Recent Version

Before migrating the configuration, each gateway has to be updated to the recent software version. Execute the software update in the Software Update Tab (see 5.11 Software Update Tab, page 405).

### Note:

Keep in mind that when updating netfence gateways to the recent version 4.2, software update has to be accomplished per cluster. Once the decision for updating has been made, the software update has to be executed for all boxes within a cluster, before the cluster can be migrated and again be managed by the management centre.

## 6.9.3 Migrating the Configuration

### Note:

Migration can only be executed to the applicable succeeding software release version (that means gateways installed with netfence 3.4 have to be migrated to version 3.6 first, before they can be migrated to version 4.0 and then to version 4.2).

As the minimum administration entity in a multi-release environment is a cluster, migration has to be performed in one step for at least one whole cluster within a range. Migration can be initiated from various locations in the configuration tree:

- **Migrate Cluster**  
in the right-click context menu of the locked node **Multi-Range** > <rangename> > <clustername>
- **Migrate Range**  
in the right-click context menu of the locked node **Multi-Range** > <rangename>
- **Migrate Clusters, Migrate Ranges, Migrate Complete Tree**

in the right-click context menu of the node **Multi-Range**

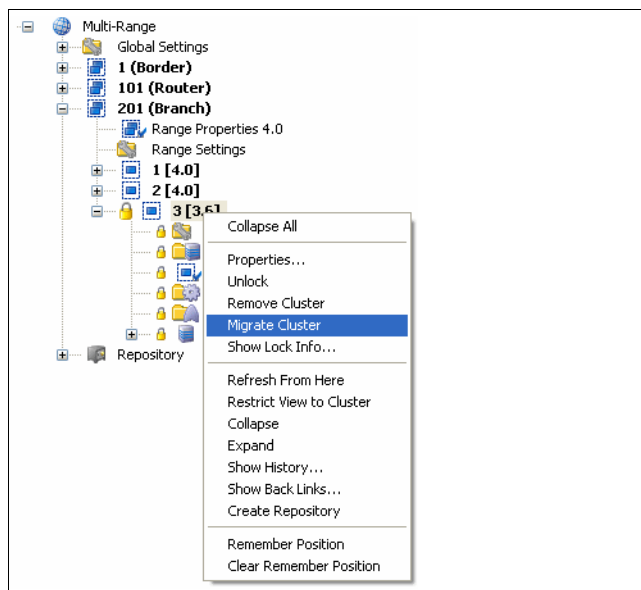
### Note:

Clicking Migrate Cluster(s), Range(s), Complete Tree migrates the configuration but does not activate the new configuration on the spot. Instead, it flags all configuration nodes, which the migration process is going to change. Click the **Activate** button to activate the new configuration (see example Migrating a Cluster).

### 6.9.3.1 Migrating a Cluster

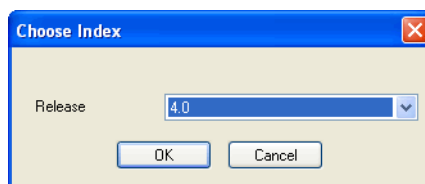
#### Step 1 Lock the cluster and select Migrate Cluster from the context menu

Fig. 18-51 Migrating a cluster - Step 1



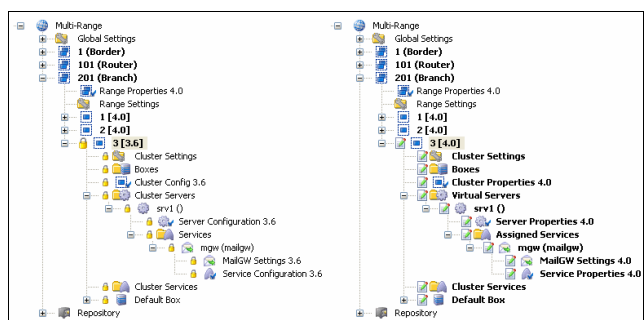
#### Step 2 Choose the software version number as migration destination

Fig. 18-52 Migrating a cluster - Step 2



#### Step 3 Review the future configuration

Fig. 18-53 Example: Mail-Gateway configuration nodes prior to and after Migrate Cluster activation

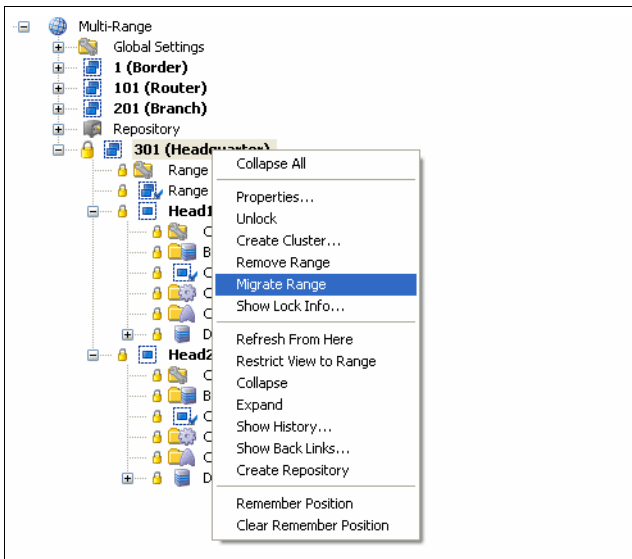


As indicated in figure 18-53, the MailGW Settings and the Service Configuration nodes will be changed during the



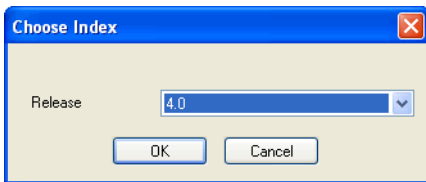
**Step 1** Lock the range and select **Migrate Range** from the context menu

Fig. 18-54 Migrating a range - Step 1



**Step 2** Choose the recent software version number as migration destination

Fig. 18-55 Migrating a range - Step 2



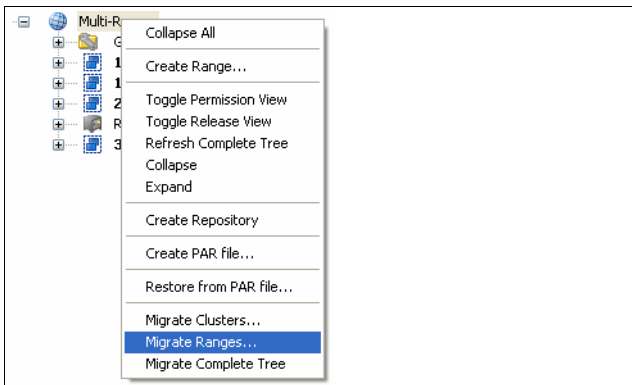
**Step 3** Click **Activate**

Click **Activate** to activate the new configuration.

**6.9.3.3 Migrating Multiple Clusters/Ranges**

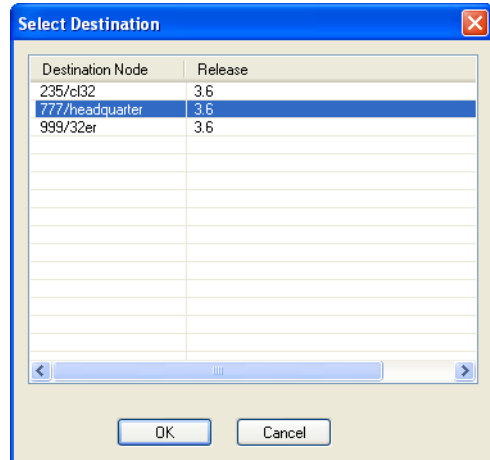
**Step 1** Select **Migrate Clusters/Ranges** from the context menu

Fig. 18-56 Migrating multiple clusters/ranges - Step 1



**Step 2** Select nodes to be migrated

Fig. 18-57 Migrating multiple clusters/ranges - Step 2



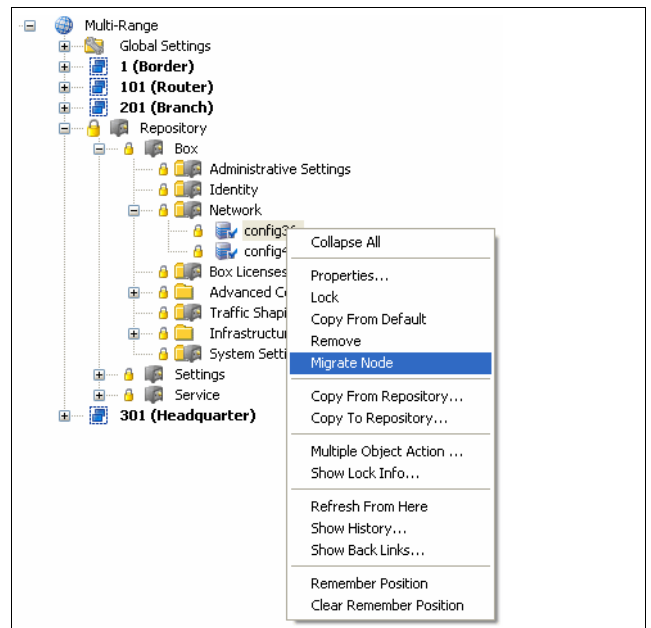
**Step 3** Click **Activate**

Click **Activate** to activate the new configuration.

**6.9.3.4 Migrating a Repository Object**

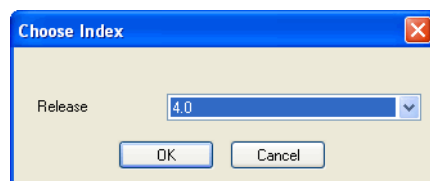
**Step 1** Lock the object and select **Migrate Node** from the context menu

Fig. 18-58 Migrating a repository object - Step 1



**Step 2** Choose the recent software version number as migration destination

Fig. 18-59 Migrating a repository object - Step 2



**Step 3** Click **Activate**

Click **Activate** to activate the new configuration.

## 6.9.4 Preparing Repository Linked Box Configurations for Migration

In most cases box configuration details will at least have been partly linked to repositories for easier administration purpose. When migrating a netfence release, special regard should be paid to these links in order to maintain the future administration structure as simple as it was.

Similar to moving/copying managed boxes (see below), if a version 3.4 cluster accessing configuration files in 3.4 version repository objects is migrated, the links cannot be maintained. The object file's contents will instead be written to a file.

If a repository object cannot be migrated because it is still in use by version 3.4 boxes, proceed as follows to maintain linked configurations:

**Step 1** Create a version 4.2 repository object with the same configuration settings as the former object.

**Step 2** Migrate the configuration.

**Step 3** Delete the configuration files, which have been created when migrating.

**Step 4** Create new links from the configuration nodes to the up-to-date repository object.

### Note:

Repository migration can only be executed to the applicable succeeding software release version (that means 3.4 version repositories have to be migrated to version 3.6 first, before they can be migrated to version 4.0 and then to version 4.2).


## 6.10 Adding/Moving/Copying

### 6.10.1 Adding Boxes

Proceed as follows to add a box to an MC:

#### 6.10.1.1 Create Box ...

Use this method to prepare a new box for installation.

**Step 1** Open the  Boxes context menu MC range/cluster the box should live in and select *Create Box ...*

**Step 2** Define a *Box Name*

**Step 3** Configure the *Box Config* file (see **Configuration Service** - 2.2.2 Box Properties, page 51 for details).

**Step 4** Configure the box (see **Configuration Service** - 2. Configuring a New System, page 48 for details). Confirm your settings by clicking the *Activate* button.

**Step 5** Create a PAR file of the box

by selecting *Create PAR file for box ...* from the context menu

**Step 6** Create a kickstart file with phion.i using the option *Create Kickstart only (Getting Started - 2.2 Creating a "standard" Kickstart Disk, page 10)*.

**Step 7** Install the box using kickstart disk and PAR file (**Getting Started - 1.3 Installation with a Saved Configuration, page 8**).

### 6.10.1.2 Import Box from PAR

This method assumes that a PAR file exists of the box, which is going to be added. Use it when adding an already installed and configured box to the MC.

**Step 1** Create a PAR file of the to-be-added box

**Step 2** Select the MC range/cluster the box should live in

**Step 3** Open the  Boxes context menu and select *Import Box from PAR ...*

**Step 4** Enter a new, UNIQUE name for the box (maximum 25 characters)

**Step 5** Commit your selection via OK button and have the box moved

### Attention:

Box servers and services will only be added if NO name violation occurs. In case of already existing configuration entities with the same name, servers and services will not be added to the MC configuration.

### 6.10.2 Moving/Copying Managed Boxes, Servers and Services

### Attention:

Due to the hierarchal structure of repositories, it may happen that configurations linked from a repository are written to a file and, thus, are no links anymore.

**Table 18-16** Moving/Copying Managed Boxes, Servers and Services

Repository	Move/copy to diff. range	Move/copy to diff. cluster
General	Link remains	Link remains
Range	File is written	Link remains
Cluster	File is written	File is written

### Note:

The following describes moving a managed box within an MC. However, copying/moving servers and services is the same as mentioned in the following.

**Step 1** Enter MCs configuration tree and select the box you want to move

**Step 2** Open context menu and select *Move Box ...*

**Step 3** Select the new box location from the displayed list and enter a new, **UNIQUE** name for the box (maximum 25 characters)

**Step 4** Commit your selection via **OK** button and have the box moved

## 6.11 Supplement - Configuring the Cascaded Firewall (cfirewall)

The Cascaded Firewall (cfirewall) is a so-called cluster service. It is a variant of the phion netfence firewall specially designed to simplify firewall administration by multiple administrators. The cfirewall includes all features of the netfence firewall. Unlike the common firewall service, though, the cfirewall is not only organised into one rule set, but can include up to three rule sets. As a result, the firewall rule set topology provides three organisational scopes:

- **Global Rules** (see 6.11.3 The Global Rules Section)
- **Local Rules** (see 6.11.4 The Local Rules Section)
- **Special Rules** (see 6.11.5 The Special Rules Section)

### 6.11.1 Hierarchical Structure of Rule Sets

#### Global Rules

The Global Rule set is the first rule set considered in the cfirewall configuration. It manages rules valid for all cfirewall services within a specific cluster.

**Local** and **Special Rules** are coequal but both come after Global Rules. Local and Special rules can only work with **network objects** that have been cascaded to them from the Global Rules section.

Fig. 18-60 Cascading the localnet network object

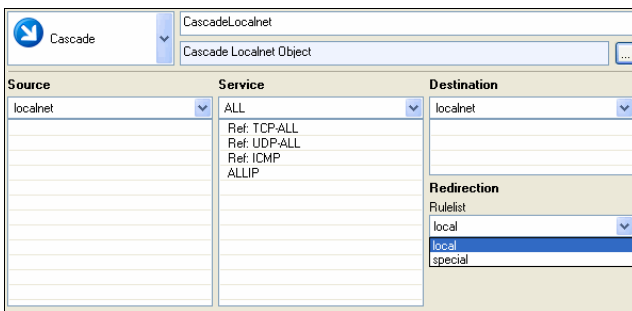
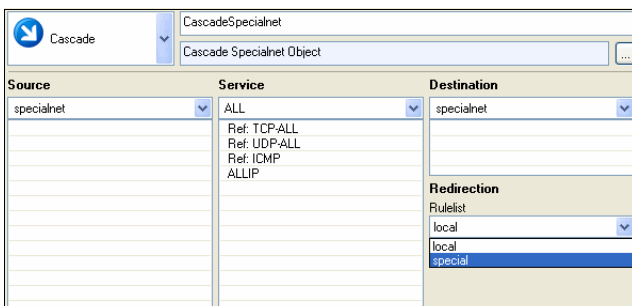
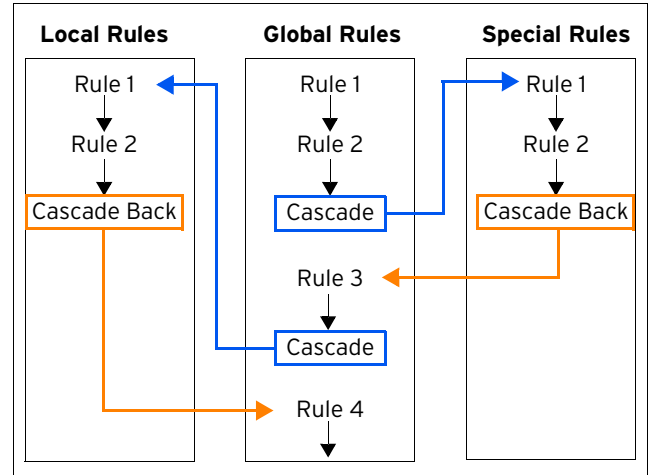


Fig. 18-61 Cascading the specialnet network object



The following scheme depicts the organisational structure of rule sets. Note, that the workflow of rules in the Global Rules section is intercepted through cascading to either Special or Local Rules section. As final step, from there the workflow is returned to the Global Rules section with a **Cascade Back**.

Fig. 18-62 Workflow of rule set processing



For further information on Cascaded Rules see **Firewall - 2.5 Cascaded Rule Sets**, page 160.

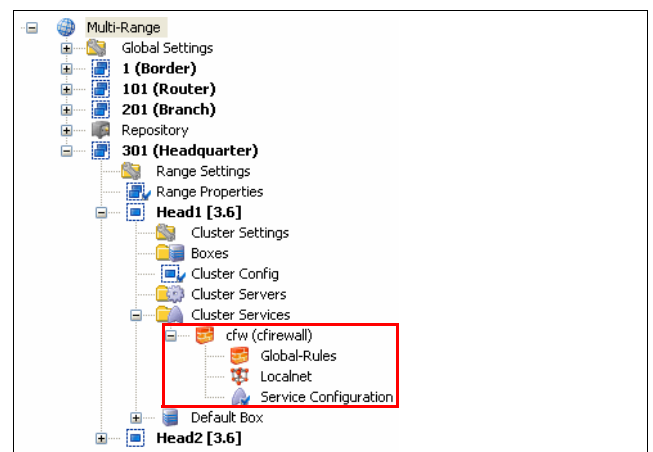
### 6.11.2 Creating a Cascaded Firewall

For general information how to create a **Shared Service**, please refer to 6.5.1.2 Creating a Shared Service, page 418.

The creation of the **Cascaded Firewall Cluster Service (cfirewall)** itself takes place in the following steps:

#### Step 1 Creation of the cfirewall service

Fig. 18-63 Configuration nodes of the cfirewall service - Global section





Beside the general **Service Properties** node (**Configuration Service - 4. Introducing a New Service**, page 97), installation of the cfirewall service generates the following sub-node:

- **Global-Rules** (see Global-Rules Node)
- **Localnet** (see Localnet Node)

#### Step 2 Adding the cfirewall service to a server

For description how to add a Cluster Service to a server, please refer to 6.5.1.3 Adding a Shared Service, page 419.

Adding the cfirewall service to a server generates the following sub-nodes below  `<servername>` >  **Cluster Services:**






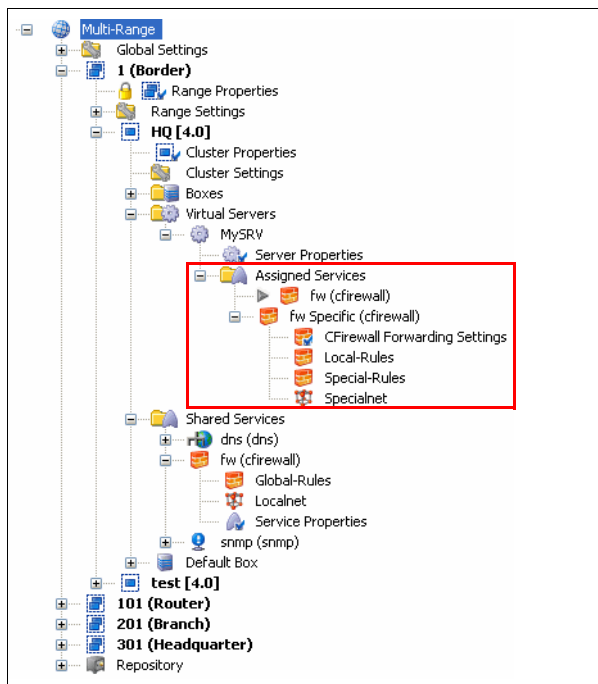
- a link to the Cluster Service Configuration below the Cluster Services node the  `<cfirewall_name Specific (cfirewall)>` node with following sub-nodes:
  -  **Cfirewall Forwarding Settings (Firewall - 2.1.2 Firewall Forwarding Settings, page 131)**
  -  **Local-Rules** (see The Local Rules Section)
  -  **Special-Rules** (see The Special Rules Section)
  -  **Specialnet** (see Specialnet Node)

Fig. 18-64 Configuration nodes of the cfirewall service - Server section



## 6.11.3 The Global Rules Section

### 6.11.3.1 Global-Rules Node

In the Global Rules section, rules valid for all cfirewall services bound to a specific cluster service are managed. To simplify maintenance, the global rules node can be linked into a repository. A consistent rule set architecture can thus be set up and administered.

### 6.11.3.2 Localnet Node

The Localnet configuration area serves for specification of **Trusted Local Networks**. These trusted networks are determined for cluster-service-wide use. Every value entered in the Trusted Local Networks dialogue results in an entry in the Network Object **localnet** in the Global Rules section.

#### Note:

The values entered into the Trusted Local Networks configuration window are not visible in the configuration dialogue of the Network Object **localnet**.

#### Note:

To enable configuration of specific rules related to trusted networks, the **localnet** network object has to be cascaded to the Local Rules section (see 6.11.1 Hierarchical Structure of Rule Sets, page 425). Do not forget to cascade the object back (**Cascade Back**), if return to the workflow of the Global Rule Set is desired.

## 6.11.4 The Local Rules Section

Local Rules are defined per server-service. They can again contain a complete rule set with full functionality. The Local Rules section is only applicable, if the Global Rules section allows it, that means it has cascaded the **localnet** object to the Local Rules section (see above).

## 6.11.5 The Special Rules Section

Special Rules as well are defined per server-service. The Special Rules section is only applicable, if the Global Rules section allows it, that means it has cascaded the **specialnet** object to the Special Rules section (see below).

### 6.11.5.1 Specialnet Node

The Specialnet configuration area serves for specification of **Special Networks**. **Specialnet** objects are configured below the cfirewall Specific node, and thus only have server-service-wide validity. Every value in the Special Networks dialogue results in an entry in the Network Object **specialnet** in the Global Rules section. A specialnet usually exists of a selective range of IP addresses, which are additionally needed to configure a subset of rules, but are not wanted in the **localnet**.

#### Note:

The values entered into the Special Networks configuration window are not visible in the configuration dialogue of the Network Object **specialnet**.

#### Note:

To enable configuration of specific rules related to special networks, the **specialnet** network object has to be cascaded to the Special Rules section (6.11.1 Hierarchical Structure of Rule Sets, page 425). Do not forget to cascade the object back (**Cascade Back**), if return to the workflow of the Global Rule Set is desired.

**Note:**

**Localnet** objects have **cluster-service-wide** validity. **specialnet** objects have **server-service-wide** validity.

**Note:**

Use the **Locals Rules** section to define rules which can generally be applied to servers within a cluster, and should be maintained centrally. Use the **Special Rules** section to define rules which should only apply to specific server services or network segments.

Local and Special Rules sections are generally suited for administration by distinct administrators. When delegating rule set administration, make sure to set the appropriate user rights on the **Global-, Special- and Local Rules** nodes, and on the **Localnet** and **Specialnet** nodes.

**Note:**

Administration rights for distinct Cascaded Firewall administrators can be set through permissions on the firewall related nodes in the configuration tree. Disallowed configuration areas will be set to read-only respectively.

### 6.11.6 Cascaded Firewall (cfirewall) - Configuration Example

A Holding enterprise owns 10 companies, each of them disposing of 10 locations. Firewalls are installed in every location. Each company has its own IT department. The locations of each company communicate with one another.

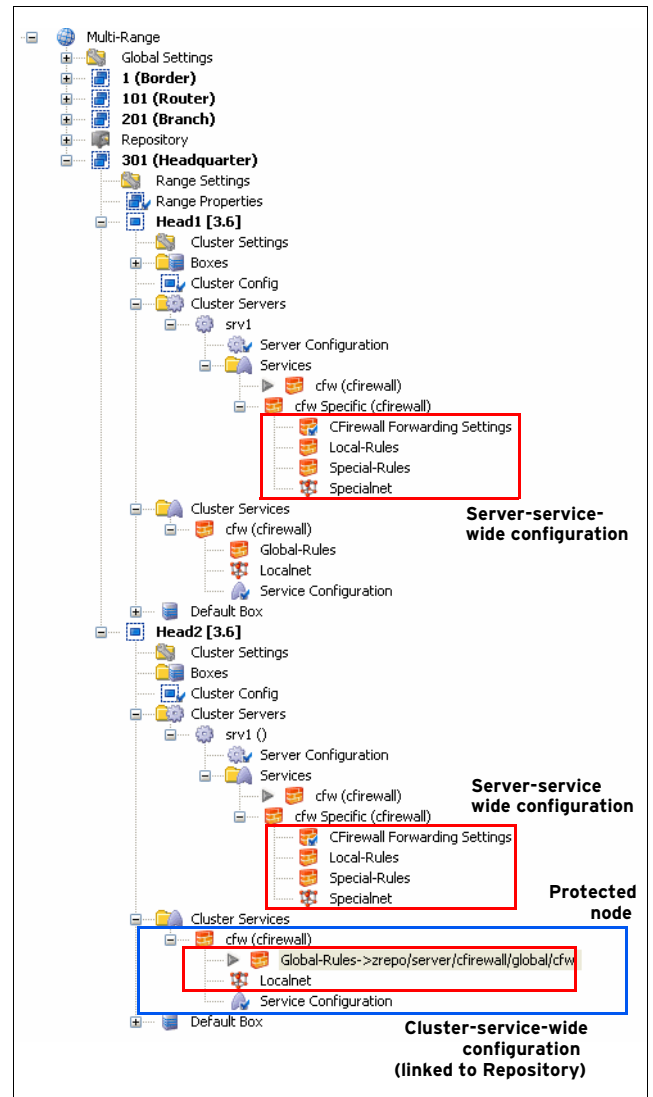
#### 6.11.6.1 Initial Situation

The holding's security policy demands the following general standards to apply:

- POP3 requests to the Internet should always be blocked.
- Internet communication processing is only allowed via gateways (proxies, mail gateways, ...).
- Communication between the Holding itself and its 10 companies (Company A-J) is only allowed to be handled through global security policies (for example only Lotus Notes is allowed).

On basis of these demands, the Cascaded Firewall can be set up as follows:

Fig. 18-65 Exemplary cfirewall setup



- 11 clusters are set up in a range (one cluster for the Holding company itself, the other 10 clusters for each of her companies).
- A cfirewall service is introduced in each cluster.
- The network addresses of Companies A-J and their respective locations are entered into the Trusted Networks of the Holding's Localnet object.
- In the Range Repository, a rule set compliant with the Holding's policy is set up in the Global Rules section.
- The Global Rules sections of the companies' cfirewalls are linked to this Global Rules object in the Range Repository.

Fig. 18-66 Content of the Global Rule Set, which is saved in the Range Repository

Nr.	Name	Source	Service	Destination	Action	Device	User
0	BlockPOP3	localnet	POP3 TCP 110	World 0.0.0.0/32	Block	Matching	
1	gotoHolding	localnet	LOTUS REP TCP 1352	192.168.0.0/8	Pass (Client)	Matching	
2	CompanyInternal	localnet	ALL ALLIP . ECH...	localnet	Cascade(local)	Matching	

- Permissions of Cluster Service node and nodes below are set to read-only, in order to prevent change of

Localnet and link to the Global Rules object in the Range Repository by the IT administrators in the companies (figure 18-65 - Protected node).

- The right to change settings in the Local Rules section is assigned to the IT administrators of the companies.

**Note:**  
With the settings depicted in figure 18-66, only the right to change company internal settings is assigned to the IT administrators, as only the destination object **localnet** is cascaded. Thus, as desired, the IT administrators will not be able to change settings for Internet access, ...

### 6.11.6.2 Special Request 1

Company B needs to open Port 5555 to the Internet for data processing. Data transfer is only needed from company B's headquarter, the software handling the transfer process is installed on two client PCs. On basis of these demands, the following configuration is possible:

- The IP addresses of the two client PCs are added to the **Trusted Networks** in the **Specialnet** object.
- A new cascading rule set allowing connections to port 5555 is added to the Global Rules section.

Fig. 18-67 Cascading of the specialnet network object

Nr.	Name	Source	Service	Destination	Action	Device	Use
0	CascadeToSpecial special	specialnet	TCP 5555	Internet 0.0.0.0/32, N...	Cascade(special)	Matching	
1	BlockPOP3	localnet	POP3 TCP 110	World 0.0.0.0/32	Block	Matching	
2	gotoHolding	localnet	LOTUS REP TCP 1352	192.168.0.0/8	Pass (Client)	Matching	
3	CompanyInternal local	localnet	ALL ALLIP, ECH...	localnet	Cascade(local)	Matching	

- A new rule set, configuring handling of connections over port 5555 is set up in the Special Rules section of Company B.

### 6.11.6.3 Special Request 2

Migration of the e-mail system from Lotus Notes to Exchange Server is planned Holding- and Company-wide. Thus, the rules regarding the companies' communication with the Holding enterprise have to be adapted. On basis of these demands, the following configuration is applicable:

- The rule set handling Lotus Notes communication in the Global Rules section is changed. The Service setting is changed from Lotus Notes to MS Exchange Server.

Fig. 18-68 Rule allowing communication over MS Exchange Server

Nr.	Name	Source	Service	Destination	Action	Device	Use
0	CascadeToSpecial special	specialnet	TCP 5555	Internet 0.0.0.0/32, N...	Cascade(special)	Matching	
1	BlockPOP3	localnet	POP3 TCP 110	World 0.0.0.0/32	Block	Matching	
2	gotoHolding	localnet	MS-EXCHANGE-2000 TCP, UDP	192.168.0.0/8	Pass (Client)	Matching	
3	CompanyInternal local	localnet	ALL ALLIP, ECHO, TCP ...	localnet	Cascade(local)	Matching	

## 6.12 Supplement: Migration of an MC to a New Segment

The task is to move a management centre to a new segment. In the example network, the management centre is to be moved from the net 10.0.8.0/8 to the net 10.0.82.0/8.

**Note:**  
It is assumed that the external IP address of the HQ border firewall (eth1: 172.31.80.3) remains unaffected.

The following network diagrams give an overview of the initial and the planned network configuration.

Fig. 18-69 Initial network situation

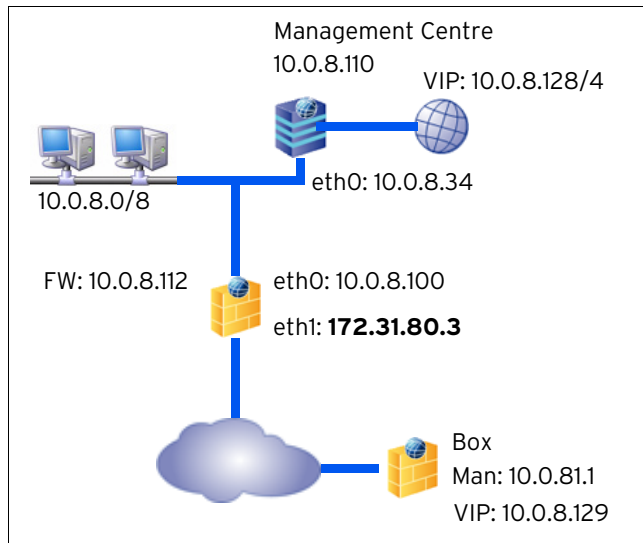
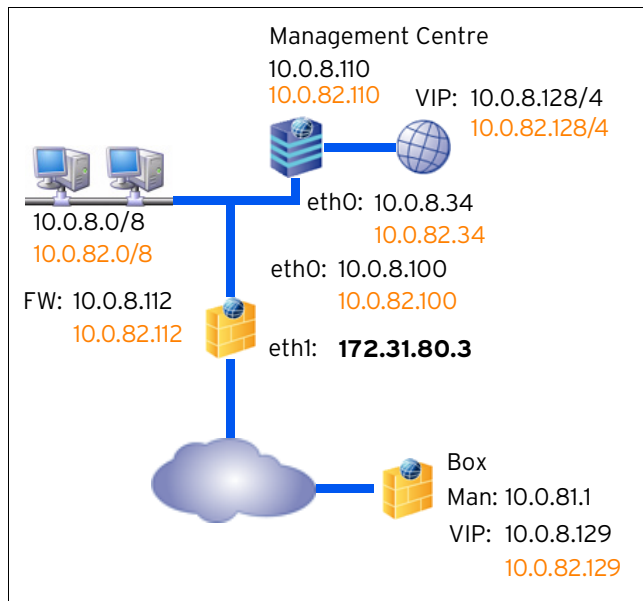


Fig. 18-70 Network after MC migration





## 6.12.1 Preparing the Network for MC Migration to a New Network

The following preliminary steps have to be taken before actual migration of the management centre (MC).

**Note:**

Always remember to acknowledge network configuration changes by clicking **OK**, and to confirm the settings by clicking **Send Changes** and **Activate**.

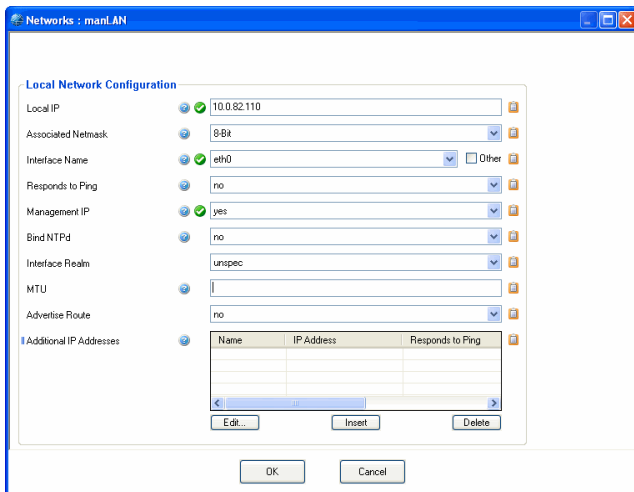
### Step 1 Introduce a new Box IP on the MC

Log into the management centre on box level using the MIP address 10.0.8.110. Introduce an **Additional Box IP** via **Config** > **Box** > **Network** > **Networks** view > section **Additional Local Networks**. In the example the new IP introduced is the address 10.0.82.110.

**Note:**

When introducing the new IP make sure to set the parameter **Management IP** in the Additional Local Networks section to **yes**.

Fig. 18-71 Further Networks configuration dialogue



### Step 2 Introduce a second server IP on the MC box (Server configuration)

Browse to **Config** > **Box** > **Virtual Servers** > <servername> > **Server Properties** > **General** view > section **Virtual Server IP Addresses**. Insert the IP address 10.0.82.34 into the **Second-IP** field.

### Step 3 Activate the new network configuration

Browse to **Control** > **Box** tab and click the **Activate New** button.

### Step 4 Introduce additional Management IPs

Log into the management centre on server level using the MC tab and the MC IP 10.0.8.34.

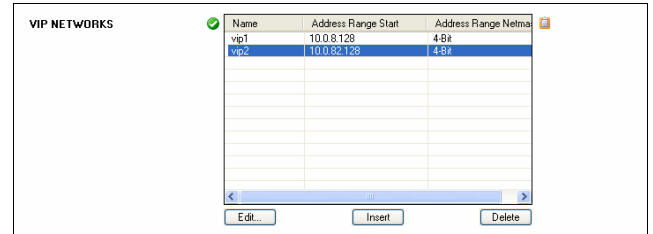
Browse to **Config** > **Multi-Range** > **Global Settings** > **MC Identity** > **General** tab.

Insert the IP addresses 10.0.82.34 and 10.0.82.110 into the field **Additional MC IP Addresses**.

### Step 5 Introduce new Box VIP ranges

While you are still logged on MC level, browse to **Config** > **Multi-Range** > **Global Settings** > **Box VIP Network Ranges**. Introduce the net 10.0.82.128/4 as new Network Range.

Fig. 18-72 Box VIP Network Ranges



### Step 6 Adapt Routing on FW

Open the network configuration of the corresponding firewall via the configuration tree of the MC and set the Standard Routing (Config) to the new LAN (for example manLAN: 10.0.82.0/8).

Confirm the new settings by clicking **Send changes** and **Activate**.

**Note:**

If you are migrating a HA (High Availability) system, do not forget to apply the changes on the HA partner as well.

### Step 7 Introduce the additional Server IP on the Firewall (FW)

On the netfence gateway employing the firewall browse to **Config** > **Box** > **Servers** > <servername> > **Server Properties** > **General** view > section **Virtual Server IP Addresses**. Insert the IP address 10.0.82.100 into the **Additional IP** field.

**Note:**

If you are migrating a HA (High Availability) system, do not forget to apply the changes on the HA partner as well.

### Step 8 Introduce additional FW rule sets on the HQ border firewall

Only rules concerning the redirection of the remote management tunnels have to be adapted. Clone the needed existing rule sets, and perform the necessary changes on the clones.

### Step 9 Ensure correct routing from the remote boxes to the MC

### Step 10 Ensure external management access

To maintain connectivity when changing the VIP or in case of a remote management settings misconfiguration, make sure to configure management accesses to all boxes that work independently of the management VPN tunnels (for example define external management IPs on all boxes of the branch offices).

### Step 11 Activate the new network configuration

Log into the management centre on box level. Browse to **Control** > **Box** tab and click **Activate New**.

## 6.12.2 Migrating the MC to a New Network

### Note:

Administration of boxes will not be possible until the next to be taken steps are thoroughly accomplished and migration is completed.

To relocate the MC to its new environment proceed as follows:

### Step 1 Check Configuration Updates for successful completion

Log into the management centre on server level using the MC tab and the new MC IP 10.0.82.34.

Browse to **Control** > **Configuration Updates** tab and check the update status messages in the list for all boxes bound to the management centre. Do not proceed with the following steps unless all updates have been completed successfully.

### Step 2 Reconfigure remote managed boxes

Browse to **Config** > **Multi-Range** > **<rangenname>** > **<clustername>** > **Boxes** > **Box** > **Network** > **Management Access** view > **Remote Management Tunnel** section

Change the following network parameters:

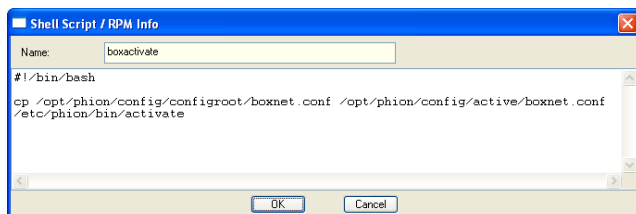
- Virtual IP (VIP)  
Switch the Virtual IP from 10.0.8.129 to 10.0.82.129.
- Tunnel Details  
Switch the **Target Networks** from 10.0.8.0/8 to 10.0.82.0/8.  
Switch the **Reachable IPs** from Server IP 10.0.8.34 to 10.0.82.34 and MIP 10.0.8.110 to 10.0.82.110.

### Step 3 Activate the new network configuration on the boxes

Browse to **Control** > **Box Execution**.

Click **New Script** to generate a script for activation of the new network configuration on all boxes.

Fig. 18-73 Shell script "boxactivate" for box network activation



Name the script for example **boxactivate**.

Add the following lines to it:

```
#!/bin/bash
cp /opt/phion/config/configroot/boxnet.conf
/opt/phion/config/active/boxnet.conf
/etc/phion/bin/activate
```

Execute the script by selecting it in the **Scripts** tab and simultaneous selection of the boxes where it is to be executed in the window left to the Scripts tab. While all needed objects are selected click the **Create Task** button in the **Selected Boxes** section. The script is now executed.

### Step 4 Check Configuration Updates for successful completion

Browse to **Control** > **Configuration Updates** tab and check the update status messages for successful completion of box network activation.

### Step 5 Set the new MC IPs

To assure that the correct MC IP address is used for communication, interchange the Management IPs created above in Step 4 Introduce additional Management IPs (see above).

Switch the MC IPs 10.0.8.34 and 10.0.8.110 with the additional MC IPs 10.0.82.34 and 10.0.82.110 respectively.

### Step 6 Delete obsolete rule sets on the HQ border firewall

Delete the former rule sets on the HQ border firewall, which have been replaced through introduction of additional r sets bound to the new IPs in "Step 8 Introduce additional FW rule sets on the HQ border firewall" (see above).

### Step 7 Assert the new network configuration

Log into the management centre on box level using the Box tab and the MIP 10.0.82.110.

Browse to **Control** > **Box** tab and click the **Activate New** button. Select **Soft** activation from the available options.

### Step 8 Perform a complete update via the management centre

Log into the management centre on server level using the MC tab and the MC IP 10.0.82.34

Browse to **Control** > **Configuration Updates** tab. Click the **Update Now** button.

## 7. MC Database

### 7.1 Database User Interface

To access the the *Database* user interface, log in to the MC on server level and select  *Database* from the box menu.

The MC Database area gives an overview of all ranges, clusters, boxes, servers, and services the management centre administers. The view is purely informational. Double-clicking an entry in any tab listing, opens the selected object in the configuration tree of the MC.

The following tabs are available for operational purposes:

- **Range** tab                    see 7.2 Range Tab, page 431
- **Cluster** tab                    see 7.3 Cluster Tab, page 431
- **Box** tab                            see 7.4 Box Tab, page 431
- **Server** tab                    see 7.5 Server Tab, page 431
- **Service** tab                    see 7.6 Service Tab, page 431

**Note:**

The button bar on top of the window is void of any functionality and may be ignored.

### 7.2 Range Tab

This tab provides information concerning all ranges that are managed via the management centre. The shown information is a summary of the input that was given during creation of the ranges and is split into columns that are named accordingly to the parameters of the Range Configuration (see 6.4 Range Configuration, page 416).

### 7.3 Cluster Tab

This tab provides information concerning all clusters that are managed via the management centre. The shown information is a summary of the input that was given during creation of the clusters and is split into columns that are named accordingly to the parameters of the Cluster Configuration (see 6.5 Cluster Configuration, page 417).

### 7.4 Box Tab

This tab provides information concerning all boxes that are managed via the management centre. The shown information is a summary of the input that was given during creation of the boxes and is split into columns that are named accordingly to the parameters of the Box Configuration (see 6.6 Box Configuration, page 419).

### 7.5 Server Tab


This tab provides information concerning all servers that are managed via the management centre. The shown information is a summary of the input that was given during creation of the servers and is split into columns that are named accordingly to the parameters of the Server Configuration (**Configuration Service** - 3. Configuring a New Server, page 94).

### 7.6 Service Tab

This tab provides information concerning all services that are managed via the management centre. The shown information is a summary of the input that was given during creation of the services and is split into columns that are named accordingly to the parameters of the Service Configuration (**Configuration Service** - 4. Introducing a New Service, page 97).

## 8. MC Admins

### 8.1 Introduction

Administrators are managed in the  **Admins** part of the MC.

But before we can start to describe the user interface and its functions, there are some theoretical points that need our attention.

Distinguishing between a stand-alone system and a system within a phion management cluster with MC the **phion Administration Concept (pAC)** offers different services for each system.

Every phion system disposes of the user **root** who has unlimited rights in the entire system. In addition, the user **phion** is granted access to the system via the operating system only.

If you need to work on the phion.a management interface, you may introduce so-called **root aliases**. Within the phion management layer the status of these users is on equal terms with the status of root. On the other hand, there are no root aliases on operating system layer allowing system access to other users than the system users **root** and **phion**. **root** and **root alias** also differ in the authentication mode: For authenticating the alias either a RSA 1024-bit key or a password can be used, whereas **root** is only authenticated through a password.

As all these users are counted among system users, the default access notification scheme that is configured for each particular service automatically applies for them.

**Table 18-17** Default user rights overview

User	Access via phion.a	SSH	Console login	Characteristics
root	yes, password or key	RSA keys, password	yes, password	
phion	no	password	password	default Linux user, UID=9999
root alias	yes, password or key	RSA keys, password	no	optional, deactivation possible

The MD5 password hashes of **root** and **phion** [ UID=9999, group **phion** ] are stored in `/etc/shadow` (operative instance for system access) and in `/opt/phion/config/configroot[active]/boxadm.conf` (global configurative instance, operative instance for system access). Any authentication data of the **root aliases** is stored in these two files.

`libpwn` has been manipulated to disable password changes on the command line via `passwd` for all users. `libpwn` is required by the PAM module `pam_pwn.so` and

is used by default, if the method for password changes requiring authentication via the phion admin DB has not been implemented. The implemented procedure provides for configurational and operational coherence of the authentication data entities.

System access of the user **phion** is recommended for serial access on the box as it is only of restricted use.

In addition to the basic services described above, the scope and the performance of the pAC is significantly broadened and enhanced in combination with a phion multi-administrator MC. Administrators are managed in the management centre and are reported to the phion systems within their executive scope.

For high availability purposes, the administrators **master** and **ha** equivalent to **root** are introduced:

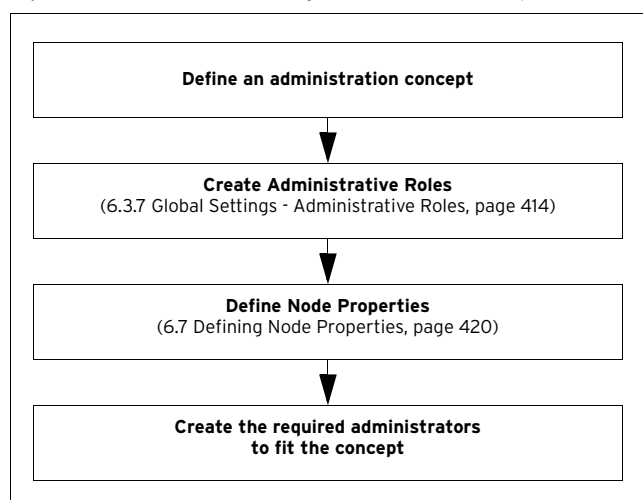
- **ha** is used for data synchronisation of two HA partner systems (for example `fw-sync`).
- **master** is used for configuration updates, status updates, ...

The user does not directly dispose of these admins, however, their names may appear in the corresponding log files of the box configuration daemon.

### 8.2 Concept

The following flowchart gives an overview of the prerequisites that have to be met when creating administrators.

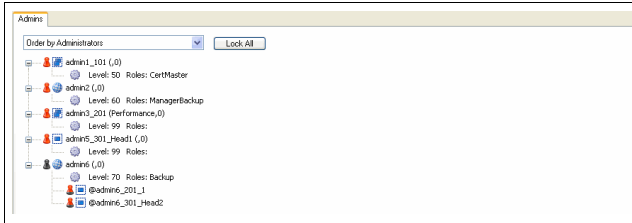
**Fig. 18-74** Workflow for establishing an administration concept



### 8.3 Admin User Interface

To access the the Admin User Interface, log in to the MC on server level and select **Admins** from the box menu.

Fig. 18-75 Admins tab



The user interface is divided into two configurational areas, a button bar on top of the window, and the **Admins** tab in the main window.

The buttons have the following functions:

- **Activate** button  
Clicking **Activate** applies configuration changes.
- **Undo** button  
Clicking **Undo** revokes configuration changes that have not yet been activated.
- **New Entry ...** button  
Clicking **New Entry** allows creating a new administrator profile (see 8.3.1 Creating a New Admin Profile, page 433).
- **Refresh** button  
Clicking **Refresh** updates the view in the **Admin** tab.

In the **Admin** tab existing administrator profiles can be arranged as follows:

- **Order By Administrators**  
Arranges administrator profiles alphabetically by name.
- **Order By Hierarchy**  
Arranges administrative scopes by range and cluster.
- **Order By Roles**  
Arranges administrator profiles by assigned roles.
- **Order By Level**  
Arranges administrator profiles by assigned administrative level.

The icons indicate the following:

Table 18-18 Administration scopes overview

Type	Scope	Characteristics
root [MC cluster]	Entire assembly without right restrictions	root [MC] is inherited from the MC as basic single system (box) of carrier system. <b>Note:</b> The root administrator is not evident in the administrator list, since he is always present in the system and not parameterisable.
	Global administration rights	Not editable.
	Administration rights on dedicated ranges	Not editable.
	Administration rights on dedicated clusters	Not editable.
	Global administration rights (linked)	Editable.

Table 18-18 Administration scopes overview

Type	Scope	Characteristics
	Administration rights on linked ranges	Editable.
	Administration rights on linked clusters	Editable.
	Link information (range)	For information purpose only.
	Link information (cluster)	For information purpose only.

**Note:**  
Icons that are displayed partly transparent indicate inherited, that means linked access permissions.

#### 8.3.1 Creating a New Admin Profile

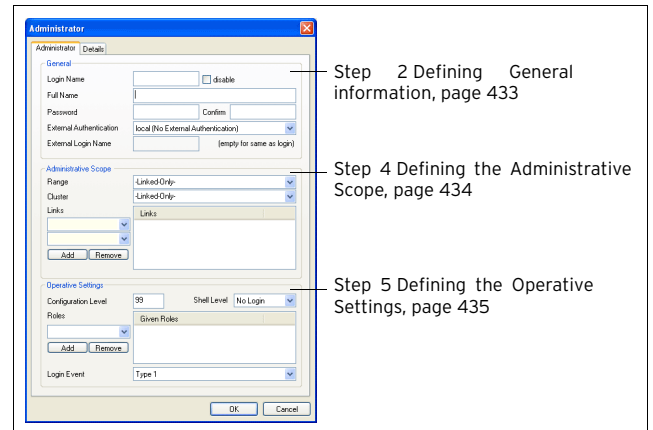
**Note:**  
Create administrative roles (see 6.3.7 Global Settings - Administrative Roles, page 414) and define node properties (see 6.7 Defining Node Properties, page 420) before creating a new administrator profile.

##### Step 1 Locking the data set

Click the **Lock** button to enable content modification in the **Admins** tab.

Then click the **New Entry** button to open the **Administrator** configuration window.

Fig. 18-76 Administrator configuration dialogue



##### Step 2 Defining General information

In the General section the following options are available:

List 18-25 Creating a new administrator - Administrator tab - section General

Parameter	Description
<b>Login Name</b>	Here the administrator's name for the phion.a login is to be defined. <b>Note:</b> A unique ID must be assigned to every administrator. The ID may be adapted to your needs, though the following names may not be used: • root, bin, adm, daemon, lp, system, sync, shutdown, halt, mail, operator, nobody, phion, uucp, as they have a special meaning in the OS • ha, master, as they are already reserved by the phion system.
<b>Full Name</b>	This parameter can hold either the administrator's full name or a description.



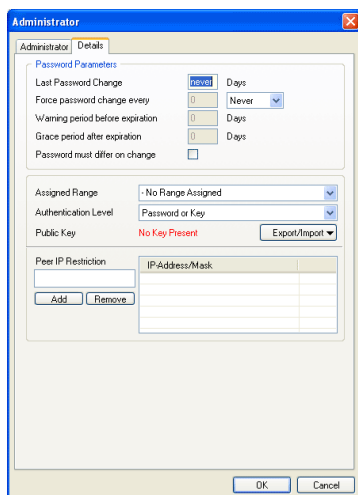
**List 18-25** Creating a new administrator - Administrator tab - section General

Parameter	Description
<b>Password</b>	Via this parameter the password for the phion.a login has to be specified. The password has to be verified by reentering it in the field <b>Confirm</b> . For additional parameters concerning configuration of password/key handling, check Details tab (see below). In addition to the parameters mentioned above, the <b>Basic Data</b> section offers an additional option: ➤ <b>disable</b> checkbox By ticking this check box, the administrators profile is deactivated for further usage. <b>Attention:</b> Please take into consideration that disabling affects the system only as soon as the modified admin configuration is activated.
<b>External Authentication field</b>	If external authentication is required, the corresponding method can be selected here. The following authentication schemes are available: ➤ <b>msnt</b> - see <b>Configuration Service</b> - 5.2.1.6 MSNT Authentication, page 114 ➤ <b>ldap</b> - see <b>Configuration Service</b> - 5.2.1.3 LDAP Authentication, page 113 ➤ <b>radius</b> - see <b>Configuration Service</b> - 5.2.1.4 Radius Authentication, page 114 ➤ <b>msad</b> - see <b>Configuration Service</b> - 5.2.1.1 MSAD Authentication, page 111 ➤ <b>rsaace</b> - see <b>Configuration Service</b> - 5.2.1.5 RSA-ACE Authentication, page 114 <b>Note:</b> Since it is mandatory that the to-be-used authentication scheme is configured on both, MC box and administered box, phion highly recommends to configure the authentication schemes via the repository and, then, to set appropriate references.
<b>External login name field</b>	Here the login name configured within the corresponding authentication scheme has to be entered.

**Step 3 Details tab**

The Details tab makes further options for password and key handling available.

**Fig. 18-77** Administrator Details configuration dialogue



**List 18-26** Creating a new administrator - Details tab - section Password Parameters

Parameter	Description
<b>Last Password Change</b>	This parameter serves only informational purpose (as it is read-only) and displays the number of days since the last time the password was changed.
<b>Force password change every</b>	Here the time interval for mandatory password changes can be specified. The menu to the right of this parameter offers the entries <b>Days</b> and <b>Weeks</b> to define the duration. As soon as this period expires, the administrator is forced to change the password. Selecting the menu entry <b>Never</b> deactivates this and the following parameters of the <b>Password Parameters</b> section.

**List 18-26** Creating a new administrator - Details tab - section Password Parameters

Parameter	Description
<b>Warning period before expiration</b>	Specifies the number of days before the password expiry date on which a request for password change is displayed.
<b>Grace period after expiration</b>	Specifies the number of days after the password expiry date on which the password is still accepted.
<b>Password must differ on change</b>	This checkbox defines whether the current password may be re-used on password change.
<b>Assigned Range</b>	This parameter defines the visibility of configuration sessions. By selecting a range, only administrators authorised to configure this range see active configuration sessions of this administrator.
<b>Authentication Level</b>	This parameter defines the authentication that is required to access a system. The following types of authentication are available: <b>Password or Key</b> (default), <b>Password, Key, Password AND Key</b> .
<b>Public Key</b>	This section of the configuration dialogue serves for handling the public key. The button <b>Export/Import</b> offers import options.
<b>Peer IP Restriction</b>	Specifies IP addresses and/or subnets of administration workstations on which phion.a runs.

**Step 4 Defining the Administrative Scope**

By assigning elements like range or cluster, the scope implicitly defines those systems to which the admin basically has access rights. The default settings only provide for GUI-based access. Optionally, the administrator may receive access rights to the operating system layer (shell login) which widens the scope.

Additionally, every administrator is granted access to the central services of the MC, whereas his view on the system is restricted to his administrative scope.

**Note:**

Access to the system layer is only provided for the MC root.

**Note:**

Please take into consideration that these settings are sorts-of "global" settings. If it is necessary to define administrative settings for specific services (for example the VPN server or the Firewall), those settings are made in the **Service Properties** of the corresponding service.

The section **Administrative Scope** provides the following settings:

**List 18-27** Creating a new administrator - Administrator tab - section Administrative Scope

Parameter	Description
<b>Range menu</b>	This menu is used for assigning existing ranges to the administrators scope. Beside the entries <b>-ALL-</b> (maximising the scope to all existing ranges) and the currently available ranges, the menu provides an additional entry <b>-Linked-Only-</b> . Selecting this option, activates the <b>Links</b> menus where the scope may be customised. <b>Note:</b> When using the option <b>-Linked-Only-</b> , be sure to click the <b>Add</b> button after selecting in order to add the selection to the profile. The <b>Range</b> menu also steers the available options of the <b>Cluster</b> menu (see below). The following table shows the interconnections between selected <b>Range</b> -menu entry and the available <b>Cluster</b> -menu entries:
<b>Range menu entry</b>	<b>Cluster menu entries</b>
-ALL-	-ALL-
-Linked-Only-	-Linked-Only-
any range	-ALL-, -Linked-Only-, any cluster



**List 18-27** Creating a new administrator - Administrator tab - section Administrative Scope

Parameter	Description
<b>Cluster</b> menu	<p>This menu is used for assigning existing clusters to the administrators scope. Beside the entries <b>-ALL-</b> (maximising the scope to all existing clusters) and the currently available clusters, the menu provides an additional entry <b>-Linked-Only-</b>. Selecting this option, activates the <b>Links</b> menus where the scope may be customised.</p> <p><b>Note:</b> When using the option <b>-Linked-Only-</b>, be sure to click the <b>Add</b> button after selecting in order to add the selection to the profile.</p>

**Step 5** Defining the **Operative Settings**

This section specifies the administrators' rights.

The following options are available:

**List 18-28** Creating a new administrator - Administrator tab - section Operative Settings

Parameter	Description
<b>Configuration Level</b>	Via this parameter the access to configuration nodes is defined (see 6.7 Defining Node Properties, page 420).
<b>Shell Level</b>	<p>This menu provides options to control the shell access of the administrator. The following entries are available:</p> <p><b>No_Login</b> prevents the administrator from accessing the shell.</p> <p><b>Standard_Login</b> allows access to the system on OS layer via a default/standard user account (home directory: <code>user/phion/home/username</code>).</p> <p><b>Attention:</b> Everything a user saves to his home directory is deleted when he logs out.</p> <p><b>Restricted_Login</b> permits system access via a restricted shell (rbash). This type of shell has several restrictions, as its name already implies, such as specifying commands containing slashes, changing directories by entering <code>cd, ...</code> Such a login also restricts any writing operation to the users home directory.</p>
<b>Roles</b>	This menu provides the currently available administrative roles (see 6.3.7 Global Settings - Administrative Roles, page 414). Be sure to click <b>Add</b> in order to assign the selected role(s).
<b>Login Event</b> menu	This menu specifies the way a login is recorded. The entry <b>Service Default</b> (default) is a reference to the settings made within the <b>Access Notification</b> (see 6.3.6 Global Settings - MC Access Notification, page 413). The entry <b>Silent</b> suppresses any event notification.

### 8.3.2 Context Menu

Right-clicking on an entry opens the context menu containing the following entries:

- **Edit ...**  
Clicking **Edit** opens the configuration dialogue for editing an available administrator profile.
- **Remove**  
Clicking **Remove** deletes the selected profile.
- **New ...**  
Clicking **New** (correspondingly to clicking the **New Entry** button, see 8.3 Admin User Interface, page 433) opens the configuration window for creating a new profile.

## 9. MC Statistics

### 9.1 Service Configuration

The services **MC-StatCollect** (*dstatm*) and **MC-StatView** (*qstatm*) are responsible for collecting and viewing of statistics files generated on MC-administered boxes. They have to be introduced on the management centre box.

#### Note:

To introduce the services using the graphical administration tool *phion.a*, make sure to log on via the **Box-Address (Main Box IP)** of the management centre.

For a description how to introduce servers and services on a netfence gateway 3.1 Configuring the Box, page 393 and **Configuration Service - 4. Introducing a New Service**, page 97.

#### Note:

A license for management centre Statistics is not included in netfence MC Entry Edition. On systems running this software version, the services **MC-StatCollect** (*dstatm*) and **MC-StatView** (*qstatm*) are not applicable.

#### 9.1.1 Configuring the MC-StatCollect Service (dstatm)








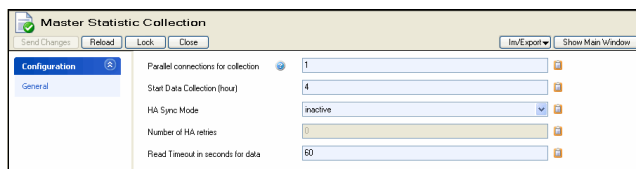
To configure *dstatm*, log on to the MC box, in the box menu click  **Config**, and then double-click  **Master Statistic Collection** (accessible through  **Box** >  **Virtual Servers** >  <servername> >  **Assigned Services** >  <servicename> (*dstatm*)).

Fig. 18-78 Master Statistic Collection Configuration dialogue



The following configuration options are available:








List 18-29 Master Statistic Collection Configuration

Parameter	Description
<b>Parallel connections for collection</b>	This option defines the number of parallel connections for collection of statistics data.

List 18-29 Master Statistic Collection Configuration

Parameter	Description
<b>Start Data Collection (hour)</b>	This option defines the begin of statistics data collection. The field expects time specification using international time format, for example, the value <b>4</b> triggers data collection initiation at 04:00, and the value <b>13</b> triggers data collection initiation at 13:00.
<b>HA Sync Mode</b>	Specification of the HA Sync Mode is required, when the MC that collects statistical data operates as <b>High Available (HA)</b> system. On a solitary system, leave the default setting <b>inactive</b> . On an HA-system set the <b>HA Sync Mode</b> to <b>rsync</b> , in order to activate statistics data synchronisation between the two HA partners. <b>Note:</b> Statistics data synchronisation is triggered by the script file <code>mirrorstat</code> that is executed on a regular basis. Data is synchronised over an SSH connection, thus, prior to synchronisation, <code>mirrorstat</code> establishes an SSH connection between the HA partners. It therefore expects the DSA key fingerprint of the HA partner to be known on the primary system. If the fingerprint is not yet known, because an SSH connection has not yet been established between the two systems, it cannot be processed any further. Therefore, if you are unsure, about the status of the DSA key fingerprint, prior to statistics data synchronisation launch, initiate an SSH connection from MC to its HA partner manually, in order to make the DSA key fingerprint known. To establish an SSH connection, at the command line interface on the MC type: <pre># ssh -lroot &lt;HA partner IP&gt;</pre>
<b>Sync Timeout (s)</b>	Timeout until the connection termination for synchronization will be executed (default 100 seconds)
<b>Number of HA retries</b>	This option is only available when <b>HA Sync Mode</b> is set to <b>rsync</b> . It specifies the number of retries for synchronisation of stored data.
<b>Read Timeout in seconds for data</b>	This parameter specifies the timeout when polling the boxes for statistical data (default: <b>60</b> ).

#### 9.1.2 Configuring the MC-StatView Service (qstatm)

To configure *qstatm*, in the box menu click  **Config**, and then double-click  **Service Properties** (accessible through  **Box** >  **Virtual Servers** >  <servername> >  **Assigned Services** >  <servicename> (*qstatm*)).

For a description of service configuration options see **Configuration Service - 4. Introducing a New Service**, page 97.

## 9.2 Data Collection Configuration

On a management centre, statistics collection settings may be defined by range and by cluster, in which cluster specific settings override range specific settings. Provided that MC-administered boxes are configured to supply statistics data (see 9.4 Transfer Settings, page 440), statistics files may be collected from multiple systems miscellaneously.

**Note:**

Cluster and range specific statistics collection configuration is done on the management centre. Therefore, when connecting to the MC with the graphical administration tool *phion.a* make sure to log on via the *MC- Address* of the management centre.

### 9.2.1 Range Specific Settings

To configure range specific collection settings, in the box menu click *Config*, and then double-click *Range Properties* (accessible through *Multi-Range* > <rangename>).

Fig. 18-79 Range Configuration dialogue

To enable statistics data collection for all boxes within a range, set parameter *Collect Statistics* to *yes* (default). When enabled, data will be collected as specified in the *Transfer Settings* section of each box within the range (see 9.4 Transfer Settings, page 440).

### 9.2.2 Cluster Specific Settings

To configure cluster specific collection settings, in the box menu click *Config*, and then double-click *Cluster Properties* (accessible through *Multi-Range* > <rangename> > <clustername>).

Fig. 18-80 Cluster Configuration dialogue

To enable statistics data collection for all boxes within the cluster, set parameter *Collect Statistics* to *yes* (default).

To inherit data collection configuration settings of the superordinate range, set parameter *Collect Statistics* to *like-range*.

When enabled, data will be collected as specified in the *Transfer Settings* section of each box within the cluster (see 9.4 Transfer Settings, page 440).

## 9.3 Compression Cooking and Deletion

Statistics files from MC-administered boxes are collected by the management centre as raw data, regardless of local cooking settings on the corresponding boxes themselves.

On a management centre, cooking settings for collected statistics files may be defined globally, by range or by cluster, in which cluster specific settings override range specific settings, and these again override global settings. Cooking is done directly on the management centre. When statistics files are configured for deletion, they are deleted from the pool of transferred files on the MC and not on the boxes themselves.

Globally defined cooking settings do not apply for cooking of statistics data generated by the management centre itself. Instead, analogous to self managed netfence gateways, local cooking settings may be configured separately (**Statistics - 3.1 Service Configuration**, page 300).

### Example:

On a management centre, two ranges (Range 1 and Range 2) are configured. Range 1 contains two clusters (Cluster A and Cluster B).

By default, global statistics settings will be used for all MC-controlled netfence gateways.

If specific statistics settings are defined for Range 1, these settings will be used for data originating from this range.

If specific statistics settings are defined for Cluster A, these settings will be used for data originating from this cluster. Boxes within Cluster B will use the specific statistics settings from Range 1.

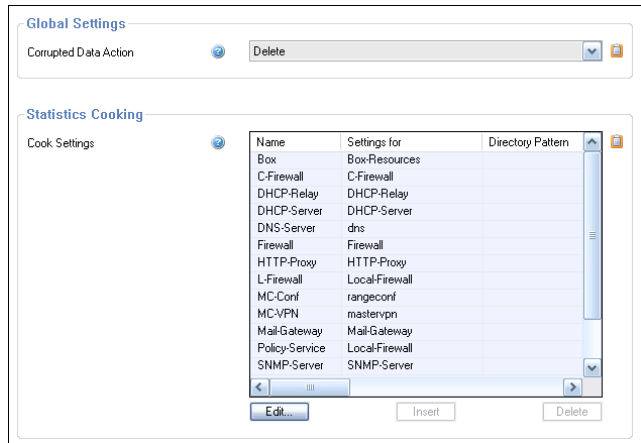
All boxes within Range 2 will use the global statistics settings.

Local cooking and deletion of statistics data are processed on the boxes themselves and without coherence to the processes running on the MC. Local cooking settings are configurable separately on each box (**Statistics - 3.1 Service Configuration**, page 300).

### 9.3.1 Global Settings

To configure global collection settings, in the box menu click **Config**, and then double-click **Statistics Cook Settings** (accessible through **Multi-Range > Global Settings**).

Fig. 18-81 Statistics Cook Settings



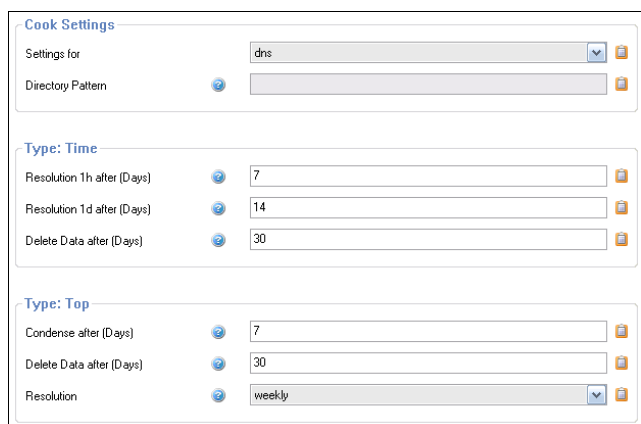
The dialogue allows configuration of cooking use and corresponding cooking settings for each type of statistics data.

List 18-30 Statistics Cook Settings - section Global Settings

Parameter	Description
<b>Corrupted Data Action</b>	This option defines the action <code>dstats</code> executes when it recognises a corrupted DB file. The following options are available: ⚡ <b>Delete</b> - deletes the corresponding DB file (default). ⚡ <b>Archive</b> - moves the DB file to a lost+found directory <b>Note:</b> Recognising a corrupted data file always triggers the event <b>Corrupted Data File</b> [150].

Settings for all types of statistics data are already defined by default. However, they may be modified freely to suit specific needs.

Fig. 18-82 Cook Settings configuration dialogue



The following cooking settings options are available:

List 18-31 Statistics Cook Settings - Statistics Cooking - section Cook Settings

Parameter	Description
	In this section, it may be defined how <code>dstats</code> should handle specific data types.

List 18-31 Statistics Cook Settings - Statistics Cooking - section Cook Settings

Parameter	Description
<b>Settings for</b>	In this field, select the software module to whose statistics data the settings below should apply. In the list, all software modules with appropriate default configuration are available that generate statistics data. Optionally, <b>Pattern-Match</b> may be selected to define a file pattern that should apply for cooking of statistics data. Selecting <b>Pattern-Match</b> enables the <b>Directory Pattern</b> field below, which expects insertion of an applicable file pattern.
<b>Directory Pattern</b>	<p><b>Pattern-Match</b> settings apply to statistics files available in sub-folders of <code>/var/phion/mainstat</code>. Patterns may be specified by either inserting full folder names or by using wildcards (? and *), in which the question mark wildcard (?) stands for a single character and the asterisk wildcard (*) stands for an arbitrary number of characters.</p> <p><b>Attention:</b> Generally, there is no need to make use of directory patterns when specifying cooking settings, as the default settings suffice most needs. If you do use directory patterns, make sure that they do not interfere with the module settings configuration. For a specific data type always use EITHER module OR directory pattern settings. <code>dstats</code> works through the configured instances successively, and will omit directory patterns that apply to directories it has already processed. Additionally, for clearly arranged management, place directory patterns at the end of the configuration file.</p> <p><b>Example pattern:</b> To include all statistics files starting with 'conn' generated by Firewall services running on all servers starting with 'S' in ranges 1 and 2, insert the following pattern structure:</p> <p><b>Actual file structure:</b>  <pre>/var/phion/mainstat/1/S1/service/FW/conn&lt;xxx&gt; /var/phion/mainstat/1/S2/service/FW/conn&lt;xxx&gt; /var/phion/mainstat/2/S3/service/FW/conn&lt;xxx&gt;</pre> </p> <p><b>Directory pattern:</b>  <pre>*/S*/service/FW/conn*</pre> </p> <p><b>Attention:</b> Avoid too openly defined patterns spanning multiple folders, such as <code>*/service/*/*</code>. If you do use patterns spanning multiple folders, be aware of their implication and always position them at the list bottom.</p>

List 18-32 Statistics Cook Settings - Statistics Cooking - section Type: Time

Parameter	Description
	<p><b>Note:</b> Options in this section apply to <b>Time</b> statistics only (for example <b>byte (Time for Dst)</b>, <b>conn (Time for Src)</b>, ...).</p>
<b>Resolution 1h after (days)</b>	Number of days, after which the granularity of statistics data of type time should be increased to one hour. Data more recent than the inserted number of days will not be affected.
<b>Resolution 1d after (days)</b>	Number of days, after which the granularity of statistics data of type time should be increased to one day. <p><b>Note:</b> The period between cooking from hour to day granularity has to be 2 days minimum. If set to 1 day it will result in a summary offset for hourly granularity of 0 days per instance. This will lead to an error message in the <code>dstat</code> log file similar to the following: <b>Cannot create, file byte.hour_tot&lt;cookInstStartTS&gt; exists already.</b></p>
<b>Delete Data after (days)</b>	Number of days, after which statistics data of type time should be deleted.

List 18-33 Statistics Cook Settings - Statistics Cooking - section Type: Top

Parameter	Description
	<p><b>Note:</b> Options in this section apply to <b>Top</b> statistics only (for example <b>byte (Top Dst)</b>, <b>conn (Top Src)</b>, ...).</p>

List 18-33 Statistics Cook Settings - Statistics Cooking - section Type: Top

Parameter	Description
<b>Condense after (days)</b>	Number of days, after which statistics data of type top should be merged into larger temporal bins. Data more recent than the inserted number of days will not be affected.
<b>Delete Data after (days)</b>	Number of days, after which statistics data of type top should be deleted.
<b>Resolution</b>	Available resolutions are <b>weekly</b> and <b>monthly</b> . Settings trigger data rearrangement so as to be representative of an entire week or a month. <p><b>Attention:</b> It is recommendable only to change this parameter as long as the system is not productive. Thoughtless modifying may cause imprecise visualisation in the statistics viewer due to incomplete cook instances.</p>

### 9.3.2 Range Specific Settings

To configure range specific cook settings, in the box menu click **Config**, and then double-click **Range Properties** (accessible through **Multi-Range** > <rangename>).

To enable specific Cook Settings for all boxes within a range, set parameter **Own Cook Settings** to **yes** (default: **no**) (see 6.4.2 Range-specific Settings, page 417).

For a description of configuration options see 9.3.1 Global Settings, page 438.

### 9.3.3 Cluster Specific Settings

To configure cluster specific cook settings, in the box menu click **Config**, and then double-click **Cluster Properties** (accessible through **Multi-Range** > <rangename> > <clustername>).

To enable specific Cook Settings for all boxes within a cluster, set parameter **Own Cook Settings** to **yes** (default: **no**) (see 6.5.2 Cluster-specific Settings, page 419).

For a description of configuration options see 9.3.1 Global Settings, page 438.

### 9.3.4 Local Settings

**Note:**  
Local cook settings only affect the way statistics data is processed on the netfence gateway itself. They have no impact on how the management centre processes the statistical data.

To configure local cook settings of a netfence gateway, in the box menu click **Config**, and then double-click **Statistics** (accessible through **Multi-Range** > <rangename> > <clustername> > **Boxes** > <boxname> > **Box Services**).

For a description of configuration options see **Statistics** - 3.1 Service Configuration, page 300.

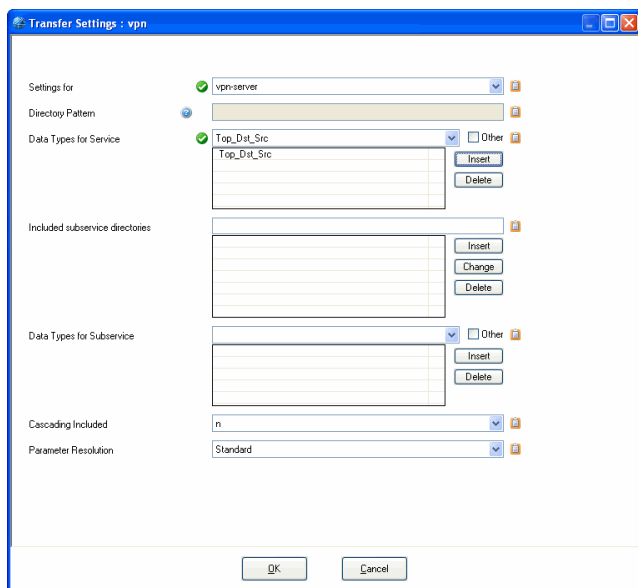
## 9.4 Transfer Settings

The Transfer Settings sections is only available on MC-administered netfence gateways. Configuration is required in context with collection of statistics files by the MC-StatCollect service (dstatm) running on the management centre.

In the Transfer Settings section, define the statistics files which should be transferred to the management centre.

To configure transfer settings for a netfence gateway, in the box menu click **Config**, and then double-click **Statistics** (accessible through **Multi-Range** > <rangename> > <clustername> **Boxes** > <boxname> > **Infrastructure Services**).

Fig. 18-83 Transfer Settings configuration dialogue



List 18-34 Statistics Cook Settings - Transfer Settings

Parameter	Description
<b>Settings for</b>	In this field, select the software module to whose statistics data the settings below should apply. In the list, all software modules are available that generate statistics data. Optionally, <b>Pattern-Match</b> may be selected to define a file pattern that should apply for cooking of statistics data. Selecting <b>Pattern-Match</b> enables the <b>Directory Pattern</b> field below, which expects insertion of an applicable file pattern.

List 18-34 Statistics Cook Settings - Transfer Settings

Parameter	Description
<b>Directory Pattern</b>	<p><b>Pattern-Match</b> settings apply to statistics files available in sub-folders of <code>/var/phion/mainstat</code>. Patterns may be specified by either inserting full folder names or by using wildcards (? and *), in which the question mark wildcard (?) stands for a single character and the asterisk wildcard (*) stands for an arbitrary number of characters.</p> <p><b>Attention:</b> When using directory patterns, make sure that they do not interfere with the module settings configuration. For a specific data type always use EITHER module OR directory pattern settings. dstatm works through the configured instances successively, and will omit directory patterns that apply to directories it has already processed. Additionally, for clearly arranged management, place directory patterns at the end of the configuration file.</p> <p><b>Example pattern:</b> To include all statistics files starting with 'conn' generated by Firewall services running on all servers starting with 'S' in ranges 1 and 2, insert the following pattern structure: <b>Actual file structure:</b> <code>/var/phion/mainstat/1/S1/service/FW/conn&lt;xxx&gt;</code> <code>/var/phion/mainstat/1/S2/service/FW/conn&lt;xxx&gt;</code> <code>/var/phion/mainstat/2/S3/service/FW/conn&lt;xxx&gt;</code> <b>Directory pattern:</b> <code>*/S*/service/FW/conn*</code></p> <p><b>Attention:</b> Avoid too openly defined patterns spanning multiple folders, such as <code>*/service/*/*</code>. If you do use patterns spanning multiple folders, be aware of their implication and always position them at the list bottom.</p>
<b>Data Types for Service</b>	From this list, select the statistics type(s) that should be transferred to the management centre. Multiple selections are possible. Add each type by clicking the <b>Insert</b> button.
<b>Included subservice directories</b>	Into this field, insert subservices that should be included in statistics file transfer. <b>Note:</b> Subservices may only be specified for server modules.
<b>Data Types for Subservice</b>	From this list, select the subservice statistics type(s) that should be transferred to the management centre. Multiple selections are possible. Add each type by clicking the <b>Insert</b> button.
<b>Cascading Included</b>	When set to <b>yes</b> (default: <b>no</b> ), all cascaded sub-folders (indicated by icon 📁) in an included subservice will be transferred.
<b>Parameter Resolution</b>	When set to <b>High</b> (default: <b>Standard</b> ) all sub-folders of an included subservice will be transferred.



## 9.4.1 Examples for Transfer Settings

### 9.4.1.1 Transfer all Box and Server Files

Fig. 18-84 Transfer Settings - box and server files

The figure illustrates the configuration of transfer settings in the phion management centre. It is divided into two parts: Step 1 and Step 2.

**Step 1: Transfer settings "box"**

This step shows the configuration for the 'box' directory. The left pane displays a tree view with 'box' selected. The right pane shows the 'Transfer Settings : box' dialog box. The settings are as follows:

- Settings for: box-resources
- Directory Pattern: (empty)
- Data Types for Service: All (checked)
- Included subservice directories: (empty)
- Data Types for Subservice: (empty)
- Cascading Included: n
- Parameter Resolution: Standard

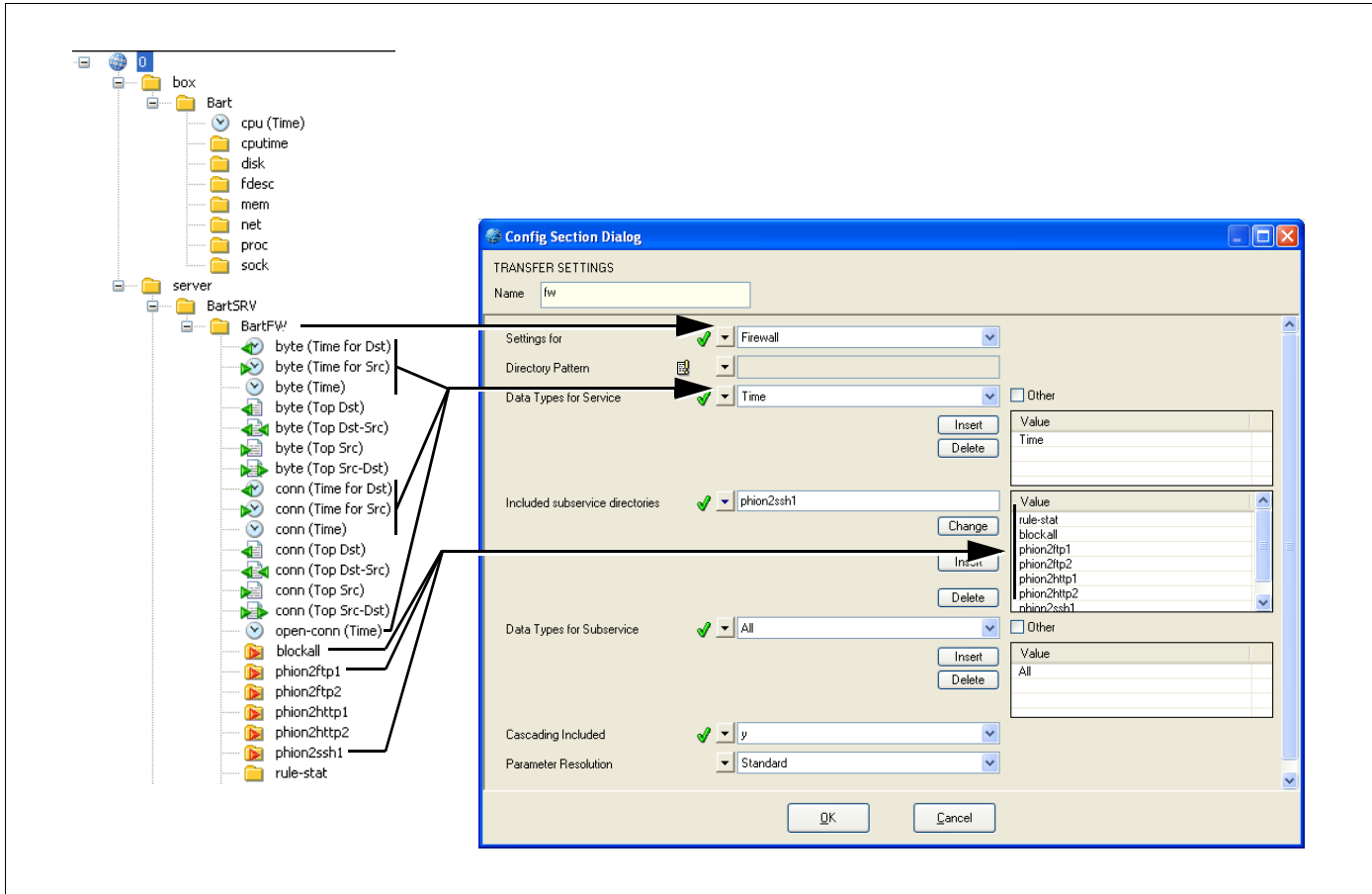
**Step 2: Transfer settings "srv"**

This step shows the configuration for the 'srv' directory. The left pane displays a tree view with 'server' selected. The right pane shows the 'Transfer Settings : srv' dialog box. The settings are as follows:

- Settings for: pattern-match (checked)
- Directory Pattern: \*/server/\* (checked)
- Data Types for Service: All (checked)
- Included subservice directories: (empty)
- Data Types for Subservice: All (checked)
- Cascading Included: y (checked)
- Parameter Resolution: Standard

## 9.4.2 Partial Transfer

Fig. 18-85 Transfer Settings - partial transfer



## 9.5 Recovery and State Analysis of Poll Sessions

Table 18-19 Error analysis of poll sessions

Session state	Analysis of error scenarios	Necessary actions	Box state
Idle	cannot connect to box	IGNORE	CLEAN
Connected	cannot receive transfer files ('toSend.timestamp') from box	IGNORE	CLEAN
State_Received	<ul style="list-style-type: none"> <li>cannot perform calculation of statistic file list</li> <li>received transfer files remain in box-specific state directory and will be ignored in subsequent poll sessions.</li> </ul>	IGNORE	CLEAN
State_Processed	A dist-operation fails. No problem because these operations are transaction protected.	IGNORE	CLEAN
Data_Received	<ul style="list-style-type: none"> <li>data files either be successfully merged or are stored within temporary data directory</li> <li>box state is dirty because a possible synchronisation with the HA partner would result in inconsistent data (files in temporary data path won't be synced).</li> </ul>	RECOVERY	DIRTY
Data_Processed	<ul style="list-style-type: none"> <li>masterAccept-file cannot be created</li> <li>masterAccept-file cannot be send</li> </ul>	RESEND_ACK	DIRTY
State_Updated	<ul style="list-style-type: none"> <li>cannot remove temporary data directory (because it's not empty)</li> <li>cannot remove obsoleted state files</li> </ul>	INTERNAL	DIRTY

# 10. MC Eventing

Event forwarding is based on a 2-way communication between the Box event module running on the operative netfence gateway (**Box**) and the MC event module running on a phion management centre (**MC**).

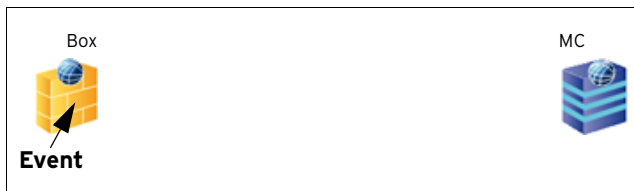
## 10.1 Example

The following example illustrates how this communication process is working.

### Step 1 Box event

An event is generated on a netfence gateway and introduced into the event system on the box.

Fig. 18-86 Box event

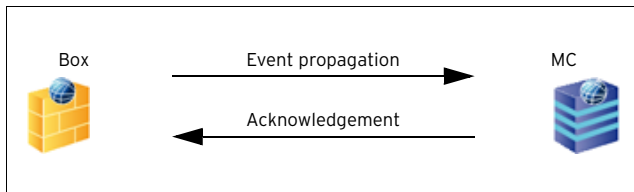


### Step 2 Event propagation

The event is propagated to the MC and the MC confirms the reception by sending an acknowledgement (ACK) to the emitter of the event.

**Note:**  
The emitter retransmits its event until it receives an ACK from the MC.

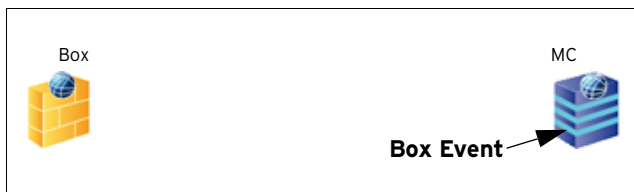
Fig. 18-87 Box event propagation to MC



### Step 3 Event introduced to MC event module

As soon as the event is transmitted to the MC, it is introduced into the MC event module and can be viewed and modified within the MC event monitor GUI.

Fig. 18-88 MC: Box event occurred

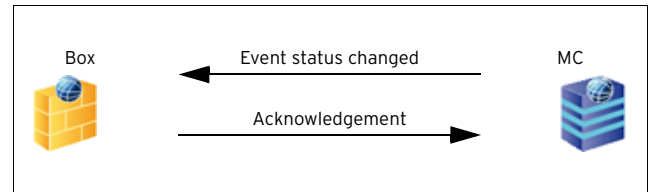


### Step 4 Alternative a - MC: Event status changed

If the status of the event is modified on the MC, the status change is propagated from the MC to the Box, which confirms the changed status by sending an ACK.

**Note:**  
The status change notification is retransmitted until the MC receives an ACK from the Box.

Fig. 18-89 MC: Event status changed

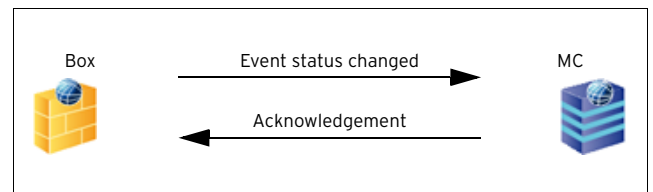


### Step 5 Alternative b - Box: Event status changed

If the event status is modified on the Box that generated the event, the status change is also propagated to the MC which confirms the new status by sending an ACK.

**Note:**  
The status change notification is retransmitted until the Box receives an ACK from the MC.

Fig. 18-90 Box: Event status changed



### Step 6 Alternative c - MC: Event deleted

If the event is deleted on the MC, the MC sends the deletion request to the Box. The Box deletes the event and returns an acknowledgement to the MC, where the event now is also deleted.

Fig. 18-91 MC: Delete Event



### Step 7 Alternative d - Box: Event deleted

If the event is deleted directly on the Box, the procedure is the same as mentioned above. The difference is that the Box sends the deletion request to the MC and awaits the acknowledgement before the event is finally deleted.

Fig. 18-92 Box: Delete Event




## 10.2 Event User Interface

### Note:

For a detailed introduction of the Event user interface, please consult **Eventing**, page 305. This document only states the differences between the MC Event GUI and the Box Event GUI.

The main difference between the two Event GUIs is that the MC Event user interface is used for displaying events of all boxes that are managed by the MC while the Box Event user interface is used for displaying the events of a specific box.

If an administrator has a limited administrative scope he will only see events of those boxes (that are netfence gateways) that are within his administrative scope in the MC Event user interface (see 8.3.1 Creating a New Admin Profile, Step 4 Defining the Administrative Scope, page 434).

To open the MC Event user interface, log on to an existing phion management centre (using the **MC** tab in the phion.a login window) and click the  **Event** button in the MC menu bar.

### Attention:

The MC Event user interface only displays events created on MC-managed netfence gateways. In order to see events created by the MC box itself it is necessary to log in to the MC box directly (by entering the box's IP address in the Box tab of the phion.a login dialogue).

The MC Event user interface is handled in the same way as the Box Event GUI. Please consult **Eventing** - 2.2 Event Monitoring, page 311 for further information.

For a complete list of all available events see **System Information** - 5. List of Default Events, page 516.

### 10.2.1 Context Menu

The context menu offers the same options as described in **Eventing** - 2.2.1.1 Context Menu, page 312.

## 10.3 Event Configuration

### Note:

This document only covers the special configuration options that are offered when using a management centre. For information on how to configure an event, please consult **Eventing** - 2. Event Configuration, page 306.

With a management centre you are able to define different event configurations for specific ranges and specific clusters.




### Note:

The propagation of an event has to be configured within the box configuration.

Due to the hierarchical structure of the MC, events can be configured on several levels depending on the requirements of your security policy.

### 10.3.1 Global Event Settings

These settings affect all events that are being propagated from the netfence gateways to the management centre unless you have defined range- or cluster-specific event settings.








To modify the global event settings, select  **Multi-Range** >  **Global Settings** >  **Eventing** in the MCs configuration tree (see 6.3.1 Global Settings - Eventing, page 411).

### Note:

After having accomplished the required modifications, make sure to click **Send Changes** and **Activate** in order to activate the new configuration.

### 10.3.2 Range-specific Event Settings

Range-specific event settings are used if multiple ranges requiring individual event settings are defined in the MC-configuration tree.

To configure range-specific event settings, first set the parameter **Own Event Settings** ( **Multi-Range** >  <rangename> >  **Range Properties**) to **yes**. As soon as this is done, the node  **Multi-Range** >  <rangename> >  **Range Settings** offers the entry  **Eventing** where the configuration of the range-specific event settings takes place.

The configuration itself is the same as described under **Eventing** - 2. Event Configuration, page 306.

### Note:

After having accomplished the required modifications, make sure to click **Send Changes** and **Activate** in order to activate the new configuration.

### 10.3.3 Cluster-specific Event Settings

Cluster-specific event settings are used if multiple clusters requiring individual event settings are defined in the MC-configuration tree.

To configure cluster-specific event settings, first it is necessary to set the parameter **Multi-Range** > **<rangename>** > **<clustername>** > **Cluster Properties** > **Own Event Settings** to **yes**. As soon as this is done, the node **Multi-Range** > **<rangename>** > **<clustername>** > **Cluster Settings** offers the entry **Eventing** where the configuration of the cluster-specific event settings takes place.

The configuration itself is the same as described under **Eventing** - 2. Event Configuration, page 306.

**Note:**

After having accomplished the required modifications, make sure to click **Send Changes** and **Activate** in order to activate the new configuration.

### 10.3.4 Box-specific Event Settings

In contrast to the global event settings and range/cluster-specific event settings, the box-specific settings only affect the way events are processed by the box's event system.

Therefore the effect of these settings can only be seen, if you are directly connected to the Event user interface of the corresponding netfence gateway.

The configuration itself is the same as described under **Eventing** - 2. Event Configuration, page 306.

**Note:**

After having accomplished the required modifications, make sure to click the buttons **Send Changes** and **Activate** in order to activate the new configuration.

## 10.4 Event Propagation

Via the MCs eventing you are able to define, whether a specific event or all events of a range/cluster/box should be propagated to the management centre.

### 10.4.1 No Propagation at all

To define that no events from a range/cluster/box should be propagated to the MC, open the range-/cluster-/box-specific event settings (as described above), open the **Basic** tab, and simply clear the option **Send Event to MC**.

**Note:**

After having realised the required modifications, make sure to click the buttons **Send Changes** and **Activate** in order to activate the new configuration.

### 10.4.2 Severity-sensitive Propagation

To define that no events from a range/cluster/box should be propagated to the MC, open the range-/cluster-/box-specific event settings (as described above) and open the **Severity** tab, open the wanted severity and simply clear the option **Propagate to Master**.

**Note:**

After having realised the required modifications, make sure to click the buttons **Send Changes** and **Activate** in order to activate the new configuration.

# 11. MC Syslog

## 11.1 Overview

**Note:**  
Before starting to work with Syslog Proxy and MC Syslog, it is recommended to have read and understood **Log Viewer**, page 289.

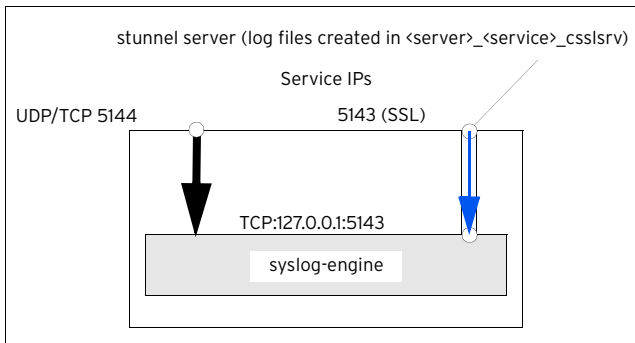
This service is intended for collecting log messages from managed netfence gateways and streaming these log messages to an external log host or sending them to the HA partner.

Basically, syslog streaming consists of three major steps:

- Step 1** Log reception
- Step 2** Log processing
- Step 3** Log delivery

### 11.1.1 Log Reception

Fig. 18-93 Example for log reception via port 5144 and/or 5143



#### Log reception via port 5144:

Since connections to the syslog-engine are unencrypted and unauthenticated the firewall default settings restrict access to port 5144 for both, TCP and UDP protocols, to:

- access only for managed boxes
- access only via VPN tunnel.

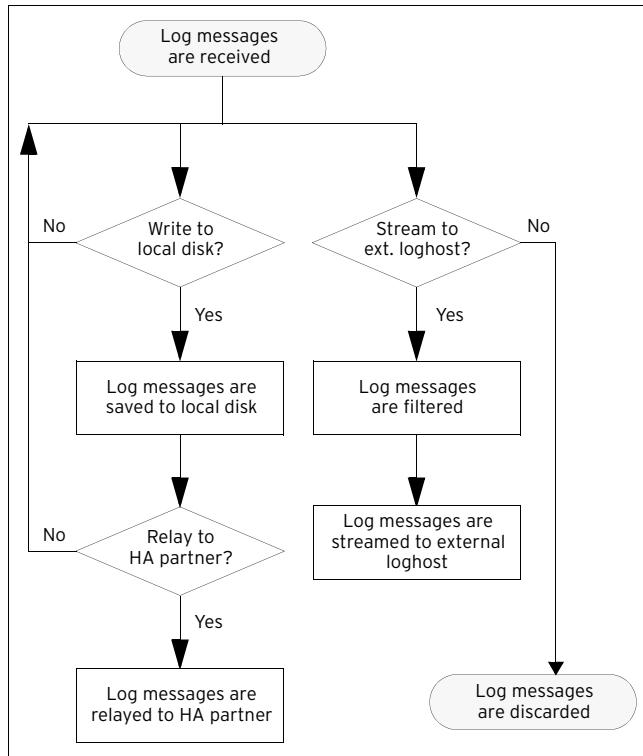
#### Log reception via port 5143:

Using port 5143 for log reception enables managed boxes without management tunnels to connect via a SSL connection to port 5143. Using SSL allows for both encryption and authentication.

### 11.1.2 Log Processing

The following flowchart offers a very basic overview of log processing:

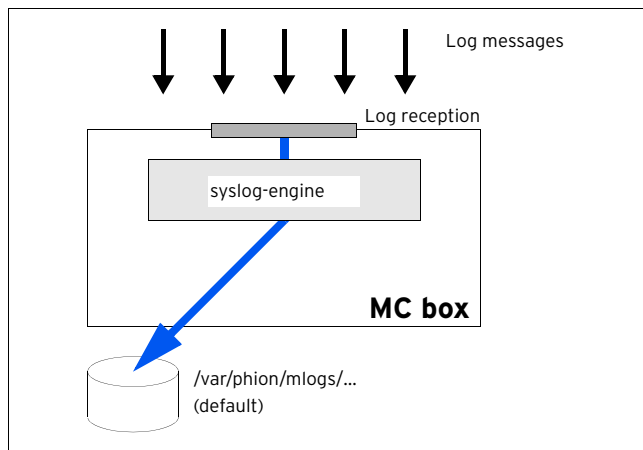
Fig. 18-94 Log processing flowchart



### 11.1.3 Log Delivery

#### 11.1.3.1 Log Delivery To Local Disk

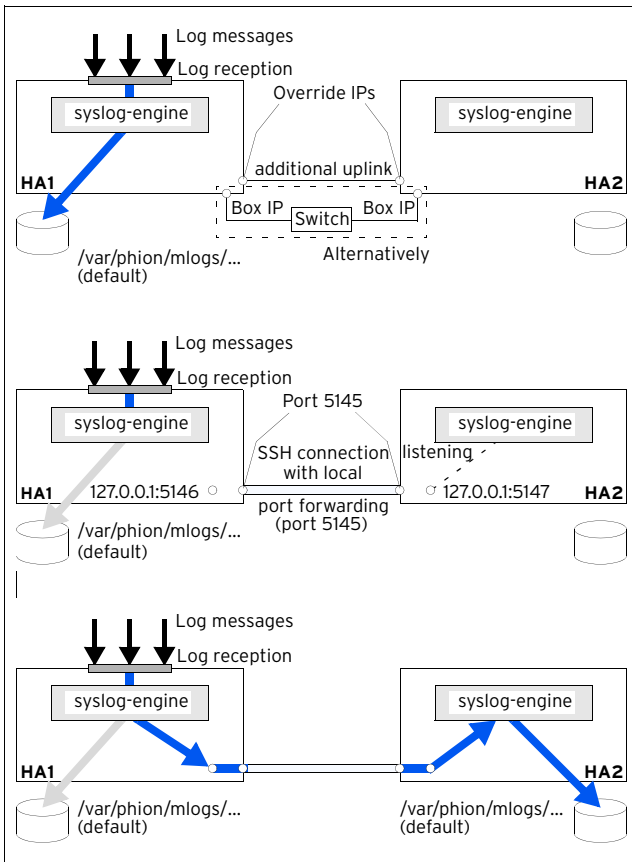
Fig. 18-95 Example for message delivery to local disk





### 11.1.3.2 Log Delivery via Private Uplink (HA Sync)

Fig. 18-96 Example for a HA sync via private uplink (using the override IPs is mandatory)



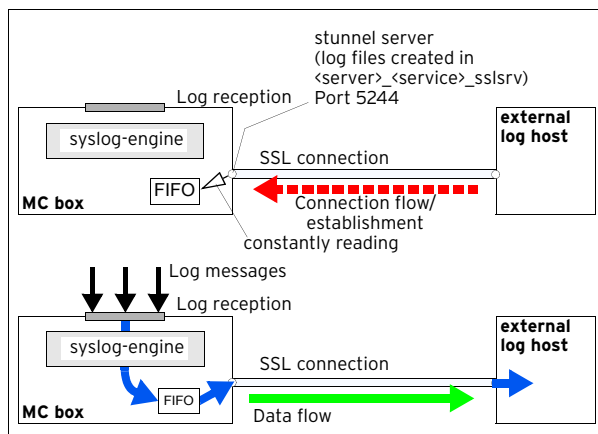
### 11.1.3.3 Log Delivery by Relaying

When relaying log messages to an external log host, phion provides three different ways to realise the task (used **SSL cypher: AES-128**):

#### ➤ SSL active querying

This type describes relaying to an external log host with permanent reading access of the log host to the MC-box-internal FIFO module (figure 18-97), that is the syslog service is the SSL server.

Fig. 18-97 Example for successful active SSL querying



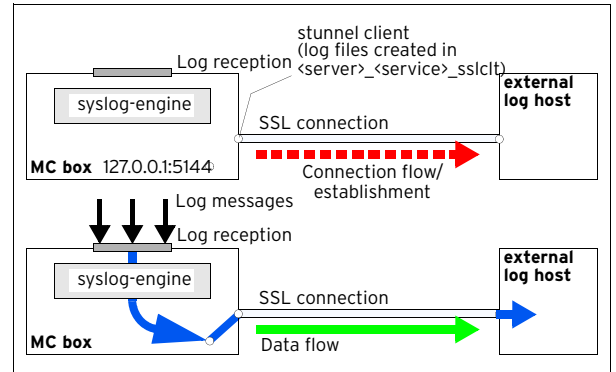
As a matter of fact, if this reading access is not provided (for example because log host is down), transferring log messages is not possible. Especially when having an HA

management centre this way of transferring is not recommended.

#### ➤ SSL passive receiving

This type describes relaying to an external log via loopback on the MC box (figure 18-98), that is the syslog service is the SSL client.

Fig. 18-98 Example for passive SSL receiving



This way of transferring should be used for an HA management centre because the external log host does not need to know which partner is currently active.

#### ➤ Plain passive receiving

This type describes standard syslog streaming without a SSL connection.

## 11.2 Installing

To install the MC Log Service simply follow the instructions in **Configuration Service - 4. Introducing a New Service**, page 97, and select **MC-Log** as **Software Module**.

## 11.3 Configuring

Beside the standard Service Properties that each software module provides, configuring takes place in the **MC Syslog Service** of the MC box. Therefore, enter the management centre on box-level and select **Box > Virtual Servers > <servername> > Assigned Services > <servicename> (msyslog) > MC Syslog Service**.

### 11.3.1 Basic Setup

List 18-35 MC Syslog Server configuration - section Operational Setup

Parameter	Description
<b>Idle Mode</b>	Syslogging is activated by default (setting <i>no</i> , that means not idle). When active, the service listens for incoming log messages from its managed boxes and hence processes them as configured through the following parameters. Nonetheless, even when idle (setting <i>yes</i> , that means idle) it as well listens for incoming messages to avoid ICMP Port Unreachable messages being sent back to the connecting systems. It then simply discards the received messages.

List 18-35 MC Syslog Server configuration - section Operational Setup

Parameter	Description
<b>Run as User</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>This parameter defines the user name that will be used when synchronising the log with the HA partner system. By default this parameter is set to system user <b>msyslog</b>. By ticking the checkbox <b>Other</b> (to the right) you may enter any other name.</p> <p><b>Attention:</b> Once set, do not change.</p>
<b>User ID</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>Here the ID of the system user (parameter <b>Run as User</b>, see above) is defined (default: <b>7999</b>).</p>
<b>Service Key</b>	<p>This parameter is required for authentication purposes against connecting clients using the SSL connections. In order to create a new 1024-bit SSL private key, simply click the <b>New Key</b> button. On the right of this line the hash of the certificate is displayed.</p> <p>By default creating a new SSL private key results in a freshly generated <b>Service Certificate</b> (see below) that is automatically signed with the new private key.</p>
<b>Service Certificate</b>	<p>This certificate is required for SSL connections, regardless whether they are passive or active ones. Via button <b>Show ...</b> the certificate is displayed, and via button <b>Edit ...</b> the certificate may be modified. Again, to the right, the hash mark is displayed.</p> <p><b>Attention:</b> It is mandatory that both, SSL Private Key AND SSL Certificate, have the same hash mark.</p>
<b>Support Trusted Data Reception</b>	<p>If this parameter is set to <b>yes</b> (as it is by default) the service will listen for incoming SSL connections on configured IPs and defined <b>SSL Listen Port</b> (port 5143; <b>Trusted Data Reception</b> view).</p> <p><b>Note:</b> This option is not needed when managed boxes deliver log content through a box management tunnel. Boxes without a management tunnel should use the SSL option for delivery. In this case you should not set this option to <b>no</b> and likewise configure the affected boxes to use SSL for log delivery.</p>
<b>Store on Disk</b>	<p>Setting this parameter to <b>yes</b> (default: <b>no</b>) causes writing the incoming log messages to the specified logging path (customisable via parameter <b>Local Log Directory</b>, see 11.3.3 Local Storage, page 449). By default the path for logging is <code>/var/phion/mlogs</code>.</p>
<b>Sync to HA Partner</b>	<p>This parameter enables the real-time transfer of log messages to the HA partner. As a matter of fact, this parameter is only available if parameter <b>Store on Disk</b> is set to <b>yes</b>. Synchronising takes place via a SSHv2 tunnel between the HA partners. For information concerning the configuration of such high available synchronisation, please have a look at 11.3.4 HA Synchronization, page 449.</p>
<b>External Relaying</b>	<p>This parameter enables the optional transfer of log messages to external loghosts. By default this parameter is set to <b>no</b>. For information concerning the configuration of such external relaying, please have a look at 11.3.5 Relaying Setup, page 450.</p>

List 18-36 MC Syslog Server configuration - section Plain Data Reception

Parameter	Description
	<p><b>Note:</b> This parameter set is only available in <b>Advanced View</b> mode.</p>
<b>Supported Protocols</b>	<p>Via this parameter you define what kind of sockets are available for incoming log messages. Available options are <b>UDP&amp;TCP</b> (opens an UDP as well as a TCP socket; default), <b>UDP</b> (opens an UDP socket only) and <b>TCP</b> (opens a TCP socket only).</p>
<b>UDP Port</b>	<p>This parameter is only available as long as the parameter <b>Supported Protocols</b> contains an UDP option and defines the port that is to be used for receiving log messages (default: <b>5144</b>).</p> <p><b>Attention:</b> If you change this port assignment to another port (be sure to use a port higher than 1024) you will have to adjust the local firewall rule set on the MC box.</p>

List 18-36 MC Syslog Server configuration - section Plain Data Reception

Parameter	Description
<b>TCP Port</b>	<p>This parameter is only available as long as the parameter <b>Supported Protocols</b> contains a TCP option and defines the port that is to be used for receiving log messages (default: <b>5144</b>).</p> <p><b>Attention:</b> If you change this port assignment to another port (be sure to use a port higher than 1024) you will have to adjust the local firewall rule set on the MC box.</p>

List 18-37 MC Syslog Server configuration - section Tuning Parameters

Parameter	Description
	<p><b>Note:</b> This parameter set is only available in <b>Advanced View</b> mode.</p>
<b>Message Queue Size</b>	<p>Via this parameter you may define the maximum possible size of the out-message queue if messages are not immediately deliverable (default: <b>16384</b>). The out-message queue is used when writing to disk, transferring to HA partner or when relaying log to external log hosts.</p>
<b>Max TCP Connections</b>	<p>This parameter is only available as long as the parameter <b>Supported Protocols</b> contains a TCP option and defines the maximum number of concurrent incoming TCP connections (default: <b>50</b>). This parameter provides improved security by preventing DoS attacks.</p>
<b>GC Idle Threshold</b>	<p>This parameter defines the threshold (number of objects in memory) after which garbage collection is initiated when idle (that means no messages within 10 ms; default: <b>200</b>).</p>
<b>GC Busy Threshold</b>	<p>This parameter defines the threshold (number of objects in memory) after which garbage collection is initiated even when busy (default: <b>3000</b>). If this limit is exceeded messages will be lost.</p>

## 11.3.2 Trusted Data Reception

### Note:

This parameter set is only available with parameter **Support Trusted Data Reception (Basic Setup)** view set to **yes**.

List 18-38 MC Syslog Server configuration - Trusted Data Reception

Parameter	Description
<b>SSL Listen Port</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>This parameter defines the listening port for SSL connections (default: <b>5143</b>).</p>
<b>SSL Busy Timeout [s]</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>This timeout defines for how long (in seconds) a SSL connection may be in busy condition until it is terminated (default: <b>300</b>).</p>
<b>SSL Close Timeout [s]</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b> mode.</p> <p>This timeout defines for how long (in seconds) a SSL connection may be in close condition until it is terminated (default: <b>60</b>).</p>
<b>SSL Idle Timeout[s]</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b>.</p> <p>This timeout defines for how long (in seconds) a SSL connection may be in idle condition until it is terminated (default: <b>43200</b>).</p>

**List 18-39** MC Syslog Server configuration - Trusted Data Reception - section *SSL* Client Authentication

Parameter	Description
<b>Service Certificate</b>	Via this menu the to-be-used service certificate is selected (default: <i>Use_MC_SSL_Cert</i> , that means the SSL certificate of the management centre will be used for authentication, see 6.3.4.2 Trust Chain, page 412). When using option <i>Use_MC_SSL_Cert</i> it is highly recommended to use <i>verify_peer_certificate</i> as type of <i>Client Authentication</i> . <b>Attention:</b> When updating (not newly installing) the system from any version prior to version 2.4.2 (all versions up to 2.4.1-x) the MC SSL Certificate is not yet present. To create the certificate, open the MC Identity file and make a dummy change followed by activation. netfence versions 2.4.2 and higher already contain the certificate, so it need not be activated.
<b>Client Authentication</b>	Here you define the way clients have to authenticate themselves (default: <i>verify_peer_with_locally_installed_certificate</i> ).
<b>Trusted Clients</b>	This section is used for importing/exporting the client certificates required for authentication when using SSL-based log delivery to the MC.

### 11.3.3 Local Storage

This tab is used for configuring the local behaviour of the syslog service on the management centre box. This tab is only editable if parameter *Store on Disk* (see 11.3.1 Basic Setup, page 447) is set to *yes*.

**List 18-40** MC Syslog Server configuration - Local Storage Setup - section Local Log Directory

Parameter	Description
<b>Local Log Directory</b>	<b>Note:</b> This parameter is only available in <i>Advanced View</i> mode.  This field holds the path where the logs of the syslog service are written to (default: <code>/var/phion/mlogs</code> ). This directory belongs to the configured system user (parameter <i>Run as User</i> , see 11.3.1 Basic Setup, page 447).
<b>Use Time Received</b>	<b>Note:</b> This parameter is only available in <i>Advanced View</i> mode.  Take into consideration that this parameter is only available if parameter <i>Store on Disk</i> is set to <i>yes</i> . Each log message has a send-time stamp when it is written to disk: <code>send_stamp log_message: yes</code> - send_stamp is rewritten using local MC receive time <code>send_stamp log_message no</code> (default) - send_stamp is not modified.
<b>Prepend Received Time</b>	<b>Note:</b> This parameter is only available in <i>Advanced View</i> mode.  Take into consideration that this parameter is only available if parameter <i>Store on Disk</i> is set to <i>yes</i> . Each log message gets its own time stamp(s) when it is written to disk ( <code>receive_time_stamp</code> showing MC receiving time; <code>send_stamp</code> showing Box sending time): <code>receive_time_stamp send_stamp log_message</code> when set to <i>yes</i> (default) <code>send_stamp log_message</code> when set to <i>no</i> .
<b>File Sync Frequency [lines]</b>	<b>Note:</b> This parameter is only available in <i>Advanced View</i> mode.  This parameter defines the number of lines after which the synchronisation is started. The default value of <i>0</i> indicates that there is currently no delay set.

**List 18-40** MC Syslog Server configuration - Local Storage Setup - section Local Log Directory

Parameter	Description
<b>Log Keep Duration</b>	Via this parameter you define for how long the log files are kept on the local system. The following periods are available: <b>day</b> - log file name: <code>&lt;logmessage&gt;.\$HOOUR.log</code> ; after 23 h the log files created by syslog are overwritten. <b>week</b> (default) - log file name: <code>&lt;logmessage&gt;.\$WEEKDAY.\$HOOUR.log</code> ; after one week the log files (that is <code>mon, tue, wed, ...</code> ) created by syslog are overwritten. After one week the log files are overwritten <b>no-limit</b> - log file name: <code>&lt;logmessage&gt;.\$HOOUR.log</code> ; <b>Note:</b> This setting is a very specific one and, therefore, should be used by experts only (contacting phion Support highly recommended).

### 11.3.4 HA Synchronization

Via this tab the log-message synchronisation between HA partners is configured.

**List 18-41** MC Syslog Server configuration - HA Synchronization - section HA Synchronization Setup

Parameter	Description
<b>SSH Authentication Key</b>	Here the SSH key management is provided. By clicking <i>New Key</i> you may create a new key for the SSH connection. Alternatively, you may import already existing keys (either from clipboard or file) or export the newly generated key (either to clipboard or file, password protected or not, or the public key only). These import/export options are available within the menu <i>Ex/Import</i> . For informational purpose the key's hash is displayed to the right of this line.
<b>SSH Host Key</b>	Here the SSH host key management is provided. By clicking <i>New Key</i> you may create a new SSH key. Alternatively, you may import already existing keys (either from clipboard or file) or export the newly generated key (either to clipboard or file, password protected or not, or the public key only). These import/export options are available within the <i>Ex/Import</i> menu. For informational purpose the key's hash is displayed to the right of this line.
<b>SSH Listen Port</b>	<b>Note:</b> This parameter is only available in <i>Advanced View</i> mode.  This parameter defines the port that will be used for establishing the SSH connection (default: <i>5145</i> ).
<b>Use Compression</b>	Here you may activate/deactivate data compression (standard gzip quality) for the SSH connection (default: <i>yes</i> ).
<b>Override SyncIP-Primary / Override SyncIP-Secondary</b>	<b>Note:</b> This parameter is only available in <i>Advanced View</i> mode.  The default HA sync is carried out between the box IPs of the HA partners. These override parameters allow using the IP addresses of the private uplink connection between the HA partners. Simply enter the proper IP addresses and the log-message transfer is done via the private uplink. This may come handy if the synchronising load is quite high.
<b>TCP Sync Frequency (lines)</b>	As a matter of fact this parameter is only available if parameter <i>Store on Disk</i> (see 11.3.1 Basic Setup, page 447) is set to <i>yes</i> . This parameter defines the number of log messages after which synchronisation is started. The default value of <i>0</i> indicates nothing else than immediate synchronisation as soon as a log message is received.

### 11.3.5 Relaying Setup

The following parameters are available for relaying configuration to an external host:

**List 18-42** MC Syslog Server configuration - Relaying Setup - section Relaying Setup

Parameter	Description
<b>TCP Retry Interval [s]</b>	Here the time interval (in seconds) is defined at which a TCP retry should be carried out if the connection breaks.

**List 18-43** MC Syslog Server configuration - Relaying Setup - section SSL Delivery Setup

Parameter	Description
<b>SSL Peer Authentication</b>	This parameter defines whether authentication takes place when establishing the SSL connection. The following options are available: <ul style="list-style-type: none"> <li>➤ <b>no_peer_verification</b> (default)</li> <li>➤ <b>verify_peer_with_locally_installed_certificate</b> Selecting this option requires manual import of a valid SSL certificate from the active connecting system to the active destination system.</li> </ul>
<b>SSL Busy Timeout [s]</b>	This timeout defines for how long (in seconds) a SSL connection may be in busy condition until it is terminated (default: <b>300</b> ).
<b>SSL Close Timeout [s]</b>	This timeout defines for how long (in seconds) a SSL connection may be in close condition until it is terminated (default: <b>60</b> ).
<b>SSL Idle Timeout[s]</b>	This timeout defines for how long (in seconds) a SSL connection may be in idle condition until it is terminated (default: <b>43200</b> ).

### 11.3.6 Relay Filters

This view offers parameters for configuring profiles, which define the log file type which is to be transferred/streamed. However, this section requires parameter **External Relaying** (11.3.1 Basic Setup, page 447) to be set to **yes** in order to become active.

For creating a new relay filter, click **Insert ...** and enter a name for the filter.

**List 18-44** MC Syslog Server configuration - Relay Filters - section Data Origin

Parameter	Description
<b>Filter Box Affiliation</b>	This parameter specifies whether additional information (for example box, cluster, range) is transmitted with the log entries (default: <b>yes</b> ). Setting this parameter to <b>yes</b> activates and requires parameter group <b>Originator Systems</b> (see below).

**List 18-44** MC Syslog Server configuration - Relay Filters - section Data Origin

Parameter	Description
<b>Originator Systems</b>	Take into consideration that this parameter group is only available if parameter <b>Filter Box Affiliation</b> is set to <b>yes</b> . The configuration dialogue for a new and/or existing entry provides the following parameters: <ul style="list-style-type: none"> <li>- <b>Hierarchy Structure</b> This parameter defines the structure of the log entry. The following structure levels are available for selection: <ul style="list-style-type: none"> <li>➤ <b>Box-Only</b> - adds only the box name to the log message</li> <li>➤ <b>Range-Only</b> - adds only the range name to the log message</li> <li>➤ <b>Range-Cluster</b> - adds both, range and cluster name to the log message</li> <li>➤ <b>Range-Cluster-Box</b> (def) - adds the complete structure to the log message</li> <li>➤ <b>Ranges</b> This parameter is only available if parameter <b>Originator Systems</b> is set to a value that contains range structure (that means all except for <b>Box-Only</b>) and allows selecting specific ranges.</li> <li>➤ <b>Clusters</b> This parameter is only available if parameter <b>Originator Systems</b> is set to a value that contains cluster structure and allows selecting specific clusters.</li> <li>➤ <b>Boxes</b> This parameter is only available if parameter <b>Originator Systems</b> is set to a value that contains box structure and allows selecting specific boxes.</li> </ul> </li> </ul>

**List 18-45** MC Syslog Server configuration - Relay Filters - section Data Selection

Parameter	Description
<b>Special File Patterns</b>	Due to the structure of a streamed log message (<range>/<cluster>/<box>/<filename>:<message>), it is possible to restrict log streaming to message containing a certain pattern in their filenames (for example pattern <b>fw</b> when having a filename like <b>server1_fw</b> ) by using this parameter.
<b>Top Level Logdata</b>	The log files offered for selection here are superordinate log files build up of several instances of box and service levels. The following data can be selected: <ul style="list-style-type: none"> <li>➤ <b>Fatal_log</b>. These are the log contents of the fatal log (log instance name: fatal)</li> <li>➤ <b>Firewall_Audit_Log</b>. These are the log contents of the firewall's machine readable audit data stream. Whether data is streamed into the <b>Firewall_Audit_Log</b> has to be configured in the Firewall Parameter Settings on box-level (see SECTION AUDIT INFO GENERATION &gt; Audit-Delivery: Syslog-Proxy). The log instance name corresponding to Syslog-Proxy selected will be <b>trans7</b>.</li> </ul> <p><b>Note:</b> When <b>Log-File</b> is selected in the firewall configuration the data will go into a log file named (Box &gt; Firewall &gt; audit, the instance is named <b>box_Firewall_audit</b>) and thus this filter setting is not applicable. The pertinent one then would be a selection of category <b>Firewall</b> within the box selection portion of the filter.</p>
<b>Affected Box Logfiles</b>	This parameter defines what kind of box logs are to be affected by the syslog daemon. The following options are available: <b>All</b> (any kind of box log is affected), <b>None</b> (default; none is affected) and <b>Selection</b> (activates parameter group <b>Box Log Patterns</b> , see below).

**List 18-45** MC Syslog Server configuration - Relay Filters - section Data Selection

Parameter	Description
<b>Box Log Patterns</b>	<p>Take into consideration that this parameter group is only available if parameter <b>Affected Box Logfiles</b> is set to <b>Selection</b>. The following parameters are available for configuration:</p> <ul style="list-style-type: none"> <li>➤ <b>Log Groups</b> This menu offers every log group for selection that is available on a netfence gateway (for example Control, Event, Firewall, ...).</li> <li>➤ <b>Log Message Filter</b> This parameter is used for defining the affected log types: <b>Selection</b> (activates parameter <b>Selected Message Types</b>, see below), <b>All</b> (default), <b>All-but-Internal</b>, <b>Notice-and-Higher</b>, <b>Warning-and-Higher</b>, <b>Error-and-Higher</b> As you can see the available options are "group selections". If one explicit log type is required, choose <b>Selection</b> and set your wanted type in parameter <b>Selected Message Types</b>, see below.</li> <li>➤ <b>Selected Message Types</b> This parameter allows you to set explicit log types to be affected by syslogging. The following types are available: <b>Panic, Security, Fatal, Error, Warning, Notice, Info, Internal</b></li> </ul>
<b>Affected Service Logfiles</b>	<p>This parameter defines what kind of logs created by services are to be affected by the syslog daemon. The following options are available: <b>All</b> (any kind of service log is affected), <b>None</b> (default; none is affected) and <b>Selection</b> (activates parameter group <b>Service Log Patterns</b>, see below).</p>
<b>Service Log Patterns</b>	<p>Take into consideration that this parameter group is only available if parameter <b>Affected Service Logfiles</b> is set to <b>Selection</b>.</p> <ul style="list-style-type: none"> <li>➤ <b>Log Server-Services</b> Here you define server and service where log messages are streamed from.</li> <li>➤ <b>Log Message Filter</b> This parameter is used for defining the affected log types: <b>Selection</b> (activates parameter <b>Selected Message Types</b>, see below), <b>All</b> (default), <b>All-but-Internal</b>, <b>Notice-and-Higher</b>, <b>Warning-and-Higher</b>, <b>Error-and-Higher</b></li> <li>➤ <b>Selected Message Types</b> This parameter allows you to set explicit log types to be affected by syslogging. The following types are available: <b>Panic, Security, Fatal, Error, Warning, Notice, Info, Internal</b></li> </ul>

### 11.3.7 Relay Destinations

This view offers parameters for configuring profiles, which define where logging ought to be transferred/streamed to.

However, this section requires parameter **External Relaying** (11.3.1 Basic Setup, page 447) to be set to **yes** in order to become active.

For creating a new relay destination, click **Insert ...** and enter a name for the destination.

**List 18-46** MC Syslog Server configuration - Relay Destinations - section Connection Type Setup

Parameter	Description
<b>Connection Type</b>	<p>This menu provides different types for the destination connection:</p> <ul style="list-style-type: none"> <li>➤ <b>Active SSL connect by destination</b> if an external system requests logs actively via SSL</li> <li>➤ <b>Stream SSL to passive destination</b> for std. secure streaming from MC box to external system via SSL</li> <li>➤ <b>Stream plaintext to passive destination</b> for streaming without SSL connection (standard syslog stream)</li> </ul>

**List 18-47** MC Syslog Server configuration - Relay Destinations - section Connect by Destination SSL Setup

Parameter	Description
<b>Local SSL Port</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b>. This menu defines the port that will be used for establishing the SSL connection between MC box and external system. The available standard port range reaches from <b>5244</b> (default) up to <b>5253</b>. If required, you may enter a custom port by simply ticking the checkbox <b>Other</b>. <b>Attention:</b> Make sure to use a port higher than 1024.</p>
<b>Destination SSL Certificate</b>	<p>This certificate is used when selecting <b>Active SSL connect by destination</b> as <b>Connection Type</b>. It holds the certificate of the connecting remote SSL client. This line consists of two buttons: the <b>Show</b> button for displaying the current SSL certificate the <b>Ex/Import</b> button for certificate transfer purpose</p>

**List 18-48** MC Syslog Server configuration - Relay Destinations - section Stream to Destination Setup

Parameter	Description
<b>Destination IP</b>	<p>This parameter is only available when <b>Stream plaintext to passive destination</b> is selected as <b>Connection Type</b>. It allows you to enter the explicit IP address of the log host.</p>
<b>Destination Port</b>	<p>This parameter is only available when <b>Stream plaintext to passive destination</b> is selected as <b>Connection Type</b>. It holds the port that will be used on the log host when connecting.</p>
<b>Transmission Mode</b>	<p>This parameter is only available when <b>Stream plaintext to passive destination</b> is selected as <b>Connection Type</b>. It allows you to choose the transmission protocol (<b>TCP</b> (default) or <b>UDP</b>). When selecting a SSL-capable destination type this parameter is implicitly set to TCP.</p>
<b>Destination SSL Certificate</b>	<p>This certificate is used when <b>Stream SSL to passive destination</b> is selected as <b>Connection Type</b>. It holds the SSL certificate of the destination server. This line consists of two buttons: the <b>Show</b> button for displaying the current SSL certificate the <b>Ex/Import</b> button for certificate transfer purpose.</p>
<b>Destination SSL IP</b>	<p>This parameter is only available when <b>Stream plaintext to passive destination</b> is selected as <b>Connection Type</b>. It is used for entering the IP address of the external system the outgoing SSL tunnel should connect to (figure 18-98, page 447).</p>
<b>Destination SSL Port</b>	<p>This parameter is only available when <b>Stream plaintext to passive destination</b> is selected as <b>Connection Type</b>. It is used for entering the port on the external system the outgoing SSL tunnel should connect to (figure 18-98, page 447).</p>
<b>Loopback SSL Port</b>	<p>This parameter is only available when <b>Stream plaintext to passive destination</b> is selected as <b>Connection Type</b> and defines the to-be-used port for the loopback interface (figure 18-98, page 447). The available standard port range spans the ports <b>5244</b> (default) up to <b>5253</b>. If required, you may enter a custom port by simply ticking the checkbox <b>Other</b>. <b>Attention:</b> Make sure to use a port higher than 1024.</p>
<b>Sender IP</b>	<p><b>Note:</b> This parameter is only available in <b>Advanced View</b>. Depending on your policy routing you may need an explicit sender IP address for streaming log files. If so, this address ought to be entered here.</p>

**List 18-49** MC Syslog Server configuration - Relay Destinations - section Data Tag Policy

Parameter	Description
<b>Keep Structural Info</b>	<p>The default setting <b>no</b> removes the structural information from streamed messages. When set to <b>yes</b> the structure information as originally sent to the MC Syslog is preserved. In other words &lt;range&gt;/&lt;cluster&gt;/&lt;box&gt;/&lt;filename&gt;:&lt;message&gt; becomes &lt;filename&gt;:&lt;message&gt;.</p>



### 11.3.8 Relay Streams

Configuring section **Relay Streams** concludes the configuration of log streaming.

However, this section requires parameter **External Relaying** (11.3.1 Basic Setup, page 447) to be set to **yes** in order to become active.

For creating a new relay stream, click **Insert ...** and enter a name for the relay stream.

**List 18-50** MC Syslog Server configuration - Relay Streams - section Relay Streams

Parameter	Description
<b>Name</b>	Here the name of the stream is displayed.
<b>Active</b>	This parameter allows you to activate/deactivate the selected log stream profile. By default, that is when creating a new profile, this parameter is set to <b>yes</b> .
<b>Log Destinations</b>	Here the available log destinations (defined in 11.3.7 Relay Destinations, page 451) can be selected.
<b>Log Filters</b>	Here the available log filters (defined in 11.3.6 Relay Filters, page 450) can be selected.

## 11.4 Service process and log file structure

<moduledir> = /opt/phion/modules/server/msyslog

**Fig. 18-99** Log file structure of service processes overview

Process name	Executable	GUI log file name	Description
activate	<moduledir>/bin/activate	<server>_<service>	configuration activation, on an optional MC HA partner the activation will also trigger the start of process <server>_<service>_sshd on both systems if HA synchronisation is configured as on
<server>_<service>	<moduledir>/bin/msylogd	<server>_<service>	the actual service running on the active MC partner which is in charge of starting, terminating and monitoring of sub-processes
<server>_<service>_slgd	/sbin/syslog-ng	<server>_<service>	the subprocess running on the active MC partner that corresponds to the actual syslog engine. This process is in charge of the actual log processing. Depending on the actual configuration settings it may write messages directly to the local disk on the active MC HA partner or transfer all [HA sync] or a filtered subset of messages to external UDP/TCP sockets using syslog protocol or to local TCP listening sockets on the loopback or to named pipes (FIFOs) from where they are read by some of the various sub-processes below.
<server>_<service>_sshc	<moduledir>/ssh/sshc.msyslog	n/a	the subprocess running on the active MC partner that is in charge of transferring log messages to the HA partner via SSHv2 port forwarding (client end)
<server>_<service>_sshd	<moduledir>/ssh/sshd.msyslog	<server>_<service>_ssh	the subprocess running on both MC HA partners that is in charge of receiving log messages from the active MC HA partner via SSHv2 protocol (server end) and forwarding them to the local syslogd process which will in turn write the messages to the local disk on the passive MC HA partner
<server>_<service>_csslsrv	/usr/sbin/stunnel	<server>_<service>_csslsrv	the subprocess running on the active MC HA partner responsible for the termination and forwarding to the syslog engine of received SSL encapsulated log messages
<server>_<service>_sslsrv	/usr/sbin/stunnel	<server>_<service>_sslsrv	the subprocess running on the active MC HA partner responsible for the termination of SSL connections (stunnel server) originating from external log host which seek to be fed relayed log messages. The subprocess will read from a named pipe (FIFO) upon successful connection by an external SSL client. Log messages are fed into the pipe by the syslog engine and reach the requestor via an SSL encapsulated log stream.
<server>_<service>_sslclt	/usr/sbin/stunnel	<server>_<service>_sslclt	the subprocess running on the active MC HA partner responsible for originating (stunnel client) SSL connections to external log hosts which are subsequently fed relayed log messages through the SSL connection. The subprocess will listen on a separate TCP listening socket per destination on the loopback for messages sent by the syslog engine and forward the messages via SSL encapsulated log streams to the log hosts.



## 11.5 Supported Ciphers and Cipher Preference by the Stunnel-based Sub-processes

AES128-SHA:DES-CBC3-SHA:AES256-SHA:DH-RSA-AES128-SHA:DHE-RSA-AES128-SHA:IDEA-CBC-SHA:EDH-RSA-DES-CBC3-SHA

**Note:**

DES encryption is not supported due to its limited resistance against brute force attacks.

## 11.6 Filtering Policy

Structure of a syslog conformant log line as received by the syslog engine:

```
'<'PRI'>'<DATE/TIME> <HOSTNAME> <PROGRAM NAME>[ '['<PID>']' ]: <MESSAGE>\n
```

- '<'PRI'>' - two digit decimal number enclosed in angled brackets containing information on both syslog facility and log level

**Note:**

All logs sent by phion systems conform to syslog facility user.

**Note:**

The log facility is a parameter that can be used when building filter conditions for log relaying.

- <DATE/TIME> - three letter English month abbreviation 'blank' day of month 'blank' 2-digit-hour [00-23]:2-digit-minute[00-59]:2-digit-second[00-59] example: Jul 31 14:08:01
- <HOSTNAME> - hostname or IP address of the system the message originates from (possibly also the address of a relay host)
- <PROGRAM NAME> >[ '['<PID>']' ] - typically the name of the application the log message originates from. Note that an appended process ID number enclosed by square brackets may be part of this so-called **program name**. A colon follows the program name. The colon is used as indicator that all remaining portions of text actually belong to the actual log message part
- <MESSAGE> - the actual log message data

phion netfence gateways use the program name to add information as to the origin of a log message. To this end the actual log line is reconstructed before being sent to the gateway's syslog proxy service (bsyslog) for external delivery. The reconstruction entails replacing the original program name by the name of the log instance, that is the file, the log message would go into in directory /var/phion/logs if it were solely written to disk. The original program name and message are simply moved further behind and now together form the new message part.

```
'<'PRI'>'<DATE/TIME> <HOSTNAME> <PROGRAM NAME>[ '['<PID>']' ]: <MESSAGE>\n
```

is changed to

```
'<'PRI'>'<DATE/TIME> <HOSTNAME> <LOG-INSTANCE-NAME>: <PROGRAM NAME>[ '['<PID>']' ]: <MESSAGE>\n
```

An example for a log instance name would be box\_Firewall referring to log file /var/phion/logs/box\_Firewall.log.

The added <LOG-INSTANCE-NAME> is used by the Syslog Proxy service on a netfence gateway to find out as to which received log messages are supposed to be sent to which destination.

On a per destination basis the program name field may be overwritten by the syslog proxy before sending the log message on to the destination. The intention behind this is that this information is extracted by the MC Syslog Server to determine the local file underneath /var/phion/mlogs into which the log message is written and additionally this information may again be used for filtering purposes when log relaying to external security management systems by the MC is intended

The policy adopted by a netfence gateway is as follows:

➤ **MC-managed box**

**Table 18-20** Filtering policy - MC-managed box

Parameter	Value	Explicit node name	Explicit hierarchy info	Used program name
Add Range/Cluster Info	yes			<box name>/<LOG-INSTANCE-NAME>
	no			
Override Node Name	no			
	yes	<NAME>	Range	<range>/<NAME>
			Range and Cluster	<range>/<cluster>/<NAME>
			Range, Cluster and Box	<range>/<cluster>/<box name>/<NAME>
Box		<box name>/<NAME>		

➤ **self-managed box**

**Table 18-21** Filtering policy - self-managed box

Parameter	Value	Explicit node name	Explicit hierarchy info	Used program name
Override Node Name	no			<box name>/<LOG-INSTANCE-NAME>
	yes	<NAME>	none	<range>/<NAME>
			Box	<box name>/<NAME>

The log messages received by the MC Syslog server thus contain additional information stored in the program name. First this information is used by the MC syslog server to determine the file into which a particular log message is meant to be written, provided local disc storage is desired. The log file is simply equal to /var/phion/mlogs/<program name of log message>. From the table above it becomes clear that this mechanism allows for hierarchical depositing of log messages. If to override settings are used on the transmitting managed box all streamed log instances of the box are simply replicated under /var/phion/mlogs/<range>/<cluster>/<box name>.

Yet it may sometimes be desirable to bundle together certain log contents, that are located in different files on the box, either for central storage or relaying purposes.

A good example for this is the firewall log. From the box's point of view firewall related log content goes into several files. On one hand there is the log output generated by the local firewall and on the other hand there is the log output generated by the forwarding firewall service. In order to collect both outputs into a single file on the MC you would define a filter on the streaming box comprising the aforementioned two logging components and a destination corresponding to the MC where you now make use of the override node name option. Choosing for example "allfirewall" as an explicit node name you have ascertained that a single file instance will be used on the MC. Depending on your exact intentions you may now adjust the explicit hierarchy information, that is the path information that is prepended to "allfirewall".

## 11.7 Example Configurations for Syslog Proxy and MC Syslog Server

In the following configuration examples, the essential settings required to be configured in the Syslog Proxy service (on the box) and on the MC Syslog Server (on box level of the MC) are described. For a detailed parameter description, please refer to 5.2.3 Syslog Streaming, page 115 and 11.3 Configuring, page 447 in this chapter.

The examples given consider the following scenarios:

- Log message streaming using TCP&UDP (non SSL)
- Log message streaming using SSL
- Relaying of log messages using SSL

### 11.7.1 Log Message Streaming using TCP&UDP (non SSL)

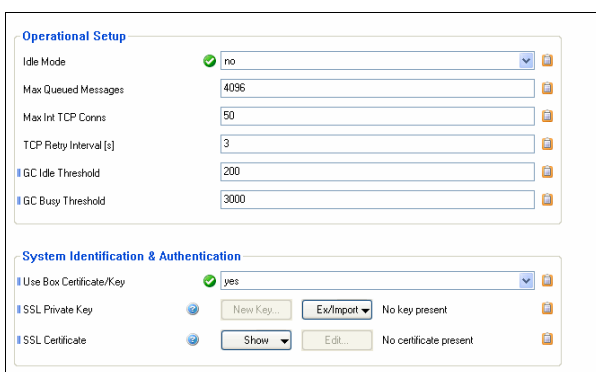
To configure log message streaming using TCP&UDP proceed as follows:

#### 11.7.1.1 Configuration of Syslog Streaming

Enter  **Box** >  **Infrastructure Services** >  **Syslog Streaming** on MCs box-level.

- **Basic Setup** view (with active **Advanced View**)

Fig. 18-100 Example 1: Syslog Proxy - Basic Setup



Set parameter **Idle Mode** to **no**.

Though not using an SSL certificate, leave parameter **Use Box Certificate/Key** set to **yes**. If setting is changed to **no**, the parameters **SSL Private Key** and **SSL Certificate** become mandatory, as it is assumed that another certificate than the box certificate will be used. With all other parameters set properly, availability of a certificate will be ignored.

- **Logdata Filters** view

Define **Infrastructure Services - Syslog Streaming - Logdata Filters - section Affected Box Logdata** and **Infrastructure Services - Syslog Streaming - Logdata Filters - section Affected Service Logdata** in this section, specify the log file types to be sent to the MC Syslog Server.

- **Logstream Destinations** view

Set parameter **Remote Loghost** to **explicit-IP**. This setting causes the log files to be streamed to the MC-Server IP.

Leave parameter **Loghost Port** at the default setting **5144**.

Set parameter **Use SSL Encapsulation** to **no**.

Set parameter **Add Range/Cluster Info** to **yes** to maintain the log files structure Range/Cluster/Box.

If set to **no**, the log files are saved in a directory labelled with the box' name below the **Local Log Directory** defined on the MC Syslog server (see below).

- **Logdata Streams** view







Define combinations of **Logdata Filters** and **Logstream Destinations** in this section. Generally, this feature is useful when

- log files are streamed to multiple destinations.
- streaming is not required continuously for all log file types.

#### Note:

Through setting parameter **Active** to **no**, streaming can be interrupted at all times.

#### 11.7.1.2 Configuration of MC Syslog Service

Enter  **Box** >  **Virtual Servers** >  <servername> >  **Assigned Services** >  <servicename> (**msyslog**) >  **MC Syslog Service** on MCs box-level.

- **Basic Setup** view

Set parameter **Idle Mode** to **no**.

Create **Service Key** and **Service Certificate**. Creation is mandatory, though key and certificate are not used without SSL Encapsulation.

Set parameter **Support Trusted Data Reception** to **no**. Set parameter **Store on Disk** to **yes** to enable saving of received log messages to harddisk.

- **Local Storage** view (with active **Advanced View**)

Specify the **Local Log Directory** as saving location for received log messages. The default path is `/var/phion/mlogs`. You may leave the default settings.

## 11.7.2 Log Message Streaming using SSL

To configure log message streaming using SSL proceed as follows:

### 11.7.2.1 Configuration of Syslog Streaming

Enter **Box** > **Infrastructure Services** > **Syslog Streaming** on MCs box-level.

- **Basic Setup** view (with active **Advanced View**)  
Set parameter **Idle Mode** to **no**.  
Set parameter **Use Box Certificate/Key** to **yes**.
- **Logdata Filters** view  
Define **Infrastructure Services - Syslog Streaming - Logdata Filters - section Affected Box Logdata** and **Infrastructure Services - Syslog Streaming - Logdata Filters - section Affected Service Logdata** in this section, specify the log file types to be sent to the MC Syslog Server.
- **Logstream Destinations** view  
Set parameter **Remote Loghost** to **Management-Centre**. This setting causes the log files to be streamed to the MC-Server IP.

**Note:**  
With **Remote Loghost** set to **Management-Centre**, the Master Certificate of the MC is automatically used as Remote Certificate, that is **Peer SSL Certificate**. Importing the Master Certificate into the **Peer SSL Certificate** field is thus not necessary.

Configure the parameter **Loghost Port** to match the value in parameter **SSL Listen Port (Trusted Data Reception)** view) on the MC Syslog Server. By default, port 5143 is used for SSL connections.

**Attention:**  
Do not use port 5144, as this setting only works when log messages are streamed without SSL Encapsulation. The log file data will arrive corrupt on the MC Syslog Server if port 5144 is used.

**Note:**  
If you change the port assignment to another port than the default 5143, adjusting the local firewall rule set might become necessary.

Set parameter **Transmission Mode** to **TCP**.  
Set parameter **Add Range/Cluster Info** to **yes** to maintain the log files structure Range/Cluster/Box.  
If set to **no**, the log files are saved in a directory labelled with the box' name below the **Local Log Directory** defined on the MC Syslog server.

- **Logdata Streams** view  
Define combinations of **Logdata Filters** and **Logstream Destinations** in this section. Generally, this feature is useful when
  - log files are streamed to multiple destinations.
  - streaming is not required continuously for all log file types.

**Note:**  
Through setting parameter **Active** to **no**, streaming can be interrupted at all times.

### 11.7.2.2 Configuration of MC Syslog Service

Enter **Box** > **Virtual Servers** > <servername> > **Assigned Services** > <servicename> (**msyslog**) > **MC Syslog Service** on MCs box-level.

- **Basic Setup** view  
Set parameter **Idle Mode** to **no**.  
Create **Service Key** and **Service Certificate**.  
Set parameter **Support Trusted Data Reception** to **yes**.  
Set parameter **Store on Disk** to **yes** to enable saving of received log messages to harddisk.
- **Support Trusted Data Reception** view (with active **Advanced View**)  
Configure the parameter **SSL Listen Port** to match the value in parameter **Loghost Port (Logstream Destinations)** view) on the Syslog Proxy. By default, port **5143** is used for SSL connections. Pay attention to the limitations concerning port choice as described above.  
Set parameter **Service Certificate** to **USE\_MC\_SSL\_Cert**. With this setting, boxes can authenticate themselves at the MC Syslog Server using their box certificates.  
Set parameter **Client Authentication** to **verify\_peer\_with\_locally\_installed\_certificate**. The setting causes the box certificate to be authenticated against the MC certificate.  
Import the box certificate of every box, whose log messages are collected by the MC Syslog Server, into the **Trusted Clients** field.
- **Local Storage** view (with active **Advanced View**)  
Specify the **Local Log Directory** as saving location for received log messages. The default path is `/var/phion/mlogs`. You may leave the default settings.

## 11.7.3 Relaying of Log Messages Using SSL

Relaying follows the streaming of log messages. Relaying can be configured with or without SSL encapsulation, regardless of encryption settings defined for streaming. Log messages can be relayed to an external host after they have been written to disk on the MC Syslog Server or they can immediately be passed to the external host without this intermediate step. The following example settings can succeed both of the configurations described above.

To configure relaying using SSL proceed as follows.

### 11.7.3.1 Syslog Proxy Configuration

No further settings are required on the box where log messages are generated.

#### Note:

A configuration requirement exists, though, regarding the setting of the parameter **Add Range/Cluster Info** in the **Log Data Tagging** section as it directly influences usage of the parameter **Filter Box Affiliation** in the **Relay Filters** view of the MC Syslog Server. See below for details.

### 11.7.3.2 MC Syslog Server Configuration

Enter **Box** > **Virtual Servers** > <servername> > **Assigned Services** > <servicename> (**msyslog**) > **MC Syslog Service** on MCs box-level.

#### ➤ Basic Setup view

Set parameter **External Relaying** to **yes**.  
Create **Service Certificate** and **Service Key**.  
Export the SSL Certificate to a file and make it available for the external host. The external host has to import the certificate in order to authenticate itself against the MC Syslog Server (see also parameter **Destination SSL Certificate** below with destination types using SSL).

#### ➤ Relaying Setup view

Set parameter **SSL Peer Authentication** to **verify\_peer\_with\_locally\_installed\_certificate**.

#### ➤ Relay Filters view

Configuration options in the **Relay Filters** view have a similar function to the filtering options specified through the **Logdata Filters** view in the Syslog Proxy configuration (**Configuration Service** - 5.2.3.2 Logdata Filters, page 116). Here they allow defining the log messages, which are to be relayed, by their type.  
The effect of parameter **Filter Box Affiliation** set to **yes** is directly dependant of parameter setting **Add Range/Cluster Info** in the **Log Data Tagging** section of the Syslog Proxy (see above). Reason for this is, that for example relaying through a Range-Cluster-Box hierarchy structure can only work, if Range-Cluster-Box information has originally been maintained during log file streaming.

#### Note:

Using **Filter Box Affiliation** demands specification of **Originator Systems**. This demand can only be satisfied, if Range/Cluster/Box information has been maintained during log message streaming.

#### Affected Box Logfiles / Affected Service Logfiles

The all-embracing method easiest to configure, is to relay **Affected Box Logfiles** and **Affected Service Logfiles**. If unfiltered relaying is not desired, choose **Selection** in the Affected Box/Service Logfiles parameters and select the log file types to be relayed. The parameter **Special File Patterns** allows setting relay filters on terms of filtering for character strings (for example `box_Event`).

#### ➤ Relay Destinations view

#### Note:

The connection type **Stream plaintext to passive destination** is used when log messages are relayed without SSL Encapsulation.

#### Using Destination Type Stream SSL to passive destination:

➤ Set parameter **Connection Type** to **Stream SSL to passive destination**, if the destination the MC Syslog server is relaying to, is passively awaiting log message delivery.

#### Destination SSL Certificate

Connection type using SSL require certificate exchange with the external client/host messages are relayed to. Import the destination server's certificate in this place. Define the destination IP through the parameter **Destination SSL IP**.

Define the connection port for relaying through the parameter **Destination SSL Port**. The standard port range for this purpose spans ports 5244 to 5253.

Set the parameter **Keep Structural Info** to **yes** to maintain the original names of the relayed log files.

#### Using Destination Type Active SSL connect by destination:

➤ Set parameter **Connection Type** to **Active SSL connect by destination** if the external host is actively querying for log messages.

➤ Specify a **Local SSL Port** (parameter requires **Advanced View** in order to be available). The connection between MC Syslog Server and destination system will be established on this port. The standard port range for this purpose spans ports 5244 to 5253.

#### Note:

In case the MC Syslog Server has been configured to **Sync to HA Partner**, do not specify the same port as is defined in the parameter **SSH Listen Port** in the **HA Synchronization** view.

#### Destination SSL Certificate

Connection types using SSL require certificate exchange with the external client/host messages are relayed to. Import the remote SSL client's certificate in this place.

Set the parameter **Keep Structural Info** to **yes** to maintain the original names of the relayed log files.

#### ➤ Relay Streams view

Define combinations of Relay Destinations and Relay Filters in this section. Generally, this feature is useful when log files are relayed to multiple destinations and/or relaying is not required continuously for all log file types.

#### Note:

Through setting parameter **Active** to **no**, relaying can be interrupted at all times.



## 12. MC Firewall Audit Viewer

### 12.1 General

Fig. 18-101 MC FWAudit Viewer

Box	Cluster	Range	Date/Time	Box	Operation	Type	Proto	Src Dev
S10-QA17	QA-Extern	1	2008 12 10 08:53:00	m1k-QA49_QA-Extern_2	LocalRemove	LIN	ICMP	INT
S10-QA27	QA-Extern	1	2008 12 10 08:53:01	m1k-QA49_QA-Extern_2	LocalAllow	LOUT	TCP	INT
m3000-QA29	QA-Extern	2	2008 12 10 08:53:01	m1k-QA49_QA-Extern_2	LocalRemove	LOUT	TCP	INT
m1k-QA49	QA-Extern	2	2008 12 10 08:53:01	m1k-QA49_QA-Extern_2	LocalRemove	LIN	UDP	INT
m3k-QA25	QA-Extern	2	2008 12 10 08:53:01	m1k-QA49_QA-Extern_2	LocalRemove	LIN	UDP	INT
m200-QA21	QA-Remote	2	2008 12 10 08:53:01	m1k-QA49_QA-Extern_2	LocalRemove	LIN	UDP	INT
			2008 12 10 08:53:02	m1k-QA49_QA-Extern_2	LocalAllow	LIN	UDP	INT
			2008 12 10 08:53:02	m1k-QA49_QA-Extern_2	LocalAllow	LIN	UDP	INT
			2008 12 10 08:53:02	m1k-QA49_QA-Extern_2	LocalAllow	LIN	UDP	INT
			2008 12 10 08:53:02	m1k-QA49_QA-Extern_2	LocalAllow	LIN	UDP	INT
			2008 12 10 08:53:02	m1k-QA49_QA-Extern_2	LocalRemove	LIN	UDP	INT
			2008 12 10 08:53:06	m1k-QA49_QA-Extern_2	LocalAllow	LOUT	TCP	INT
			2008 12 10 08:53:06	m1k-QA49_QA-Extern_2	LocalRemove	LOUT	TCP	INT
			2008 12 10 08:53:06	m1k-QA49_QA-Extern_2	LocalAllow	LIN	UDP	INT
			2008 12 10 08:53:06	m1k-QA49_QA-Extern_2	LocalAllow	LIN	UDP	INT
			2008 12 10 08:53:06	m1k-QA49_QA-Extern_2	LocalAllow	LIN	UDP	INT
			2008 12 10 08:53:09	m1k-QA49_QA-Extern_2	LocalAllow	LIN	UDP	INT
			2008 12 10 08:53:11	m1k-QA49_QA-Extern_2	LocalRemove	LIN	UDP	INT
			2008 12 10 08:53:11	m1k-QA49_QA-Extern_2	LocalAllow	LOUT	TCP	INT
			2008 12 10 08:53:11	m1k-QA49_QA-Extern_2	LocalRemove	LOUT	TCP	INT
			2008 12 10 08:53:12	m1k-QA49_QA-Extern_2	LocalRemove	LIN	UDP	INT
			2008 12 10 08:53:16	m1k-QA49_QA-Extern_2	LocalAllow	LOUT	TCP	INT
			2008 12 10 08:53:16	m1k-QA49_QA-Extern_2	LocalRemove	LOUT	TCP	INT
			2008 12 10 08:53:21	m1k-QA49_QA-Extern_2	LocalAllow	LOUT	TCP	INT
			2008 12 10 08:53:21	m1k-QA49_QA-Extern_2	LocalRemove	LOUT	TCP	INT
			2008 12 10 08:53:25	m1k-QA49_QA-Extern_2	LocalRemove	LIN	UDP	INT
			2008 12 10 08:53:26	m1k-QA49_QA-Extern_2	LocalAllow	LOUT	TCP	INT
			2008 12 10 08:53:26	m1k-QA49_QA-Extern_2	LocalRemove	LOUT	TCP	INT

This service allows debugging and traffic information viewing for multiple gateways in one central location, thus allowing to diagnose connection problems within complex network environments usually in a fraction of the time that would be required as compared to diagnosing the problems from the logs or the access cache on every single gateway.

The collection and processing of audit log information is realized by a service on the phion management centre, the MC Audit Info Service.

For large environments or high performance environments, dedicated netfence boxes can be used to collect and retrieve Firewall Audit info, the so-called FW Audit Collector.

The MC Audit service receives structured firewall data from multiple netfence boxes and stores the firewall audit information in relational database installed on the MC.

The firewall audit information provides all information related to firewall session in a machine-readable format. The information is similar to the already available Firewall Audit log, but additionally the relational database allows complex queries. In contrast to the Firewall Access Cache, the MC Audit Viewer does not automatically aggregate

data but includes date and time as well as all session-related information and allows filtering on these.

Filtering of FW Audit data supports the following criteria:

- Rule name
- Protocol
- Source IP Address (netmasks may be used)
- Destination IP Address (netmasks may be used)
- Interface name (either Source or Destination)
- Address, i.e. either Source or Destination IP matches (netmasks may be used)
- Port number and service name
- Source Interface name
- Destination Interface name

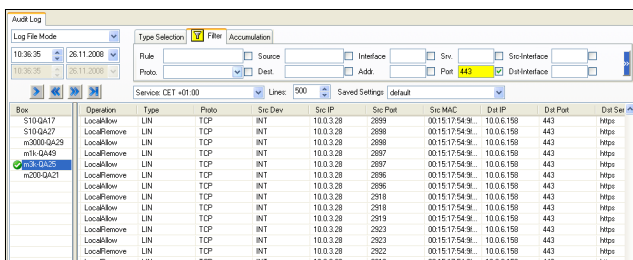
Additionally, the so-called **Type Selection** supports restriction based on the following criteria:

- Traffic Selection: Forwarding traffic, Local In traffic, Local Out traffic, Loopback traffic

- Event Selection:  
Allowed, Blocked, Dropped, Fail, ARP, IPS Hit, Removed

Similar to the phion.a Log Viewer, the Firewall Audit Info Viewer supports navigating to a dedicated date/time as well as browsing backward and forward. After a session has been removed, the FW Audit also contains the number of transferred bytes for this session. Through optional accumulation of FW Audit data a consolidated view similar to the access cache can be achieved. Additionally the centralized FW Audit Viewer supports FW Audit queries across multiple boxes.

Fig. 19 Audit Info Viewer



Box	Operation	Type	Proto	Src Dev	Src IP	Src Port	Src MAC	Dst IP	Dst Port	Dst Ser
S10-Q417	LocalAllow	Local	TCP	INT	10.0.3.28	2889	0015:17:54:9c	10.0.6.158	443	Https
S10-Q427	LocalRemove	Local	TCP	INT	10.0.3.28	2888	0015:17:54:9c	10.0.6.158	443	Https
m000-Q428	LocalAllow	Local	TCP	INT	10.0.3.28	2888	0015:17:54:9c	10.0.6.158	443	Https
m11-Q449	LocalRemove	Local	TCP	INT	10.0.3.28	2887	0015:17:54:9c	10.0.6.158	443	Https
m000-Q428	LocalAllow	Local	TCP	INT	10.0.3.28	2887	0015:17:54:9c	10.0.6.158	443	Https
m000-Q421	LocalRemove	Local	TCP	INT	10.0.3.28	2886	0015:17:54:9c	10.0.6.158	443	Https
	LocalAllow	Local	TCP	INT	10.0.3.28	2886	0015:17:54:9c	10.0.6.158	443	Https
	LocalRemove	Local	TCP	INT	10.0.3.28	2918	0015:17:54:9c	10.0.6.158	443	Https
	LocalAllow	Local	TCP	INT	10.0.3.28	2918	0015:17:54:9c	10.0.6.158	443	Https
	LocalAllow	Local	TCP	INT	10.0.3.28	2919	0015:17:54:9c	10.0.6.158	443	Https
	LocalRemove	Local	TCP	INT	10.0.3.28	2923	0015:17:54:9c	10.0.6.158	443	Https
	LocalAllow	Local	TCP	INT	10.0.3.28	2923	0015:17:54:9c	10.0.6.158	443	Https
	LocalRemove	Local	TCP	INT	10.0.3.28	2922	0015:17:54:9c	10.0.6.158	443	Https
	LocalAllow	Local	TCP	INT	10.0.3.28	2922	0015:17:54:9c	10.0.6.158	443	Https

#### Note:

Which data will be collected depends on box settings in **Config > Box > Infrastructure Services > General Firewall Configuration > Audit and Reporting > Audit Information Generation** (see **Firewall - 2.1.1.5 Audit and Reporting**, page 129, section **Recorded Conditions** list 4-12, page 130).

## 12.2 Activation

The Audit Info service is available for three different scenarios:

### ➤ local FW Audit Info viewer

Writing FW audit data locally on the netfence gateway can be enabled within the configuration dialogue Box > Infrastructure Services > General Firewall Configuration > Audit and Reporting > Audit Info Generation. In the Settings dialogue select Local-File for Audit Delivery settings.

The firewall now generates appropriate entries for both local and forwarding traffic.

The FW Audit Info viewer is available by using phiona to connect to the Firewall module and selecting the Audit tab.

#### Licensing

The local Audit Info viewer is available on every netfence gateway where an FW audit logfile is generated without the need for an additional license.

### ➤ MC Audit Info viewer

To enable the MC Audit Info Viewer you need to introduce the novel service MC Audit Info Viewer on the MC box. The MC Audit Info viewer is now ready to retrieve audit information from boxes managed by this management centre.

The service uses TCP port 680 to receive FW Audit data. The host firewall ruleset of an updated MC box thus needs to be extended to allow access to port 680 on the management IPs and server IPs. If you have not

modified the host firewall ruleset manually you could simply select "Copy from default" in the context menu. Generation and forwarding of FW Audit data still needs to be enabled for the netfence boxes (see below). Transport of FW Audit data is encrypted by using the MC- and box RSA keys.

If an unmanaged netfence system should send Audit Info data to the introduced MC Audit Info service, the MC Audit Info service provides a configuration to manually import box keys.

To enable generation and forwarding of FW Audit data, connect to the MC configuration tree and open the configuration node Box > Infrastructure Services > General Firewall Configuration. Open the Settings dialogue for Audit and Reporting > Audit Info Generation and change the Audit Delivery parameter to Forward-only or Local-File-and-Forward. The destination IP address and port can be left empty - in that case the FW Audit data is automatically forwarded to the MC IP address.

Querying is possible by using the phiona user interface connecting either to the MC management IP (box) or to the MC server IP (MC).

#### Licensing

The MC Audit Info viewer is available with phion management centre Global Player edition or with phion management centre option pack 2.

### ➤ Audit Info collector (separate box)

Collecting FW Audit data on a separate netfence box is realized by the new service "Audit Info collector". You need to introduce the new service. Configuration see MC Audit Info viewer. Due to performance issues the service should be run on a dedicated system.

Queries are done by first connecting to the box management IP.

#### Licensing

The Audit Info collector requires an extra license and is only available in conjunction with a phion management centre Global Player or with a management centre option pack 2.

## 12.3 Limitations

Please note that writing or querying FW Audit data within the relational database is quite CPU and IO consuming. It is thus strongly recommended to enable transport of FW Audit data with care.

A netfence firewall can handle several thousand of session requests per second, which is already a limit for relational databases (transactions per second). The centralized FW Audit service may get data from dozens of netfence firewalls thus overloading the relational database.

phion recommends to make use of the granular configuration options, which allow reducing traffic by explicitly specifying which data should be forwarded to the FW Audit host.

The FW Audit Service does not synchronize audit data within a HA cluster, neither when running as server service (Audit collector) or when running as local FW Audit Info viewer. For the MC Audit Info viewer and for the FW Audit Info collector, the service may run on the backup box to



collect new data. In case of a failover to the backup box, new Audit data is stored on the backup box and querying of this data needs to be performed on the backup box.

## 13. MC PKI

The phion PKI (Public Key Infrastructure) is a solution similar in scope and functionality to Microsofts PKI delivered with Microsoft Windows 2000/2003 servers and uses ITU-T x509v3 certificates.

A certificate with the V3 extension basic constraints set to CA:true is handled as a CA. This CA can sign end user certificates or other CAs. An x.509v3 certificate contains the fully distinguished name and V3 extensions defining the range of application.

To mark a certificate as revoked, there are certificate revocation lists. Applications can fetch certificate revocation lists from LDAP or HTTP servers. These servers are specified in the certificate as V3 extension crlDistributionPoints.

**Note:**

For theory about certificates have a look at "Kryptografie und Public-Key-Infrastrukturen im Internet" by Klaus Schmeh (ISBN 3-932588-90-8)

Usage of Certificates

- SSL/TLS encryption and authentication of TCP-based protocols like HTTP, SMTP, POP, IMAP, LDAP, ...
- S/MIME: Encryption and signature of e-mails
- IPSec, L2TP
- VPN connections

### 13.1 Installing and Configuring phion PKI

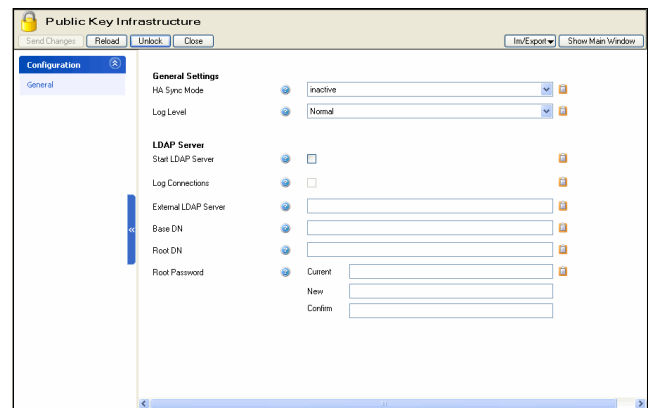
**Attention:**

PKI has to be licensed separately.

Log on to the management centre on box level and create a new service using the software module **MC-PKI**.

Enter the configuration dialogue via **Config > Box > Virtual Servers > <servername> > Assigned Services > <servicename> (pki)**.

Fig. 18-1 Configuration dialogue - PKI



List 18-51 Public Key Infrastructure (PKI) Configuration Settings - section General Settings

Parameter	Description
<b>HA Sync Mode</b>	This parameter enables/disables synchronisation with an optional HA partner.
<b>Log Level</b>	Here you specify the amount of logging. The following options are available: <b>Silent</b> - No logging except for fatal logs <b>Normal</b> - Regular logging <b>Verbose</b> - Regular logging including additional logs (for example for troubleshooting)

List 18-52 Public Key Infrastructure (PKI) Configuration Settings - section LDAP Server

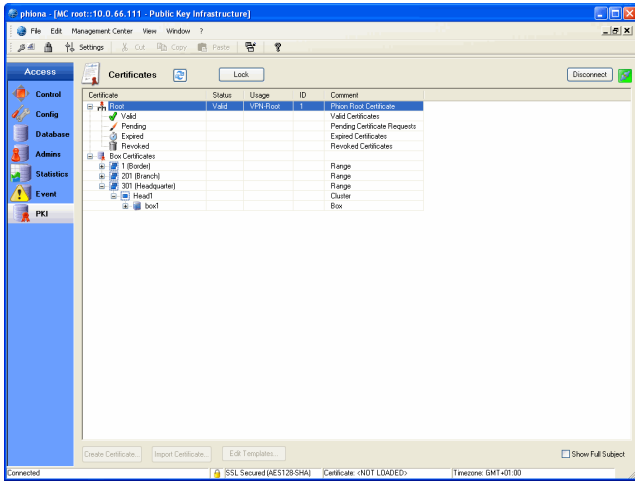
Parameter	Description
<b>Start LDAP Server</b>	Ticking this checkbox starts an LDAP server on the MC box listening on Management IP address port 389 (ldap) and port 636 (ldaps).
<b>Log Connections</b>	Ticking this checkbox enables connection logging on the internal LDAP server.
<b>External LDAP Server</b>	If an external LDAP server ought to be used instead of the internal one, the server IP address or DNS-resolvable name have to be entered here.
<b>Base DN</b>	This parameter specifies the <b>Base Distinguished Name</b> for inserting and searching CRLs on the LDAP server (for example <code>dc=phion,dc=com</code> ).
<b>Root DN</b>	Here the distinguished name of the LDAP user for importing CRLs on the LDAP server is defined.
<b>Root Password</b>	This parameter holds the password for writing on the LDAP server.

### 13.2 User Interface

The PKI shows the certificates in a hierarchical tree view (accessible via box menu entry **PKI**, see figure 18-2). The top level shows all root certificates, which have to be certificate authorities. Additionally, there are the box certificates to get the information of all installed boxes managed by the MC. This information is generated

automatically on the first start of the PKI. If changes apply to installed boxes, right-click **Box Certificates** and then select **Update Box Certificates** from the context menu.

Fig. 18-2 PKI - User Interface



Each CA node contains four subdirectories:

- **Valid** contains all valid and not expired certificates.
- **Pending** contains all unsigned certificate requests.
- **Expired** contains all certificates with exceeded finish dates.
- **Revoked** contains all certificates revoked by the administrator (for example an end-user has lost his/her USB stick holding the VPN certificate).

For viewing the details of a certificate, right-click on the certificate of interest and select **View Certificate**.

Instead of the common name, which is used by default, the certificates can be displayed with their full subject in the user interface's view. To change the view setting, select **Show Full Subject** in the context menu available by right-click on either top level of **Root** or **Box Certificates**.

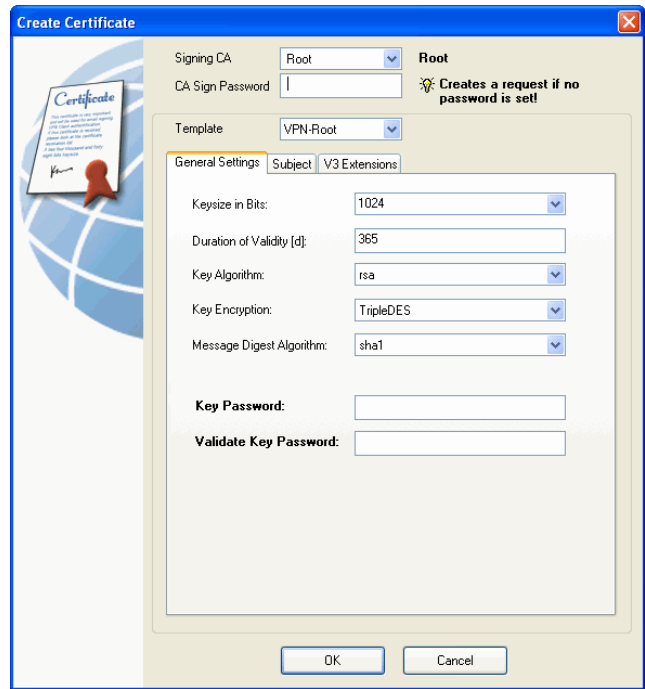
## 13.3 Working with PKI

### 13.3.1 Creating a Certificate

For creating a certificate it is necessary to change from read-only to read-write mode by clicking **Lock**.

Now the PKI is ready for creating a new certificate (via button **Create Certificate ...**).

Fig. 18-3 Configuration dialogue - General Settings tab



List 18-53 Public Key Infrastructure (PKI) - Certificate Creation

Parameter	Description
<b>Signing CA</b>	Via this parameter you specify the certificate authority which ought to sign the new certificate.
<b>CA Sign Password</b>	This field allows entering the password required for signature by the CA. If no password is entered only a certificate request will be created.
<b>Template</b>	Here you may select a pre-defined template (see 13.3.3 Editing Templates, page 461) in order to fill the parameters of this dialogue with "default" values.

#### 13.3.1.1 General Settings Tab

List 18-54 Public Key Infrastructure (PKI) - Certificate Creation - General Settings tab

Parameter	Description
<b>Keysize in Bits</b>	Via this parameter the key size is defined. Normally the value ranges from 512 up to 4096 bits (default: <b>1024</b> bits). Due to modern CPU power, the size should be at least 1024 bits for end-user certificates. When the CAs lifetime is 10 years or longer, the key size should be at least 2048 bits (4096 bits recommended).
<b>Duration of Validity</b>	Defines the validity period of the certificate (in days; default <b>5000</b> days). For example this leads to 5475 days for a root certificate with 15-years validity (365 * 15).
<b>Key Algorithm</b>	Specifies the algorithm used for key creation ( <b>rsa</b> - default; <b>dsa</b> ).
<b>Key Encryption</b>	Specifies the algorithm used for key encryption ( <b>TripleDES</b> - default; <b>IDEA</b> ; <b>DES</b> ).
<b>Message Digest Algorithm</b>	Specifies the hash algorithm ( <b>md2</b> , <b>md5</b> , <b>mdc2</b> , <b>sha1</b> - default).
<b>Password</b>	Defines the certificate password.
<b>Validate Password</b>	Validates the certificate password.

### 13.3.1.2 Subject Tab

List 18-55 Public Key Infrastructure (PKI) - Certificate Creation - Subject tab

Parameter	Description
<b>Common Name</b>	Name of the certificate. <b>Note:</b> Do not use special characters and underscores in the common name.
<b>Email Address</b>	E-mail address of the certificate owner.
<b>Country State or Province Locality Organisation Organisation Unit</b>	Address and organisational information (for example name of the organisation, unit name, ...).

### 13.3.1.3 V3 Extensions

**Note:**

Several parameters in this tab are, in addition to the regular active/inactive equipped with a **Critical** checkbox. Ticking this checkbox enforces the application to use **V3 Extensions**. Additionally, this causes that the certificate may not be used for any other purposes than the ones defined through the parameters **keyUsage** and **extendedKeyUsage**.

**Note:**

For additional information concerning V3 extensions, please have a look at 13.3.13 V3 Extensions (look at RFC 3280), page 463.

List 18-56 Public Key Infrastructure (PKI) - Certificate Creation - V3 Extensions tab

Parameter	Description
<b>basicConstraints</b>	Defines whether the certificate is a CA ( <b>CA:true</b> ) or not ( <b>CA:false</b> - default).
<b>keyUsage</b>	Defines the intended use for the certificate. The following types of usage are available: <b>digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly</b> .
<b>extendedKeyUsage</b>	Extension to the intended use for the certificate. The following types of extended usage are available: <b>serverAuth, clientAuth, emailProtection, codeSigning, timeStamping, OCSPSigning, smarCardLogon, secureMail, msCodInd (MS Individual Code Signing), msCodeCom (MS Commercial Code Signing), msCTLSign (MS Trust List Signing), msSGC (MS Server Gated Cryptography), msEFS (MS Encrypted File System)</b> .
<b>subjectKeyIdentifier</b>	Hash of the subject.
<b>authorityKeyIdentifier</b>	The subject key identifier extension provides a means of identifying certificates that contain a particular public key. The following types of identifiers are available: <b>keyid:always, keyid:copy, issuer:always, issuer:copy</b>
<b>authorityInfoAccess</b>	The authority information access extension indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may include online validation services and CA policy data.
<b>subjectAltName</b>	The subject alternative names extension allows additional identities to be bound to the subject of the certificate. The following types are available: <b>Email, DNS, URI, IP, MS Domain GUID, MS Domain User</b> .
<b>issuerAltName</b>	This extension is used to associate Internet style identities with the certificate issuer.

List 18-56 Public Key Infrastructure (PKI) - Certificate Creation - V3 Extensions tab

Parameter	Description
<b>crlDistributionPoints</b>	Here the distribution points for the Certificate Revocation List (CRL) are defined.
<b>DomainController</b>	Microsoft-specific extension for entering DomainControllers.
<b>nsComment</b>	Allows entering a commentary.

### 13.3.2 Viewing Certificates

For viewing a certificate, select the wanted one, open the context menu and select **View Certificate ...** This opens the **View Certificate** dialogue with 3 tabs providing the complete information.

### 13.3.3 Editing Templates

Clicking **Edit Templates ...** opens the dialogue for editing existing templates.

It has almost the same functionality as the **Create Certificate** dialogue (see 13.3.1 Creating a Certificate, page 460) except for that there is neither a password field nor, of course, a CA selection option.

To edit a template, select it from the **Select Template** pull-down menu, make your changes, and save it with clicking **Save Template**.

To create a new template, select any existing template from the pull-down menu, make your changes, enter a new name in the **Select Template** field, and save it with clicking **Save Template**. The new template will promptly be available in the **Template** list of the **Create Certificate ...** dialogue.

**Attention:**

Deleted predefined templates can only be restored if the PKI is deleted and newly established. Deletion of the PKI will cause deletion of all available certificates as well. Be careful not to delete predefined templates.

### 13.3.4 Create Request

If the password for the signing CA is omitted in the **Create Certificate ...** dialogue, a certificate request is created instead of a certificate.

### 13.3.5 Revoke a Certificate

To revoke a yet valid certificate, select it in the **Valid** folder, right-click on it and select **Revoke Certificate ...** from the context menu. You will be prompted to enter the parent CAs **Sign Password**. After doing so, the revoked certificate is moved to the **Revoked** folder.

### 13.3.6 Delete a Request

Go to a certificate request in the **Pending** directory and right-click on it. Select **Delete Request ...** and click the **Yes** button.

### 13.3.7 Approve a Request

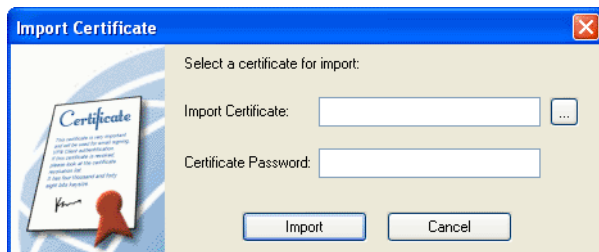
Right-click on a certificate request and select **Approve Request ...** from the context menu. The corresponding dialogue is opened displaying the values of the request. Enter the **Sign Password** of the CA to approve the request.

### 13.3.8 Import Certificates

Select a certificate for import and enter the certificate password. Afterwards click the **Import** button. If no problem arises, the certificate is imported. The PKI reloads the certificates automatically.

An end-user certificate will be added to the signing certificate, if existing. Otherwise the import will fail.

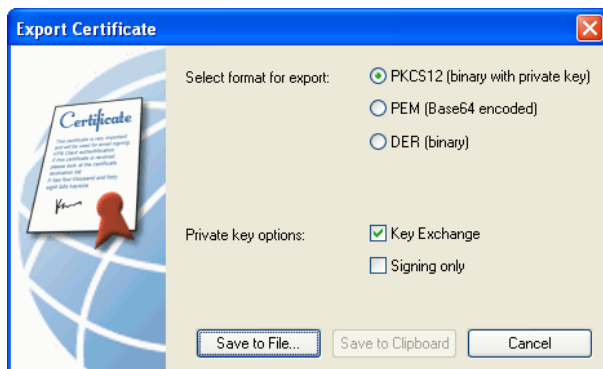
Fig. 18-4 Import Certificate dialogue



### 13.3.9 Export Certificates

For exporting a certificate, mark it and select **Export Certificate ...** from the context menu. This opens the **Export Certificate** dialogue for selecting the required format.

Fig. 18-5 Export Certificate dialogue



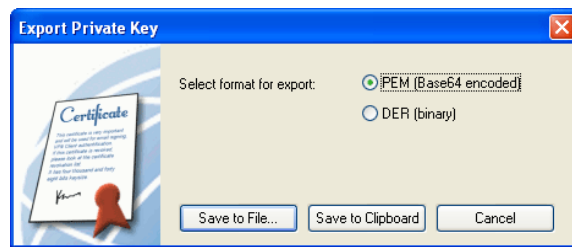
### 13.3.10 Export Private Key

Select the required format and export the key to a file or to the clipboard.

**Note:**

For exporting to clipboard only PEM format is allowed, since DER is a binary format.

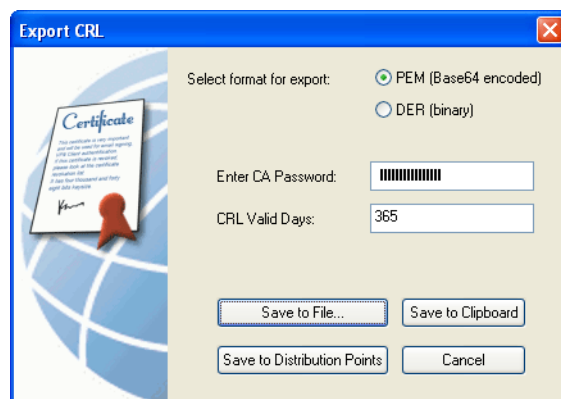
Fig. 18-6 Export Private Key dialogue



### 13.3.11 Export a CRL

A Certificate Revocation List (CRL) is a list of client certificates that were revoked before they expired. To export a CRL, right-click on the Certification Authority and select **Export CRL ...** from the context menu. This opens the **Export CRL** dialogue, where the password of the CA and the duration of validity have to be entered.

Fig. 18-7 Export CRL dialogue



The CRL can either be exported as file, to clipboard or to distribution points. The distribution points are on the ldap server as configured in the PKI service configuration and the local http server of the MC box.

The CRL is accessible at

- ldap://mcip/cn=CommonName,dc=AsInConfig
- ldaps://mcip/cn=CommonName,dc=AsInConfig
- mcip/pki/CommonName.crl

Example:

192.168.10.10/pki/VPN-Root.crl

ldaps://192.168.10.10/cn=VPN-Root,dc=phion,dc=com

**Note:**

For accessing the local http server a local redirect rule has to be added in the MC Firewall.

### 13.3.12 Search a Certificate

In order to search a certificate click CTRL+F or open the context menu of a certificate and select **Search Certificate ...**

For example if you enter "lient" in the **Common Name** field, all certificates containing this string in the common name will be found, as "Client", "Client1" or also "MILIENT".

With key F3 all found certificates can be stepped through.

### 13.3.13 V3 Extensions (look at RFC 3280)

Table 18-22 Definition of V3 Extensions (RFC 3280)

Parameter	Description
<b>basicConstraints</b>	<p>The cA boolean indicates whether the certified public key belongs to a CA. If the cA boolean is not asserted, then the keyCertSign bit in the key usage extension MUST NOT be asserted.</p> <p>OID = 2.5.29.19 CANBECRIT=true</p> <p>Values: true false</p>
<b>keyUsage</b>	<p>The key usage extension defines the purpose (for example, encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted.</p> <p>OID = 2.5.29.15</p> <p>Values (BIT STRING): digitalSignature - (0) nonRepudiation - (1) keyEncipherment - (2) dataEncipherment - (3) keyAgreement - (4) keyCertSign - (5) cRLSign - (6) encipherOnly - (7) decipherOnly - (8)</p> <p>0) sign for entity authentication and data origin authentication with integrity 1) sign with a non-repudiation service 2) encrypt keys for transport using RSA like algorithms, 3) encrypt data, 4) exchange keys using D-H like algorithms, 5) sign certificates, 6) sign CRLs, 7) encrypt data using D-H like algorithms, and 8) decrypt data using D-H like algorithms.</p>
<b>extendedKeyUsage</b>	<p>This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates.</p> <p>OID = 2.5.29.37 CANBECRIT=true</p>
<b>subjectKeyIdentifier</b>	<p>The subject key identifier extension provides a means of identifying certificates that contain a particular public key.</p> <p>OID = 2.5.29.14 CANBECRIT=false</p> <p>Values: hash</p>

Table 18-22 Definition of V3 Extensions (RFC 3280)

Parameter	Description
<b>authorityKeyIdentifier</b>	<p>OID = 2.5.29.35 CANBECRIT=false</p> <p>Values: keyid:always keyid:copy issuer:always issuer:copy</p>
<b>authorityInfoAccess</b>	<p>The authority information access extension indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data. (The location of CRLs is not specified in this extension; that information is provided by the cRLDistributionPoints extension.) This extension may be included in end entity or CA certificates, and it MUST be non-critical.</p> <p>OID = 1.3.6.1.5.5.7.1.1</p> <p>Values: a string, for example OCSP;URI:ocsp.my.host/ or caIssuers;URI:my.ca/ca.html</p>
<b>subjectAltName</b>	<p>The subject alternative names extension allows additional identities to be bound to the subject of the certificate. Defined options include an Internet electronic mail address, a DNS name, an IP address, and a uniform resource identifier (URI).</p> <p>OID = 2.5.29.17 CANBECRIT=true</p> <p>Values: Email - enter an e-mail address or "copy" for copying from subject DNS URI IP MS Domain GUID - for Smartcard Server MS Domain User - for Smartcard User</p>
<b>issuerAltName</b>	<p>This extension is used to associate Internet style identities with the certificate issuer.</p> <p>OID = 2.5.29.18 CANBECRIT=true</p> <p>Values: issuer:copy</p>
<b>cRLDistributionPoints</b>	<p>OID = 2.5.29.31 This lists the distribution points for CRLs.</p> <p>Example: ldap://some.ldap-test.eu/cn=rootcert,dc=ldap-test,dc=eu some.ldap-test.eu/crl/rootcert.crl</p>
<b>DomainController</b>	<p>OID = 1.3.6.1.4.1.311.20.2</p> <p>This is a Microsoft specific extension needed for smartcard logon.</p> <p>Values: Machine ... for a machine SmartCardLogon ... for a user (logon) SmartCardUser ... for a user (logon and e-mail)</p>
<b>nsComment</b>	<p>OID = 2.16.840.1.113730.1.13 Just an extension to provide a possibility for a comment. This is an old Netscape extension.</p>



# 14. MC Firewall

For remote managed netfence gateways a so-called **box tunnel** between MC and boxes can be used.

These box tunnels are handled by the MC service **MC-VPN** and require the configuration of **Virtual Box IPs**.

## 14.1 General

When using virtual management Box IPs (Box Management Tunnels) it is possible either to use the MC as a generic forwarder or to add additional protection using the MC Firewall.

Fig. 18-8 User Interface of a generic forwarder



# 15. VPN GTI

The netfence VPN Graphical Tunnel Interface (GTI) combines phion's leading VPN technology with comfortable VPN tunnel creation and management.

VPN GTI functionality is also available per **Range** and per **Cluster**.

Main features:

- VPN tunnel creation by drag&drop functionality
- Global parameters for VPN compounds
- Individual oversteering of global parameters per tunnel

## 15.1 User Interface

The GTI is accessible via:

- **Config** > **Multi-Range** > **Global Settings** > **VPN GTI Editor (Global)** for company wide VPN structures

- **Config** > **Multi-Range** > **<rangename>** > **Range Settings** > **VPN GTI Editor** for range wide VPN structures

**Note:**  
Requires parameter **Own VPN GTI Editor (Range Configuration)** to be set to **yes**.

- **Config** > **Multi-Range** > **<rangename>** > **Range Settings** > **Cluster** > **Cluster Settings** > **VPN GTI Editor** for cluster wide VPN structures

**Note:**  
Requires parameter **Own VPN GTI Editor (Cluster Configuration)** to be set to **yes**.

A generic forwarder acts like a router and simply forwards traffic to the destination. Since each netfence gateway applies access restrictions by using the configured box ACL a basic security level is guaranteed.

However, if a higher security level is required the management centre can be equipped with a forwarding firewall (**MC Firewall**).

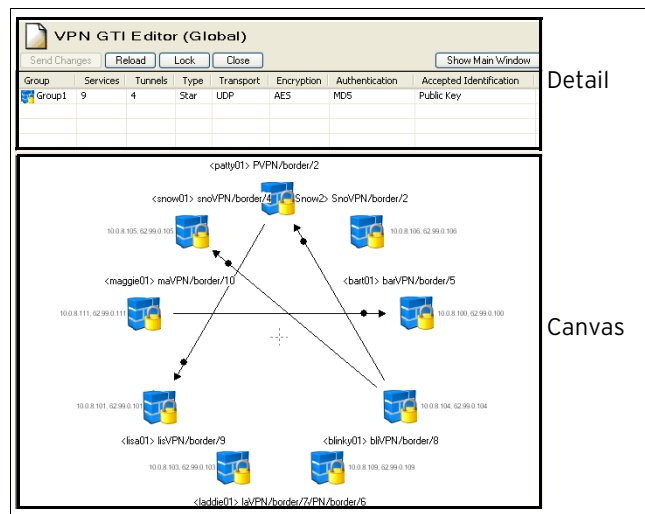
The MC Firewall contains the same features as described in **Firewall**, page 123.

For introducing an MC Firewall it is necessary to have a valid firewall license for the management centre.

The MC Firewall service is created on box level of the MC as described in **Configuration Service** - 4. Introducing a New Service, page 97, and selecting **firewall** as service module.

The configuration of the MC Firewall is analogous to the forwarding firewall of a netfence gateway.

Fig. 18-9 User Interface



As shown above, VPN GTI consists of two sections:

- **Detail** - providing information concerning the **global** tunnel settings of this compound (only in detailed view; see below):
  - **Group** - Name of the VPN group and type-dependent icon (star - ; hub - ; meshed - )
  - **Services** - No. of services that are part of this group
  - **Tunnels** - Number of tunnels within the compound
  - **Type** - Compound type
  - **Transport** - Used transport protocol
  - **Encryption** - Used/required encryption algorithm
  - **Authentication** - Used/required authentication method
  - **Accepted Identification** - Used/required identification method



➤ **Canvas** - here tunnels are created, VPN services are added; that means here your VPN compound is *created*. For creating a tunnel, simply left-click on the tunnel's designated start VPN service and move the cursor (keeping left-clicked) to the designated end VPN service.

**Note:**

By default, tunnels created in VPN GTI are active-passive ones. In order to create active-active tunnels, simply overrule the parameter **Direction** (see 15.2.2.4 Defining Tunnel Properties, page 469) by setting to **active**.

**Note:**

Creating tunnels between external VPN services is NOT possible.

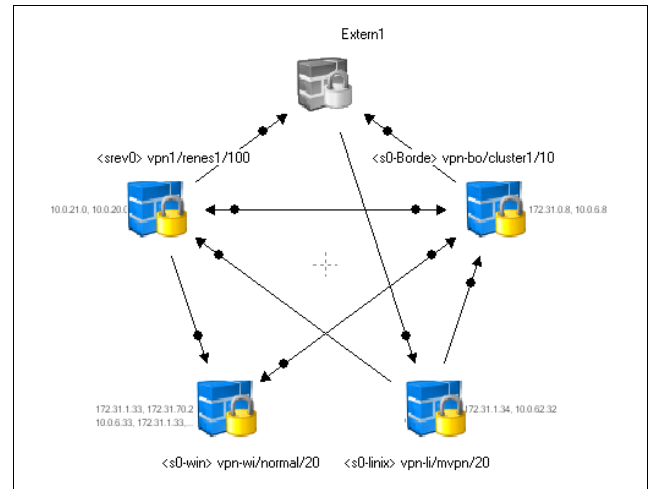
### 15.1.1 User Interface - Detail Section

For adding/editing/deleting VPN groups simply right-click in the **Detail** section and select the desired action from the context menu:

- **Edit Group ...** - opens a dialogue for editing already existing VPN groups; the dialogue itself is identical to the one opened when a new group is added (see 15.2.2 Defining Global Settings for a VPN Group, page 466).
- **Add Group ...** - opens a dialogue for adding new VPN groups (see 15.2.2 Defining Global Settings for a VPN Group, page 466).
- **Delete Group ...** - removes the existing VPN group
- **Add VPN Service to GTI Editor** - adds a VPN service to the selected VPN group
- **Delete VPN Service from GTI Editor ...** - removes a VPN service from the selected VPN group
- **GTI Editor Defaults ...** - opens a dialogue for defining default values used when new VPN groups are created (see 15.2.1 Defining GTI Editor Defaults, page 466).
- **Swap List View** - toggles the group view between TINA and IPSec. The default preference is TINA.
- **Views** - provides several types of views for the Detail section (Tiles, Icons, List, Details).
- **Tools** - standard context menu (contains: Search for Text, Print options, ...)

### 15.1.2 User Interface - Canvas Section

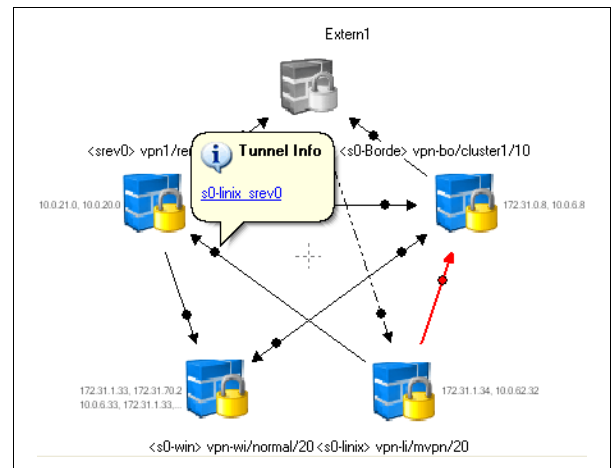
Fig. 18-10 Example VPN group



The GTI canvas provides the following information:

- Name of the VPN service; used format for netfence VPN services:  
`<servername> servicename/cluster/range`
- Configured server **IP addresses** and, optionally, Explicit Bind IP addresses
- Tunnel and tunnel direction with an arrow to the designated tunnel end point using the following colours and line types:
  - black - enabled tunnel
  - grey - disabled tunnel
  - solid line - TINA tunnel
  - chain-dotted line - IPSec tunnel
  - tunnels flagged with one arrow tip - active-passive tunnel (arrow tip points to the passive tunnel endpoint)
  - tunnels flagged with arrow tips on both ends - active-active tunnel
- Tunnel Info node

Fig. 18-11 Open Tunnel Info node

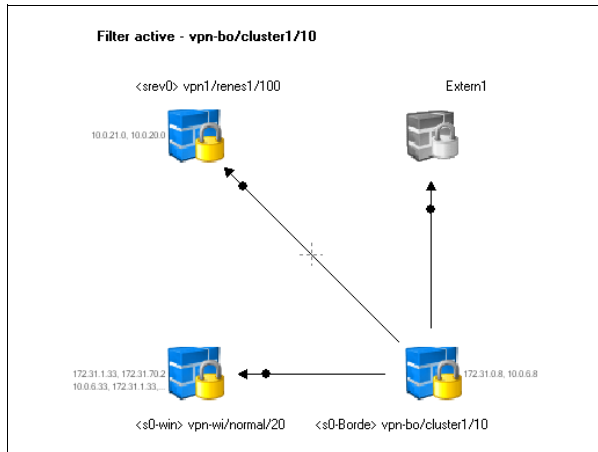


As depicted above, an information bubble is displayed when clicking on a Tunnel Info node. Clicking the link provided, opens a dialogue for viewing/editing tunnel settings.

In addition to the drag&drop functionality, the canvas section offers a context menu providing the following entries:

- **<VPN service name>** - opens a dialogue window displaying the properties of the selected VPN service see 15.2.2.3 Defining VPN Service Properties, page 468).
- **Set Filter to <VPN service name>** - hides every VPN service that is not endpoint of a tunnel initiated by the selected VPN service.

Fig. 18-12 New filtered for <s0-Borde> vpn-bo/cluster1/10



- **Clear Filter** - deletes the set filter
- **Go to Config Tree ...** - opens the configuration tree for the selected VPN service
- **Go to Box <box name>-<box IP address>** - starts the login procedure for the box the VPN service is configured on
- **Add VPN Services to GTI Group ...** - adds a VPN service to the VPN group
- **Delete VPN Service from Group ...** - removes a VPN service from the VPN group
- **Edit Tunnel ...** - opens a dialogue for modifying settings of the selected tunnel
- **Delete Tunnel** - removes the selected tunnel
- **Force Full Update** - forces a complete update of all nodes within the VPN group
- **Show Tunnel Names** - adds the tunnel names to the canvas; reselecting this entry hides the tunnel names again
- **Zoom out/in** - decreases/increases the zoom level
- **Fit to Screen** - ticking this option causes that the complete VPN group is resized according to the available canvas size; however, when increasing canvas size this entry has to be selected again in order to resize view.
- **Show Full Screen (F11)** - switches canvas into full screen mode; for leaving full screen mode, simply use either this entry again or hit F11.

- **View as list** - displays the VPN group structure in table-format; since this view is read-only you will have to change back to graphical display in order to make changes. This is done by using this entry again.

Fig. 18-13 Example VPN group displayed as table

Name	To	Tunnel Type	Disabled	Transport	Encryption	Authenticator
Extern1						
vpn-bo/cluster1/10	vpn-wi/normal/20	TINA	No	UDP	AES	MD5
Extern1_s0-win	Extern1	TINA	No	UDP	AES	MD5
s0-Borde_Extern1	vpn-wi/normal/20	TINA	No	UDP	AES	MD5
s0-Borde_s0-win	vpn1/renes1/100	TINA	No	UDP	AES	MD5
s0-Borde_srev0						
vpn-wi/normal/20						
s0-link_s0-Borde	vpn-bo/cluster1/10	TINA	No	UDP	AES	MD5
s0-link_srev0	vpn1/renes1/100	TINA	No	UDP	AES	MD5
vpn-bo/cluster1/10						
vpn-wi/normal/20	vpn-bo/cluster1/10	TINA	No	UDP	AES	MD5
vpn1/renes1/100						
srev0_Extern1	Extern1	TINA	No	UDP	AES	MD5
srev0_s0-Borde	vpn-bo/cluster1/10	TINA	No	UDP	AES	MD5
srev0_s0-win	vpn-wi/normal/20	TINA	No	UDP	AES	MD5

#### Note:

For every tunnel endpoint introduced through the VPN GTI Editor (Global), dynamical Global GTI Objects are created. These network objects can be utilised when creating firewall rules (see **phion management centre** - 6.3.2.1 Global GTI Objects, page 411 and **Firewall** - 2.2.3 Rules Configuration, page 135, parameter **Reload GTI Objects**).

## 15.2 Configuration

### 15.2.1 Defining GTI Editor Defaults

Especially for lots of VPN groups sharing almost identical configurations it comes handy to define your own default values. These customised values are set as default when creating new VPN groups.

The parameters are the same as above except for an additional **Root Certificates** tab allowing you to import root certificates for further usage.

### 15.2.2 Defining Global Settings for a VPN Group

The first step when creating a new VPN group is to configure global settings valid for every tunnel of this group.

After selecting **Add Group ...** from the **Details** section, the following parameters are available:

#### Note:

Take into consideration that these global settings are not "tacking" ones. Each one of the global parameters can be adapted to individual needs of tunnels within the VPN group.

### 15.2.2.1 TINA Tab

List 18-57 VPN GTI Editor - Group Edit - TINA tab - section General Settings

Parameter	Description
<b>Name</b>	This is a read-only field, displaying the group name as defined when creating the VPN group.
<b>Transport</b>	<p>This setting defines the to-be-used transport protocol and offers the following options:</p> <ul style="list-style-type: none"> <li>➤ <b>UDP</b> Tunnel uses UDP port 691 to communicate. This connection type is best suited for response optimised tunnels.</li> <li>➤ <b>TCP</b> Tunnel uses TCP connection on port 691 or 443 (for HTTP proxies). This mode is required for connection over SOCKS4 or HTTP proxies.</li> <li>➤ <b>UDP&amp;TCP</b> Tunnel uses TCP AND UDP connections. The tunnel engine uses the TCP connection for UDP requests and the UDP connection for TCP requests and ICMP-based applications.</li> <li>➤ <b>ESP</b> Tunnel uses ESP (IP protocol 50) to communicate. This connection type is best suited for performance optimised tunnels.</li> </ul> <p><b>Note:</b> Do NOT use ESP if there are filtering or NAT interfaces in between.</p> <ul style="list-style-type: none"> <li>➤ <b>Routing</b> This transport type is only of interest in combination with Traffic Intelligence configuration (see 2.7.1.2 Traffic Intelligence (TI), page 223). Specifying routing as transport disables data payload encryption within the tunnel. This transport should only be used for uncritical bulk traffic. Transport type Routing activates parameter <b>Routing Next-Hop</b> in the tunnel configuration dialogue, where the next-hop address for routed data packets has to be specified.</li> </ul> <p><b>Note:</b> To enter a <b>Routing Next-Hop</b> address when the <b>Direction</b> is <b>Passive</b> follow these steps:</p> <ul style="list-style-type: none"> <li>➤ Select <b>Direction: Active</b></li> <li>➤ Select <b>Transport: Routing</b></li> <li>➤ Enter the <b>Routing Next-Hop</b> address</li> <li>➤ Select <b>Direction: Passive</b></li> </ul>
<b>Encryption</b>	<p>Encryption mode the tunnel wants to establish as the active part. phion tunnels work with various encryption algorithms. The initialising partner tries to establish the encrypted connection by offering ONE of the following methods.</p> <ul style="list-style-type: none"> <li>➤ <b>AES</b> Advanced Encryption Standard; default; capable of 128 / 256 bit key length</li> <li>➤ <b>3DES</b> Further developed DES encryption; three keys with each 56 bit length are used one after the other resulting in a key length of 168 bit.</li> <li>➤ <b>CAST</b> by Carlisle Adams and Stafford Tavares; algorithm similar to DES with a key length of 128 bit.</li> <li>➤ <b>Blowfish</b> works with a variable key length (up to 128 bit)</li> <li>➤ <b>DES</b> Digital Encryption Standard; since DES is only capable of a 56 bit key length, it cannot be considered as safe any longer.</li> </ul> <p><b>Attention:</b> Do NOT use DES with high risk data.</p>
<b>Authentication</b>	<p>Defines the to-be-used algorithm for authentication. Available methods are:</p> <ul style="list-style-type: none"> <li>➤ <b>MDS</b> Message Digest 5; hash length of 128 bit</li> <li>➤ <b>SHA</b> Secure Hash Algorithm; hash length of 160 bit</li> </ul>

List 18-57 VPN GTI Editor - Group Edit - TINA tab - section General Settings

Parameter	Description
<b>Root Certificate</b>	In the pull-down menu available root certificates are offered for selection (as defined in the GTI Editor Defaults, see above).
<b>Key Time Limit</b>	This parameter defines the period of time after which the re-keying process is started. Possible settings are <b>5, 10</b> (default), <b>30</b> and <b>60</b> minutes.
<b>Key Traffic Limit</b>	This parameter defines the amount of traffic after which the re-keying process is started. Possible settings are: <b>No Limit, 1 MB, 5 MB, 10 MB</b> (default), <b>50 MB</b>
<b>Tunnel Probing</b>	The probing parameter defines the interval of sent probes. If such a probe is not answered correctly, the parameter <b>Tunnel Timeout</b> (see below) is in charge. The available time settings (in seconds) for the probing parameter are: <b>silent</b> (no probes are sent; disables the parameter), <b>10 secs, 20 secs, 30 secs</b> (default) and <b>60 secs</b> .
<b>Tunnel Timeout</b>	If for some reason the enveloping connection breaks down the tunnel has to be re-initialised. This is extremely important for setups with redundant possibilities to build the enveloping connection. The timeout parameter defines the period of time after which the tunnel is terminated. The available settings (in seconds) for the timeout parameter are: <b>10 secs, 20 secs</b> (default), <b>30 secs</b> and <b>60 secs</b> <b>Note:</b> The choice of the ideal timeout parameter strongly depends on the availability and stability of the connection. phion recommends setting the timeout to <b>30 seconds for internet connections</b> and to <b>10 seconds for intranet</b> or connections over a dedicated line.
<b>Accept Identification Type</b>	Offers three types of identification: <b>Public Key</b> (default), <b>X509 Certificate (CA signed)</b> and <b>X509 Certificate (explicit)</b>
<b>Hide in netfence VPN World</b>	Select the checkbox and the tunnel will not be visible in the VPN world software.
<b>Meshed</b>	Selecting this checkbox (at the bottom of the configuration window) automatically creates tunnels when adding a new VPN service to the group. <b>Note:</b> Take into consideration that the tunnels are NOT removed after deselecting this checkbox.

List 18-58 VPN GTI Editor - Group Edit - TINA tab - section Accepted Ciphers

Parameter	Description
<b>Accepted Ciphers</b>	Indicates what kind of ciphers are allowed for connecting to the VPN server for users of this group. <b>Reset</b> functionality is available as soon as a cipher setting was modified and restores default values.

List 18-59 VPN GTI Editor - Group Edit - TINA tab - section Bandwidth Protection

Parameter	Description
	Bandwidth Protection settings are a part of Traffic Intelligence configuration. For a description of Traffic Intelligence please see <b>VPN - 2.7.1.2 Traffic Intelligence (TI)</b> , page 223. For a detailed parameter description please see <b>VPN - Bandwidth Protection</b> , page 225.

List 18-60 VPN GTI Editor - Group Edit - TINA tab - section VPN Envelope Policy

Parameter	Description
	VPN Envelope settings are a part of Traffic Intelligence configuration. For a description of Traffic Intelligence please see <b>VPN - 2.7.1.2 Traffic Intelligence (TI)</b> , page 223. For a detailed parameter description please see <b>VPN - VPN Envelope Policy</b> , page 226.

### 15.2.2.2 IPsec Tab

This tab is used for defining parameters concerning both, Phase 1 and Phase 2, of an IPsec connection:

- **Phase 1** involves policy negotiation, key material exchange, and authentication.
- **Phase 2** involves policy negotiation, session key material refresh or exchange, and establishment.

List 18-61 VPN GTI Editor - Group Edit - IPsec tab - section Phase 1 / Phase2

Parameter	Description
<b>Encryption</b>	defines what kind of description is used Available algorithms for <b>Phase 1</b> : <b>3DES</b> (default), <b>DES</b> and <b>CAST</b> . Available algorithms for <b>Phase 2</b> are: <b>AES</b> , <b>3DES</b> (default), <b>CAST</b> , <b>Blowfish</b> and <b>DES</b> .
<b>Hash Meth.</b>	defines the used hash algorithm; available algorithms are <b>MD5</b> (default for both phases) and <b>SHA</b> .
<b>DH-Group</b>	Diffie-Hellman Group defines the way of key exchange; available options for this parameter are <b>Group1</b> (default for both phases; 768-bit modulus), <b>Group2</b> (1024-bit modulus), and <b>Group5</b> (1536-bit modulus).
<b>Lifetime</b>	defines rekeying time in seconds a server offers to the partner (default Phase 1: <b>28800</b> , default Phase 2: <b>3600</b> ).
<b>Min. Lifetime</b>	defines minimum rekeying time in seconds a server accepts from its partner (default Phase 1: <b>25200</b> , default Phase 2: <b>1200</b> ).
<b>Max. Lifetime</b>	defines maximum rekeying time in seconds a server accepts from its partner (default Phase 1: <b>32400</b> , default Phase 2: <b>4800</b> ).

List 18-62 VPN GTI Editor - Group Edit - IPsec tab - section General Settings

Parameter	Description
<b>Accepted Identification Type</b>	offers three types of identification: <b>Shared Passphrase</b> (default), <b>X509 Certificate (CA signed)</b> and <b>X509 Certificate (explicit)</b> . A passphrase is automatically generated when an IPsec tunnel is drawn.
<b>Root Certificate</b>	offers all available root certificates for selection (as defined in the GTI Editor Defaults, see above)

### 15.2.2.3 Defining VPN Service Properties

Fig. 18-14 Adding a VPN Service to a VPN Group - Step 1

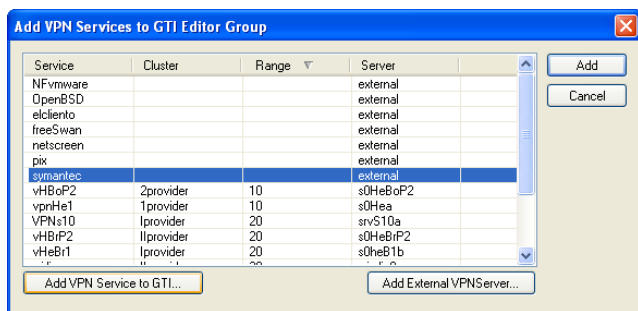
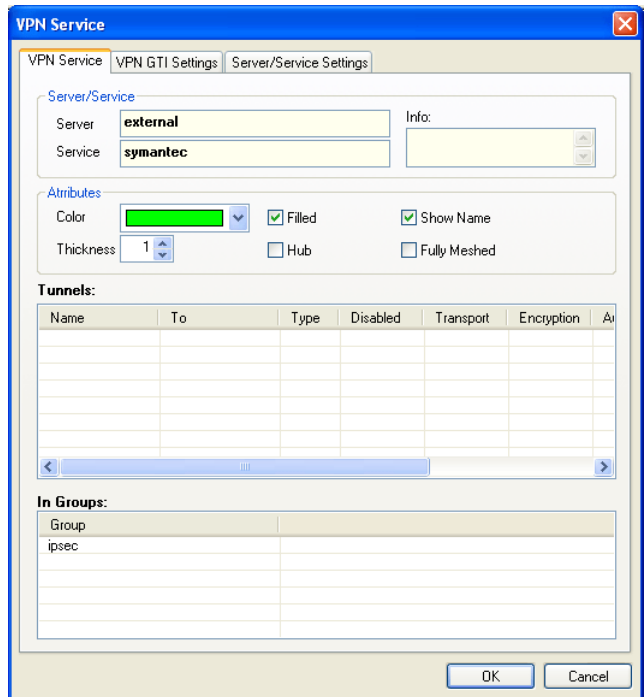


Fig. 18-15 Adding a VPN Service to a VPN Group - Step 2



When adding a VPN service to the VPN group, you may define several specific parameters.

List 18-63 VPN GTI Editor - Adding a VPN Service to a VPN Group - section Server/Service

Parameter	Description
<b>Server</b>	displays server name; read-only
<b>Service</b>	displays service name; read-only
<b>Info</b>	displays an optional information text; read-only

List 18-64 VPN GTI Editor - Adding a VPN Service to a VPN Group - section Attributes

Parameter	Description
<b>Color</b>	defines the colour in which the tunnels created from this VPN service to another one are displayed. Take into consideration that disabled tunnels are not affected by this parameter and are displayed grey regardless of the colour set. Additionally, the colour is used in conjunction with parameter <b>Filled</b> (see below) (default: black).
<b>Thickness</b>	defines the thickness of displayed tunnels created from this VPN service to another one (default: 1 pt)
<b>Filled</b>	ticking causes the background of the selected VPN service is equipped with a solid circle in color defined above (default: disabled)
<b>Hub</b>	ticking causes the selected VPN service to serve as a hub (default: disabled)
<b>Show Name</b>	enables/disables display of the selected VPN service name (default: enabled)
<b>Fully Meshed</b>	ticking causes automatic tunnel creation for the selected VPN service (default: disabled)

List 18-65 VPN GTI Editor - Adding a VPN Service to a VPN Group - section Tunnels

Parameter	Description
	displays every tunnel connection created from this VPN service to another one (including the set parameter values); context menu offers items <b>Edit Tunnel ...</b> (see 15.1.2 User Interface - Canvas Section, page 465), <b>Delete Tunnel</b> (see 15.1.2 User Interface - Canvas Section, page 465) and standard context menu entries

List 18-66 VPN GTI Editor - Adding a VPN Service to a VPN Group - section In Groups

Parameter	Description
	purely informational and displays all groups the VPN service is part of

The tabs VPN GTI Settings and Server/Service Settings in the VNP Service window are read only areas. Their content is delivered through the VPN GTI Settings tab (**VPN - 2.4 Configuring VPN GTI Settings**, page 209) and the Server Configuration tabs (**Configuration Service - 3. Configuring a New Server**, page 94).

**Note:**

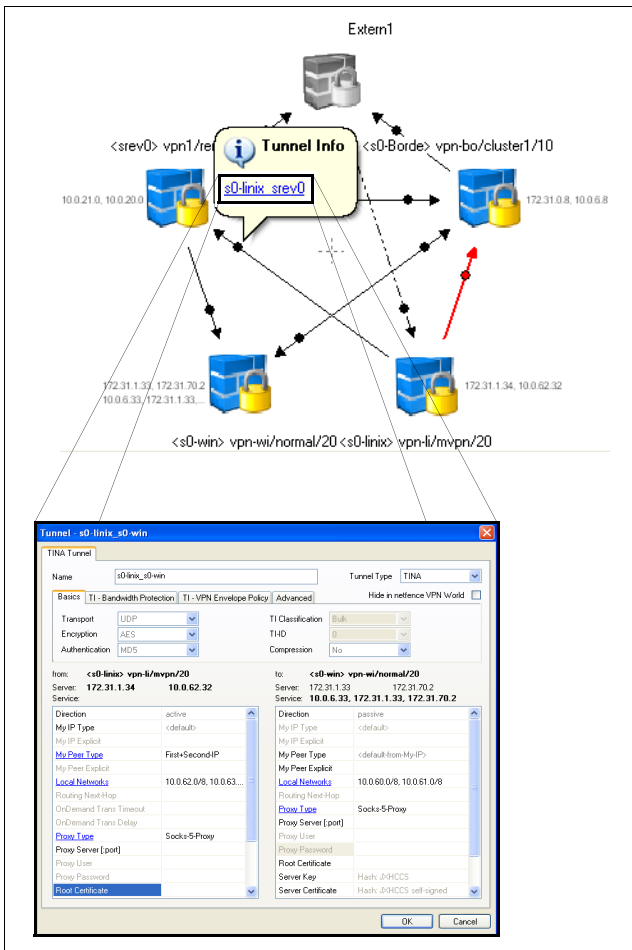
Networks, which should be reachable behind the tunnel's endpoints have to be entered into the **Networks** parameter of the Server Configuration area (see 3.3.2 GTI Networks, page 96).

**15.2.2.4 Defining Tunnel Properties**

As already mentioned above, netfence VPN GTI offers the possibility to tweak any tunnel parameter to your needs.

For tweaking tunnel parameters simply left-click the Tunnel Info node and open the configuration dialogue via the link (displayed in blue).

Fig. 18-16 Open Tunnel Info node and Tunnel configuration dialogue



The configuration dialogue provides every parameter relevant for the selected tunnel.

**Attention:**

Tweaking tunnel parameters disables global settings.

When editing a parameter the following visualisation effects are shown:

- Parameter name turns from black into blue and is displayed underlined (as shown in figure 18-16)
- Parameter value changes from grey (indicating default values) into black

**Note:**

In order to reset the modification, simply click on the blue, underlined parameter name and select **Reset to Group default value** from the menu.

**Note:**

The information displayed is merged of the following configuration entities:

- **Global VPN Settings** - see 15.2.2 Defining Global Settings for a VPN Group, page 466
- **Local VPN GTI Settings** on the corresponding boxes - see **VPN - 2.4 Configuring VPN GTI Settings**, page 209.

**15.2.2.5 Configuring Traffic Intelligence Settings in the GTI VPN Editor**

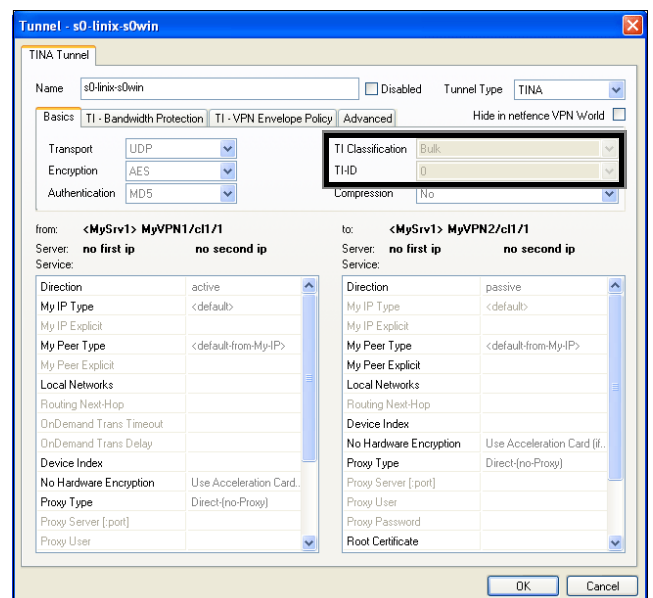
The GTI VPN Editor offers various configurations settings for Traffic Intelligence employment.

**Note:**

Functionality, characteristics and configuration parameters of Traffic Intelligence are described in detail in **VPN - 2.7.1.2 Traffic Intelligence (TI)**, page 223. **Please read this chapter before proceeding.** In this place, only transport creation and modification process will be described.

As described in 15.1.1 User Interface - Detail Section, page 465, a tunnel is created by drawing a line from the tunnel's start to its end point. A left click on the **Tunnel Info** node and click on the link with the tunnel name opens the tunnel configuration dialogue (figure 18-17).

Fig. 18-17 Tunnel configuration dialogue

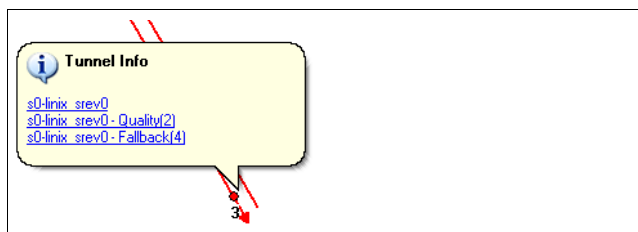


**TI-Classification** and **TI-ID** for the transport can be assigned through the lists in the framed area. The first transport is by default equipped with the attributes Bulk O. These values cannot be edited.

Drawing further lines between the same tunnel end points creates further transports. The configuration dialogues for these transports immediately open expecting specification of unique TI-Classification and TI-ID.

After having saved the settings, the **Tunnel Info** node displays links indicating the specific transports. Tunnels, which have been configured with multiple transports, are depicted by two parallel lines.

Fig. 18-18 Tunnel Info node displaying links to transports



Transport specific **TI Bandwidth Protection** (VPN - Bandwidth Protection, page 225) and **VPN Envelope settings** (VPN - 2.7.1.2 Traffic Intelligence (TI), page 223) are configured through accordingly named tabs in the tunnel configuration window.



## 16. netfence VPN world

### 16.1 General

netfence VPN world is a graphical real time monitoring utility for your VPN site to site connection tunnels.

Usage is only possible with GTI VPN tunnels as the management centre needs to determine a relationship between both tunnel endpoints. In case of traditionally configured VPN tunnels due to NAT-issues a relationship between the endpoints cannot be determined.

**Note:**

netfence VPN world is only available in combination with the MC-Global-player & MC-enterprise licenses.

### 16.2 MC Settings

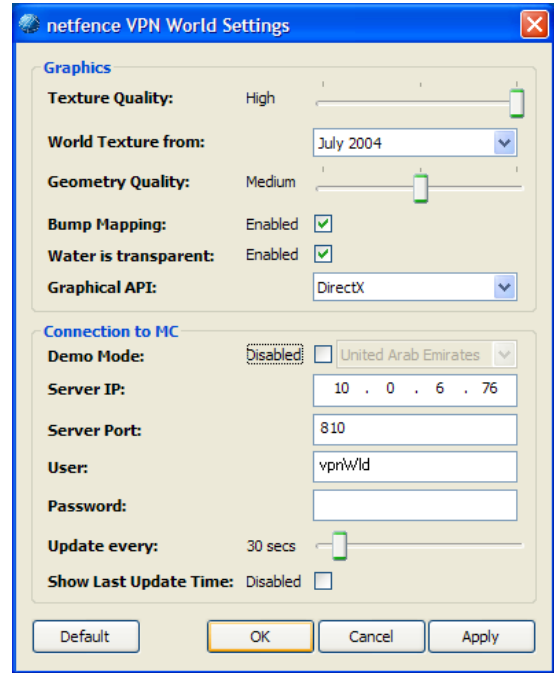
- In the MC set the parameter **Poll Box VPN Status** to **yes** (*Global Settings > MC Parameters > VPN World Setup*)  
(see **phion management centre** - 6.3.5 Global Settings - MC Parameters, page 413, list 18-10)
- To define the position of the VPN connectors, insert the coordinates in parameter **Global Position** for all your boxes (*Boxes > <boxname> > Box Properties > Operational > VPN World Settings*)  
(see **Configuration Service** - 2.2.2.2 Creating a Box - Operational Settings, page 53, list 3-3).

### 16.3 Requirements

- Processor: Intel Pentium IV, AMD Athlon 64 or better
- OS: Windows XP SP2 or Windows VISTA 32 / 64-bit
- Graphic card: DirectX 9 level graphics card or better
- Generic Network Adapter
- a MC and adequate licences (see 16.1 General, page 471)
- usage of GTI VPN tunnels

### 16.4 netfence VPN world Settings

Fig. 18-19 netfence VPN world settings



**Note:**

Please notice that for configuration settings, Administrative rights are required.

Define the settings best fitting to your video card, as the application is using DirectX 9. Check for the latest driver update at [www.microsoft.com](http://www.microsoft.com).

List 18-67 VPN world - section Graphics

Parameter	Description
<b>Texture Quality</b>	Move the slider to select the texture quality level. The higher the texture level the higher the CPU load. <ul style="list-style-type: none"> <li>➤ <b>Low</b> world.200407.2048x1024.tga (6.145 KB)</li> <li>➤ <b>Medium</b> world.200407.8100x4050.tga (96.109 KB)</li> <li>➤ <b>High</b> world.200407.10800x5400.tga (170.860 KB)</li> </ul>
<b>World Texture from</b>	Choose the world texture
<b>Geometry Quality</b>	Move the slider to select the geometry quality (number of polygons). This setting influences your performance substantially. Recommended value is <b>medium</b> . <ul style="list-style-type: none"> <li>➤ <b>High</b> 124.416 polygons</li> <li>➤ <b>Medium</b> 31.104 polygons</li> <li>➤ <b>Low</b> 7.776 polygons</li> </ul>
<b>Bump Mapping</b>	Choose <b>Enabled</b> or <b>Disabled</b> . This setting allows the video-card to apply texture maps (bumps) to flat textures, this setting can affect performance.
<b>Water is transparent</b>	Choose <b>Enabled</b> or <b>Disabled</b> . Select the way the water will be presented, this setting can affect performance.
<b>Graphical API</b>	Choose <b>DirectX</b> or <b>OpenGL</b> . If your system does not support DirectX you can choose OpenGL as an alternative. Please notice that as the application starts with DirectX selection by default, a check on DirectX driver version will be performed.

List 18-68 VPN world - section Connection to MC

Parameter	Description
<b>Demo Mode</b>	When no configuration is selected the application will start in demo mode, representing virtual tunnels. If selected, choose between different demo regions or customize your own demo tunnels.
<b>Server IP</b>	Insert the IP address to connect to the MC
<b>Server Port</b>	Insert the server port to connect to the MC
<b>User</b>	Insert username to connect to the MC
<b>Password</b>	Insert password to connect to the MC.  <b>Attention:</b> The password is encrypted and stored in the ini-file. Be aware that stored passwords even in encrypted form may be brute-force attacked.  <b>Note:</b> phion strongly recommend that those responsible for the netfence VPN world client ensure that the management workstation is operated in an environment which is free of malicious software (Trojan horses, ...). Additionally phion recommends to create a named administrator specifically for this purpose. The administrator should only be granted permissions for monitoring box states and tunnel status. For these permissions the admin requires the following roles on the management centre ( <b>Global Settings &gt; Administrative Roles &gt; Administrative Role Configuration &gt; Role</b> ): In section <b>MC Control Module</b> : ➤ <b>Access to MC Control</b> selected ➤ In section <b>MC Control Permissions</b> parameter <b>Show Map</b> enable (6.3.7 Global Settings - Administrative Roles, page 414)  <b>Note:</b> Please note that the rights from the selected user will be in place. So hierarchy rights on range/cluster/box have impact on the represented objects.
<b>Update every</b>	Scale updates from every 5 s to 300 s (5 minutes)
<b>Show Last Update Time</b>	Select the checkbox for an overlay stamp about last update time

## 16.5 User Interface

Fig. 18-20 VPN world



### 16.5.1 Hotkeys

Table 18-23 VPN world - Hotkey

Hotkey	Description
b	Bitmap bump map on/off
n	New 2D View. Open a new 2D window that can be moved on different desktop (especially for dual head graphics card)
s	Transparent sphere on/off
t	VPN Tunnel Mode on/off

Table 18-23 VPN world - Hotkey

Hotkey	Description
r	Sphere automatic rotation ON
<F5>	Refresh data
<ALT>	open <b>view</b> context menu, options are: ➤ <b>Box info</b> - open box info context ➤ <b>Missing GPS data</b> - a list of all boxes that have no GPS data defined ➤ <b>Boxes</b> - open list of active boxes, click on one and the world will move to this box position. Press <CTRL> and select a box from the list to open a new 2D window focused on the selected box. ➤ <b>Close</b> - Exit the application
<ALT>+<F4>	Exit the application

### 16.5.2 Mouse Functions

Table 18-24 VPN world - Mouse functions

Mouse Function	Description
Mouse Wheel	Zoom in/out
Right Mouse and Move	Move sphere
Left Mouse and Move	Rotate sphere
CTRL + Mouse click	Show Box / Tunnel Detail View, changing the value affects only demo mode. Get focus on the info window and press ESC to close it.
Click on box	If phiona is connected to the MC, a click on a box will open the configuration of the selected box.

### 16.5.3 Status / Colour Legend

Each tunnel / box is represented by a color depending on the status.

Table 18-25 VPN world - Colour legend for box

Box Status	Box Colour
Ready	blue
Warning	blinking green to red
Error	red

Table 18-26 VPN world - Colour legend for tunnel

Tunnel Status	Tunnel Colour
Active	green
Disabled	gray
Error	red
Multiple tunnel - not all are active	yellow

## 16.6 Troubleshooting

If the desired boxes and/or VPN tunnels are not displayed on VPN world, please follow the following steps.

### 16.6.1 MC and Box Configuration

- MC: The parameter **Poll Box VPN Status** must be set to **yes** (**Config > Multi-Range > Global Settings > MC Parameters > VPN World Setup**).
- Corresponding Box: The parameter **Poll VPN Tunnel Status** must be set to **yes** (**Config > Box > Box Properties > Operational > VPN World Settings**). In addition, the coordinates of the box must be typed into the **Global Position** parameter.

### 16.6.2 VPN Tunnel Configuration

- Ensure that the VPN tunnel is defined using the GTI editor.
- If the VPN tunnels are generated with the **Meshed** option enabled, the VPN tunnel will only be displayed when there is traffic. Double-click the group in the VPN GTI Editor to check the **Meshed** checkbox (VPN GTI Editor accessibility see 15.1 User Interface, page 464).
- Ensure that the checkbox **Hide in netfence VPN World** is not selected within the same dialogue.
- Double-click the tunnel in the VPN GTI Editor and ensure that the checkbox **Hide in netfence VPN World** is not selected within the VPN tunnel settings.

For further information about how to achieve the Group Edit dialogue and/or VPN tunnel settings see 15.1 User Interface, page 464.

### 16.6.3 netfence VPN world Configuration

- Under Windows > start > All Programs > phion ag > netfence vpn world > 3D Settings ensure that the MC server IP (not MC box IP) is typed into the Server IP parameter.

## 17. MC RCS

The phion management centre provides a **Revision Control System (RCS)** for auditing purpose. The RCS, as soon as activated, provides complete information on changes in the configuration of the phion management centre and its administered netfence gateways (in theory, back to the moment RCS was activated - depending on the amount of data).

**Attention:**

Please take into consideration that the DNS service is not supported by RCS.

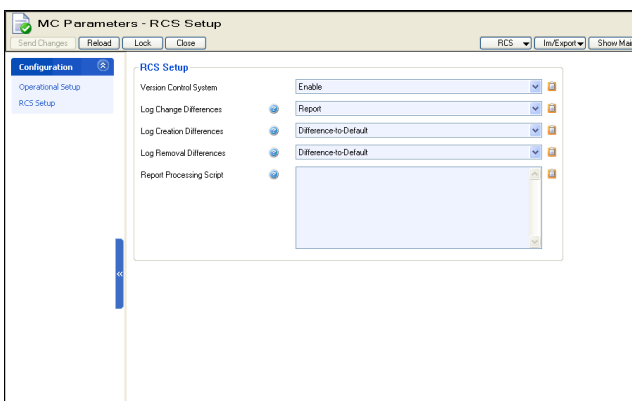
### 17.1 Activating / Configuring RCS

**Attention:**

For activating RCS an explicit license is required. Otherwise, a fatal log entry is created.

In order to activate RCS enter **Config > Multi-Range > Global Settings > MC Parameters > RCS Setup** view.

Fig. 18-21 Configuration dialogue - RCS



**Note:**

Modifying the settings of these parameters (and restoring a fresh installed MC with a par file) requires a restart of module **rangeconf** in order to get active. Depending on the size of the configuration tree, this restart may last several minutes because each configuration tree entry gets its version numbering. phion recommends to look at the log providing exact status information.

Additionally, it is necessary to make a session disconnect and reconnect, which enables the **RCS** pull-down menu in the above upper right corner as well as the context menu entries for RCS in the User Interface.

List 18-69 MC Parameters - RCS Setup

Parameter	Description
<b>Version Control System</b>	This parameter activates/deactivates the RCS function.
<b>Log Change Differences</b>	This parameter activates/deactivates the RCS functionality to log all changes made to a configuration node (file name: <code>servicename_changes</code> ).
<b>Log Creation Differences</b>	This parameter specifies how to log the change of a new configuration node. The following settings are available: <ul style="list-style-type: none"> <li>➤ <b>Difference-to-Default</b> - Only differences to the default settings are enlisted.</li> <li>➤ <b>Full-Info</b> - Every setting is enlisted.</li> <li>➤ <b>None</b> - Only changes are taken into account.</li> </ul>
<b>Log Removal Differences</b>	This parameter specifies how to log file removals within a configuration node. The following settings are available: <ul style="list-style-type: none"> <li>➤ <b>Difference-to-Default</b> - Only differences to the default settings are enlisted.</li> <li>➤ <b>Full-Info</b> - Every action is enlisted.</li> <li>➤ <b>None</b> - Removal of files is skipped.</li> </ul>

List 18-69 MC Parameters - RCS Setup

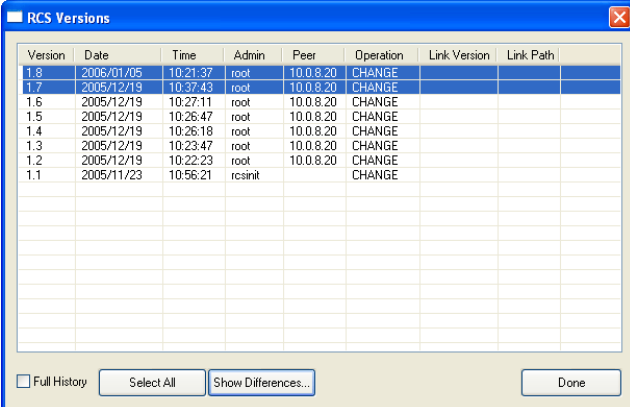
Parameter	Description
<b>Report Processing Script</b>	<p>Use this field to configure automated transmission of change reports to other destinations. A shell script invoking Secure Copy (<code>scp</code>) or e-mail delivery can be entered here.</p> <p>Example scripts for report transmission might look as follows:</p> <ul style="list-style-type: none"> <li>➤ <b>Secure copy to an external server</b>  <code>scp "\$REPORT" root@recipient.com</code></li> <li>➤ <b>mailclt to an external server</b>  <code>/opt/phion/bin/mailclt -f sender@sender.com recipient@recipient.com -s "change" -m 192.168.0.1 -a "\$REPORT"</code></li> </ul> <p><b>Attention:</b>            Make sure to use the variable <code>\$REPORT</code> when using the tools <code>scp</code> and <code>mailclt</code>. The name of the report file is stored in <code>\$REPORT</code> and is thus handed over by <code>Rangeconf</code>.</p> <p><b>Note:</b>            On netfence 4.2 <code>mailclt</code> is installed by default.</p> <p><b>Attention:</b>            The option <code>-m</code> expects the IP address of a reachable SMTP server to follow. As DNS resolution is not supported by RCS the mail server's IP address and not its MX-Record has to be specified at any rate.</p>

## 17.2 Using RCS

### 17.2.1 RCS Versions Dialogue

RCS is monitored in the **RCS Versions** window. This window may be opened either via the context menu of any item in the configuration tree below **Global Settings** or via the pull-down menu **RCS** within an explicit configuration file.

Fig. 18-22 RCS Versions window



Version	Date	Time	Admin	Peer	Operation	Link Version	Link Path
1.8	2006/01/05	10:21:37	root	10.0.8.20	CHANGE		
1.7	2005/12/19	10:27:43	root	10.0.8.20	CHANGE		
1.6	2005/12/19	10:27:11	root	10.0.8.20	CHANGE		
1.5	2005/12/19	10:26:47	root	10.0.8.20	CHANGE		
1.4	2005/12/19	10:26:18	root	10.0.8.20	CHANGE		
1.3	2005/12/19	10:23:47	root	10.0.8.20	CHANGE		
1.2	2005/12/19	10:22:23	root	10.0.8.20	CHANGE		
1.1	2005/11/23	10:56:21	rcsinit		CHANGE		

The RCS Versions window makes the the following information available:

Table 18-27 Columns available in the RCS Versions window

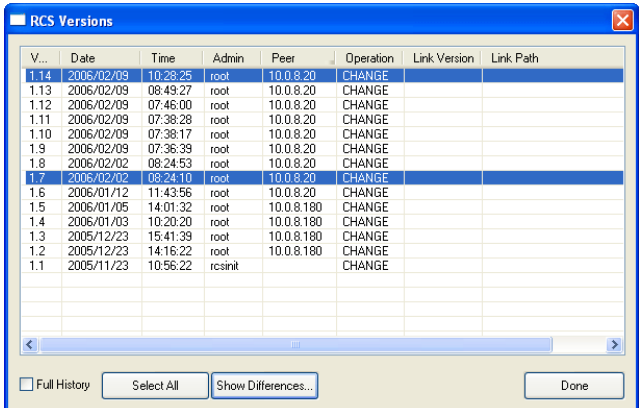
Column	Description
<b>Version</b>	This column displays the version numbers of the selected activated configuration node/file. As long as the configuration is only sent (by clicking <b>Send Changes</b> ) the displayed version is <b>session</b> . If this configuration is activated (by clicking <b>Activate</b> ) the corresponding (increased) version number is listed. Editing a linked file results in additional version information including the file version and the complete path of this link target.
<b>Date</b>	This is the date when a new or modified configuration has been activated. Data is arranged as follows: <code>yyyy/mm/dd</code> .
<b>Time</b>	This is the time when a new or modified configuration has been activated. Independent of box time settings, the effective time format is always UTC.
<b>Admin</b>	Displays the login name of the editing administrator.
<b>Peer</b>	Displays the peer address of the editing administrator.
<b>Operation</b>	Displays the peer address of the editing administrator. The following entries are possible: <ul style="list-style-type: none"> <li>➤ <b>CHANGE</b> - Indicates a modification</li> <li>➤ <b>ADD</b> - Indicates an added configuration entry (for example a newly introduced firewall rule)</li> <li>➤ <b>REMOVE</b> - Indicates a removed configuration entry (for example removing a firewall rule)</li> <li>➤ <b>LINK</b> - Indicates a link to a repository entry.</li> <li>➤ <b>UNLINK</b> - Indicates that a link to a repository entry was removed.</li> </ul>
<b>Link Version</b>	This column holds information only in conjunction with a LINK operation entry. This information consists of the version of the link target.
<b>Link Path</b>	This column holds information only in conjunction with a LINK operation entry and consists of the complete path of the link target.

#### 17.2.1.1 Working with RCS Versions Window

Selection of versions for verification is done by using the left mouse button (that means combining SHIFT and left-click will not work):

- first click sets the start version of interest
- second click sets the end version of interest

Fig. 18-23 Example for selecting versions of interest

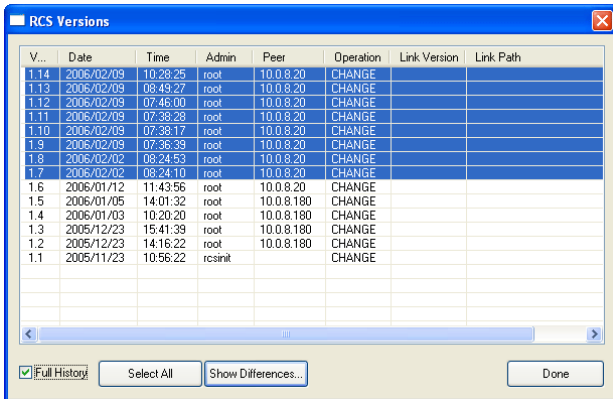


V...	Date	Time	Admin	Peer	Operation	Link Version	Link Path
1.14	2006/02/09	10:26:25	root	10.0.8.20	CHANGE		
1.13	2006/02/09	08:43:27	root	10.0.8.20	CHANGE		
1.12	2006/02/09	07:46:00	root	10.0.8.20	CHANGE		
1.11	2006/02/09	07:38:28	root	10.0.8.20	CHANGE		
1.10	2006/02/09	07:38:17	root	10.0.8.20	CHANGE		
1.9	2006/02/09	07:36:39	root	10.0.8.20	CHANGE		
1.8	2006/02/02	08:24:53	root	10.0.8.20	CHANGE		
1.7	2006/02/02	08:24:10	root	10.0.8.20	CHANGE		
1.6	2006/01/12	11:43:56	root	10.0.8.20	CHANGE		
1.5	2006/01/05	14:01:32	root	10.0.8.180	CHANGE		
1.4	2006/01/03	10:20:20	root	10.0.8.180	CHANGE		
1.3	2005/12/23	15:41:39	root	10.0.8.180	CHANGE		
1.2	2005/12/23	14:16:22	root	10.0.8.180	CHANGE		
1.1	2005/11/23	10:56:22	rcsinit		CHANGE		

The example shown in figure 18-23 would result in a comparison of version 1.1 and linked version 1.3. Ticking checkbox **Full History** (lower left corner) causes that every version step in between the selected version

gap is also taken into consideration for displaying differences (see figure 18-24).

**Fig. 18-24** Example for selecting versions of interest with selected Full History checkbox

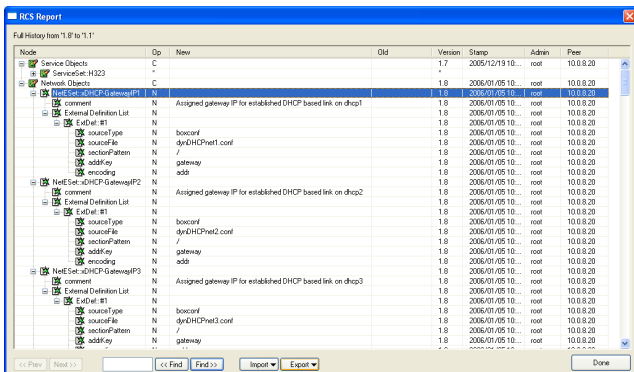


By clicking **Select All** all available versions are taken into account.

After the wanted selection is done click button **Show Differences ...** in order to open the **RCS Report**.

### 17.2.2 RCS Report Window

**Fig. 18-25** RCS Report window



This RCS Report window enlists every configuration change made according to the selected version files. It makes the the following information available:

**Table 18-28** Columns available in the RCS Report window

Column	Description
<b>Node</b>	This column offers a tree view on the changes. In the example above, the first level specifies the name of the configuration entity, the second level provides the name of the data set, the third level holds the position in the configuration dialogue, and the fourth level holds the object of editing.
<b>Operation</b>	This is the modification type. The following types are available: <ul style="list-style-type: none"> <li>➤ <b>New</b></li> <li>➤ <b>Change</b></li> <li>➤ <b>Remove</b></li> <li>➤ <b>Move</b> - this type indicates that the position of the configuration entry was moved in the hierarchy (for example moving a rule up or down in a rule set)</li> <li>➤ <b>*</b> - this type indicates multiple changes to the configuration entry</li> </ul>
<b>New</b>	This column shows the new value of the configuration entity.

**Table 18-28** Columns available in the RCS Report window

Column	Description
<b>Old</b>	This column shows the old value of the configuration entity. <p><b>Note:</b> Columns <b>New</b> and <b>Old</b> may consist of multiple lines. For viewing the complete information, open the node in the <b>Node</b> column or simply select <b>Details ...</b> from the context menu (see below).</p>
<b>Version</b>	Here the version number when editing is displayed. A * displayed indicates that there are multiple version number within this node.
<b>Stamp</b>	This is the time stamp indicating when a configuration has been modified. Independent of box time settings, the effective time format is always UTC. Date and time are arranged as follows: <i>yyyy/mm/dd hh:mm:ss</i> .
<b>Admin</b>	This is the administrator who has edited the configuration.
<b>Peer</b>	This is the IP address that is assigned to the administrator who has edited the configuration.

#### 17.2.2.1 Context Menu

The following entries are available:

- **Details ...**  
This entry opens the dialogue **RCS Report Detail** that fills the information in an easier to read view (recommended for multi-line entries).
- **Expand (All)**  
The entries **Expand** and **Expand All** cause that either the currently selected node or all nodes are expanded.
- **Collapse (All)**  
The entries **Collapse** and **Collapse All** cause that either the currently selected node or all nodes are collapsed.
- **Print (Visible Only, Landscape/Portrait)**  
Selecting the print-visible option prints the display as is on the printer. **Landscape** and **Portrait** allow selecting the paper orientation. Landscape is recommended, though.
- **Print (All, Landscape/Portrait)**  
Selecting the print-all option prints the expanded nodes (regardless whether they are currently expanded or not). **Landscape** and **Portrait** allow selecting the paper orientation. Landscape is recommended, though.

#### 17.2.2.2 Working with the RCS Report

The "tool" bar in the lower part of the dialogue offers the following functionalities:

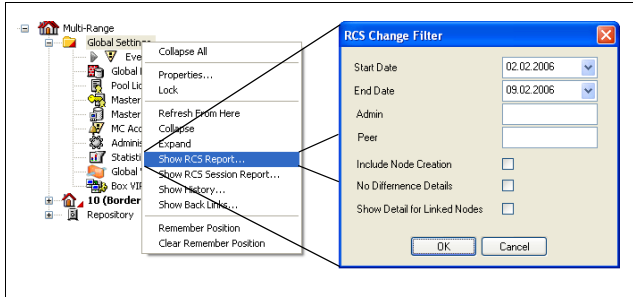
- **<< Prev / Next >>**  
These buttons allow jumping back/forward in version hierarchy using the defined version step (that means selecting 3 versions causes that the jump back/forward is also 3 versions, if possible).
- **Search string**  
Here you may define string you want to search for. Wildcards are not supported, though.
- **<< Find / Find >>**  
These buttons allow jumping back/forward in the search results.
- **Import ... / Export ...**  
Via these buttons you may export the RCS results to a prp file (**Phion RePort**) for archiving purpose or import an archived prp file.



### 17.2.3 Creating Specific RCS Reports

The RCS function also allows generating RCS Reports of certain time periods and/or administrators/peer IP addresses. Therefore select a configuration tree node, open the context menu and select **Show RCS Report ...**

Fig. 18-26 RCS Change Filter



List 18-70 RCS Change Filter settings

Parameter	Description
<b>Start Date / End Date</b>	Defines the period of time that is to be displayed.
<b>Admin</b>	Here you may enter the login name of a specific administrator (optional).
<b>Peer</b>	Here you may enter an explicit IP address (optional).
<b>Include Node Creation</b> checkbox	Ticking this checkbox collects the complete available version information. <b>Attention:</b> When using this option, be aware of the possible high amount of information.
<b>No Difference Details</b> checkbox	Ticking this checkbox collects only information about whether something has changed and NOT what was changed.
<b>Show Detail for Linked Nodes</b> checkbox	Ticking this checkbox collects the complete available change information and, additionally, takes the changes of the link target into account. <b>Attention:</b> When using this option, be aware of the possible high amount of information.

## 17.3 Retrieve Versions

The **RCS** pull-down menu offers the option **Retrieve Version**. When retrieving a version the **Send Changes** button is inactive and the header displays the corresponding icon followed by the version number.

### Attention:

The version-retrieving function does not work for the VPN server.

In order to accept the retrieved version, open the RCS pull-down menu again and select **Accept Version**. Answering the safety query with **Yes** reactivates **Send Changes** and allows sending and activating the old version of the configuration settings.



## 18. MC Reporter

### 18.1 General

The **MC-Reporter** (*rsdstats*) service is an essential component for operability of **phion reporter**.

phion reporter acts as a central reporting server that automatically processes accounting and eventing data generated by netfence systems into customisable reports. It is a tool for monitoring network behaviour and usage trend analysis. phion reporter complements a phion management centre through on-demand or scheduled processing of statistics and event data into reports.

Interaction between MC and phion reporter is designed for the following workflow:

- netfence gateways generate eventing and statistics data and propagate this information to the MC administering them.
- The phion management centre collects statistics generated by its administered boxes and receives eventing data.
- The management centre forwards collected statistics and collected and self-raised eventing data to the phion reporter. The **MC-Reporter** (*rsdstats*) service is responsible for execution of this task.

Installation and configuration description of **MC-Reporter** (*rsdstats*) are part of the phion reporter documentation, which is available as a separate document. Please refer to the **netfence reporter Administration and User Guide** for details.



# SNMP

<b>1.</b>	<b>Overview</b>	
1.1	General .....	480
<b>2.</b>	<b>Configuration</b>	
2.1	Single Box .....	481
2.2	management centre .....	481

# 1. Overview

## 1.1 General

The **Simple Network Management Protocol** (SNMP) is part of the Internet Standard Management Framework standardised by the IETF. The basic model of network management divides network nodes into the following categories:

- **managed nodes:** network nodes (for example router, switches, firewalls, servers) providing information. A so-called SNMP agent runs on each managed node to gather and provide information.
- **management nodes:** are used to monitor and control managed nodes.

Due to changing requirements nowadays three versions of the SNMP protocol are standardised.

### Note:

phion netfence gateway only supports the most widespread versions 1 and 2c.

For details about SNMP please refer to the IETF website ([www.ietf.org](http://www.ietf.org) - section RFC)

In general, SNMP is used to access information from SNMP capable interfaces, set configurative values and to notify a management station in case of failures. The latter action is called "sending an SNMP trap" and could be performed by the netfence event daemon. Thus the configuration for sending SNMP traps is described in **Eventing - 2.1.3 Notification Tab**, page 308.

SNMP over TCP/IP uses the (unreliable) UDP protocol. SNMP queries are sent on UDP port 161 while SNMP traps use UDP port 162.

In many cases the monitoring of larger network environments is performed by special network management tools (for example Tivoli NetView™ or HP OpenView™). To integrate a netfence gateway into these monitored environments, phion delivers a configurable SNMP agent (in the following called snmpd or SNMP service). Since SNMP security using SNMPv1 or SNMPv2 is generally considered low, the netfence SNMP service only allows querying of a minimum set of information.

Management information is viewed as a collection of managed objects, residing in a virtual information store, called the **Management Information Base** (MIB). Collections of related objects are defined in MIB modules.

The netfence SNMP service provides the following MIB modules:

- **system information** (for example configurable description, configurable contact information, configurable location, box name)
- **interface information** (for example available interfaces, interface media type, MAC addresses, interface statistics, IP addresses)
- **address translation table**, which permits mappings from network addresses (for example IP addresses) to physical addresses (for example MAC addresses)
- **IP information** (for example IP addresses and netmasks, routing table)

### Note:

For an overview of MIBs implemented in phion netfence, refer to the file `/usr/local/share/snmp/mibs/PHION-SNMP-MIB.txt` that is available on every netfence system.

Since netfence gateways implement their own extended configuration management, it is prohibited to set system values using SNMP.

Both SNMPv1 and SNMPv2c define a community-based administrative framework allowing implementation of basic access restrictions. The community-based administrative framework allows restrictions to MIB modules where the community name acts as a form of "password".

Note that the SNMP protocol does not specify encryption and all data transferred is thus sent unencrypted. phion recommends to restrict the usage of the SNMP service to trusted environments (for example within the corporate network). If the SNMP service is activated on perimeter firewalls phion strongly recommends to block external traffic to the SNMP service by introducing a blocking rule in the local firewall rule set (UDP port 161).

References:

- RFC 3410 - Introduction and Applicability Statements for Internet-Standard Management Framework
- RFC 1157 - Simple Network Management Protocol - [SNMPv1]
- RFC 1901 - Introduction to Community-based SNMP - [SNMPv2c]/
- RFC 1156 - Management Information Base for Network Management of TCP/IP based internets

## 2. Configuration

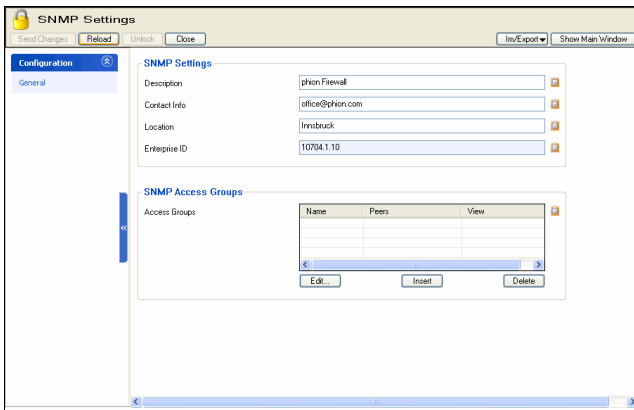
### 2.1 Single Box

Configuring SNMP on a netfence gateway starts with introducing a corresponding SNMP service. For installing simply follow the instructions mentioned in **Configuration Service - 4. Introducing a New Service**, page 97, and select **SNMPd** as **Software Module**.

After the service has been created, the following two configuration entries are available in the configuration tree:

- **Service Properties** - settings made during the introduction of the service
- **SNMP Settings** - described in the following

Fig. 19-1 SNMP service configuration dialogue



The three entries on the top of the dialogue, **Description**, **Contact Info** and **Location** are used to specify administrative information which can be queried in the systems information MIB module.

The field **Enterprise ID** contains the registered enterprise ID of phion AG (as assigned by IANA - [www.iana.org](http://www.iana.org)) and is therefore read-only. It is used to identify the vendor of the SNMP agent and to enable the vendors to define their own private enterprise objects.

The section **SNMP Access Groups** allows defining (simple) access restrictions. By default access to the SNMP service is not granted. To allow SNMP queries, a new access group has to be defined. The following parameters are available:

List 19-1 SNMP Configuration - section Access Groups

Parameter	Description
<b>Peers</b>	<p>Here the defined peers for the current access group are enlisted. To add a new peer click <b>Insert ...</b>. Each peer is defined by an identifier (Name) and consists of an IP Address/Mask and a Community.</p> <ul style="list-style-type: none"> <li>➤ <b>IP Address/Mask</b> defines which hosts/networks are granted to query the SNMP service.</li> <li>➤ <b>Community</b> defines the community name (acts as a sort of password) to identify membership of a community.</li> </ul>
<b>View</b>	<p>allows restriction to specific MIB modules. Available entries are:</p> <ul style="list-style-type: none"> <li>➤ <b>*-ALL*</b> allows access to all available MIB modules as described above</li> <li>➤ <b>*system*</b> restricts access to the MIB module "system"</li> <li>➤ <b>*interfaces*</b> restricts access to the MIB module "interfaces"</li> <li>➤ <b>*at*</b> restricts access to the MIB module "address translation table"</li> <li>➤ <b>*ip*</b> restricts access to the MIB module "ip"</li> </ul>

**Note:**

There has to be a default Access Group. If not, the service will allow queries without restriction. With SNMP services created after installation/update of netfence 4.2 a default access group is being introduced prohibiting unintended query in case of default configuration.

The SNMP service of a netfence gateway is available at the configured server IPs.

**Note:**

Please take into consideration that the local firewall rule set may block access to the SNMP service. Thus, it might be necessary to insert a local inbound rule which allows access to UDP port 161. For details concerning the local firewall rule set, see **Firewall**, page 123.

## 2.2 management centre

The SNMP service is also available as a so-called **Cluster Service (phion management centre - 6.5 Cluster Configuration**, page 417). The introduction of the SNMP cluster service simplifies the configuration as the cluster service can be added to any of the servers within the current cluster.

The configuration of such a SNMPd cluster service, however, is the same as mentioned under 2.1 Single Box, page 481.





# OSPF and RIP

<b>1.</b>	<b>OSPF and RIP</b>	
1.1	Overview .....	484
1.1.1	OSPF Basics .....	484
1.1.2	RIP Basics .....	484
1.1.3	OSPF vs RIP .....	485
1.2	Installation .....	485
1.3	Configuration .....	485
1.3.1	Operational Setup .....	485
1.3.2	OSPF Preferences .....	485
1.3.3	OSPF Router Setup .....	486
1.3.4	OSPF Area Setup .....	487
1.3.5	RIP Router Setup .....	487
1.3.6	RIP Preferences .....	488
1.3.7	Network Interfaces .....	489
1.3.8	Neighbour Setup .....	489
1.3.9	Filter Setup .....	490
1.3.10	GUI as Text .....	491
1.3.11	Text Based Configuration .....	491
1.4	Routing Configuration .....	491
1.5	HA Operation .....	491
<b>2.</b>	<b>Example for OSPF and RIP Configuration</b>	
2.1	Network Setup .....	492
2.2	Configuration Steps .....	492
2.2.1	OSPF Basic Setup .....	492
2.2.2	Redistribution of Connected Networks to OSPF .....	494
2.2.3	Injecting the Default Route to OSPF .....	494
2.2.4	OSPF Multipath Routing .....	495
2.2.5	OSPF Link Authentication .....	495
2.2.6	OSPF Route Summarisation .....	495
2.2.7	RIP Basic Setup .....	496
2.2.8	Redistribution between RIP and OSPF .....	496

# 1. OSPF and RIP

## 1.1 Overview

Currently netfence supports the dynamic routing protocols **Open Shortest Path First** (OSPF) and **Routing Information Protocol** (RIP Version 1 and RIP Version 2). Both protocols are **Interior Gateway Protocols** (IGP) and distribute routing information within an autonomous system. Firewalls sometimes need to use a dynamic routing protocol when they segment large networks where multiple paths are possible and static routing is not practicable.

Since not all systems support OSPF, there is still need for RIP which is implemented in most of the common operating systems and small routers.

OSPF is defined in RFC 2328, the standard for RIPv2 is documented in RFC 2453.

A short description of both protocols is provided below.

### 1.1.1 OSPF Basics

OSPF is a link state protocol and uses Dijkstra algorithm to calculate the shortest path tree. A router's interface is the "link". The "state" of this interface is summed up by its IP address, subnet mask, interface type, neighbour state ... Every router keeps track of all connected interfaces and states and sends this information with Multicasts to its neighbours. These packets are known as LSAs (**Link State Advertisements**).

The router builds its Link State Database with the information provided by the LSAs. Every time a network change occurs, LSAs containing the new information are sent thus triggering every router to update its database. After having received all LSAs, the router calculates the loop-free topology. LSAs cannot be filtered within an area because all routers in an area must have the same Link State database. If some information is missing, routing loops can occur.

OSPF is a hierarchical IGP - it uses **Areas** to achieve this. The top-level Area is known as Backbone Area and the number of this Area always has to be **0** or **0.0.0.0** - this is **a must**. All other Areas must be physically connected to this Backbone Area. A very important thing within OSPF is that Areas must not be split. (If this cannot be avoided, a virtual link has to be used to expand Area 0 over any other area.)

Routers within an area are known as Area Routers. Routers connected to two or more areas are known as **Area Border Routers** (ABR) and routers connected to other Autonomous systems are called **Autonomous System Boundary Routers** (ASBR). Routing information may be summarised on ABRs and ASBRs, it is not possible to summarise routing information within an area.

The metric used by OSPF is **cost**. Every link has an associated cost value, derived from the link bandwidth. The metric to a destination is calculated by adding up all costs. If there are more possible paths to a destination the route with the lowest cost is chosen as the best route.

To advertise LSAs, the router has to live in OSPF neighbourhood with other routers. When this neighbourhood is fully established, the interfaces begin sending the updates (LSAs). To build an adjacency, hello packets are continuously exchanged between neighbouring routers. This also keeps track of the existence of the connected OSPF neighbours.

To lower down the number of updates exchanged on a Broadcast Medium (for example Ethernet), LSAs are only sent to a so called **Designated Router** (DR). This interface advertises the information to all other routers on the shared medium. Without a DR, an any-to-any neighbourhood between all OSPF routers on this segment would be needed. For backup reasons, a **Backup DR** (BDR) is elected. Each other router establishes neighbourhood only with the DR and BDR.

Areas can be configured as stub areas, where external routes are not advertised by ABRs to the Area Routers. Instead, a default route is injected to the area. Area 0 cannot be stub.

#### Note:

OSPF is very CPU and memory intensive. Therefore, be careful when enabling OSPF on low-end interfaces in a large network.

### 1.1.2 RIP Basics

RIP is a distance-vector protocol. The expression "distance-vector" can be defined as follows: The vector is the direction to the destination (next hop); the distance is treated as a metric type. Example: Destination A is a distance of 3 hops away and the direction is via router AA.

RIP uses **Hop Count** as metric. A maximum of 15 hops are possible; metric 16 means that a network is unreachable.

All RIP routers periodically send routing updates. Every update includes the whole routing table. The following techniques have been introduced to prevent routing loops:

#### ➤ *Split Horizon*

When sending Updates out a particular interface, the routes learned from this interface are not included in the update

#### ➤ *Split Horizon with Poison reverse*

This method is an extension to Split Horizon. The router includes learned routes in the update but marks these routes as unreachable.

#### ➤ *Counting to infinity*

To recognise unreachable networks on link failures. Infinity in RIP is defined as 16 hops. Every time a routing update passes a router, the hop count is increased by 1. When the counter reaches 16, the network is considered unreachable.

RIPv1 is *classful*, which means that subnet information cannot be distributed. RIPv2, on the other hand, is *classless*, that means the subnet mask is included in the routing update.

### 1.1.3 OSPF vs RIP

The following table summarises the feature differences between OSPF and RIP.

**Table 20-1** Feature differences between OSPF and RIP

Attribute	OSPF	RIP
<b>Convergence</b>	Fast	Slow
<b>Network size</b>	For large and small networks	Only for small to medium networks due to the fact that max. metric is 15 hops
<b>Need of device resources</b>	Memory and CPU intensive	Much less memory and CPU intensive than OSPF
<b>Need of network resources</b>	Less than RIP; Only small Updates are sent	Bandwidth consuming; Whole Routing table is sent (default: every 90 seconds)
<b>Metric</b>	Is based on bandwidth	Is based on hop count, no matter how fast the connections are
<b>Design</b>	Hierarchical network possible	Flat network
<b>Troubleshooting</b>	More complex	Less complex

## 1.2 Installation

To configure either OSPF or RIP on a netfence system a new server service has to be introduced. Select **Config** from the box menu and introduce the service by choosing **Create Service** from the context menu of **Assigned Services**. Select **OSPFv2/RIP** as software module.

**Note:**

Please see **Configuration Service - 4. Introducing a New Service**, page 97, for detailed information concerning procedure and available options for service creation.

## 1.3 Configuration

To configure OSPF/RIP Settings browse to **OSPF/RIP Settings** (accessible through **Config** > **Box** > **Virtual Servers** > <servername> > **Assigned Services** > <servicename> (**ospf**) in the configuration tree.

### 1.3.1 Operational Setup

In this section, the general parameters of the dynamic routing protocols, like enabling/disabling the protocol and handling of dynamic routes are configured.

**Note:**

On a netfence gateway, route selection is directly dependant of the metric of a route; routes with a lower metric are preferred to routes with a higher metric. Static routes have a metric of **1** by default. RIP routes can have a maximum metric of **15** hops and OSPF routes will mostly have a cost of more than **20**.

As it is desirable that OSPF routes be preferred to RIP routes, metrics can be increased artificially through defining administrative distances. The corresponding parameter **Administrative Distance** for RIP (see Administrative Distance, page 488) is by default set to **120**. The congeneric parameter **Admin Distance** related to OSPF (see Admin Distance, page 486) is by default left empty. The value specified for the administrative distance is going to be added to every route learned through OSPF or RIP respectively.

**List 20-1** OSPF/RIP Settings - section Operational Setup

Parameter	Description
<b>Idle Mode</b>	If this parameter is set to <b>yes</b> , the OSPF/RIP wrapper gets started by the control daemon but does not start up the actual OSPF and RIP routing service.
<b>Run OSPF Router</b>	By setting this value the OSPF routing functionality can be enabled or disabled.
<b>Run RIP Router</b>	By setting this value the RIP routing functionality can be enabled or disabled.
<b>Hostname</b>	Allows overriding the propagated hostname, which by default is the box hostname.
<b>Operation Mode</b>	The operation mode defines handling of route learning and propagation. The following settings are possible: <ul style="list-style-type: none"> <li> <b>advertise-only</b> routes are only advertised</li> <li> <b>learn-only</b> networks are not propagated, except those networks living on the interfaces configured for OSPF or RIP themselves; learned routes from other systems are still advertised</li> <li> <b>advertise-learn</b> OSPF routes are learned and propagated</li> </ul>
<b>Router ID</b>	Every OSPF router is identified by its Router ID. This ID is defined by an IP address explicitly configured for this router. If the Router ID is not set, the system uses any IP address for it. For troubleshooting reasons, it is common to set this option manually.
<b>Router ID Mask</b>	Here the mask of the router is defined (default: 8-Bit).

### 1.3.2 OSPF Preferences

**List 20-2** OSPF/RIP Settings - OSPF Preferences - section OSPF Preferences Configuration

Parameter	Description
<b>Log Level</b>	Specifies the verbosity of the OSPF routing service. Available values are: <ul style="list-style-type: none"> <li> critical</li> <li> debugging</li> <li> emergencies</li> <li> errors</li> <li> informational (default)</li> <li> notifications</li> <li> warnings</li> <li> alerts</li> </ul>
<b>Use Special Routing Table</b>	By setting this parameter to <b>yes</b> and selecting a table name below, routes learned by the OSPF service are introduced into an own routing table. Note that the routing table is not automatically introduced but has to be configured manually by introducing <b>Policy Routes</b> .

List 20-2 OSPF/RIP Settings - OSPF Preferences - section OSPF Preferences Configuration

Parameter	Description
<b>Table Names</b>	A list of policy routing names can be specified here. Routes learned by the routing daemon are introduced into each of the enlisted routing tables.
<b>Multipath Handling</b>	<ul style="list-style-type: none"> <li>➤ <b>ignore</b> multipath routes will be discarded</li> </ul> <p><b>Attention:</b> OSPF summarises routes to multipath routes automatically if more than one next hop to a prefix exists. Use setting "ignore" with caution.</p> <ul style="list-style-type: none"> <li>➤ <b>assign-internal-preferences</b> multipath routes will be translated to several routes with different metrics (preferences)</li> <li>➤ <b>accept-on-same-device</b> multipath routes will be introduced as multipath if all nexthops are reachable on the same interface</li> <li>➤ <b>accept-all</b> (default) multipath routes will be introduced</li> </ul>

List 20-3 OSPF/RIP Settings - OSPF Preferences - section RIP SETTINGS

Parameter	Description
<b>Log Level</b>	Specifies the verbosity of the RIP routing service. Available values are: <ul style="list-style-type: none"> <li>➤ critical</li> <li>➤ debugging</li> <li>➤ emergencies</li> <li>➤ errors</li> <li>➤ informational (default)</li> <li>➤ notifications</li> <li>➤ warnings</li> <li>➤ alerts</li> </ul>
<b>Use Special Routing Tables</b>	By setting this parameter to <b>yes</b> and selecting a table name below, routes learned by the RIP service are introduced into an own routing table. Note that the routing table is not automatically introduced, but has to be configured manually by introducing Policy Routes.
<b>Table Names</b>	A list of policy routing names can be specified here. Routes learned by the routing daemon are introduced into each of the enlisted routing tables.
<b>Multipath Handling</b>	<ul style="list-style-type: none"> <li>➤ <b>ignore</b> multipath routes will be discarded</li> </ul> <p><b>Attention:</b> RIP summarises routes to multipath routes automatically if more than one next hop to a prefix exists. Use setting "ignore" with caution.</p> <ul style="list-style-type: none"> <li>➤ <b>assign-internal-preferences</b> multipath routes will be translated to several routes with different metrics (preferences)</li> <li>➤ <b>accept-on-same-device</b> multipath routes will be introduced as multipath if all nexthops are reachable on the same interface</li> <li>➤ <b>accept-all</b> (default) multipath routes will be introduced</li> </ul>

### 1.3.3 OSPF Router Setup

This tab only has to be configured when OSPF has been activated in the General tab through setting the **Run OSPF Router** parameter to **yes**.

The essential OSPF configuration, specification of global parameters and definition of networks used by OSPF to build neighbourhood and advertise routes, is done in this place.

For tuning interface or area specific parameters, please use the Network Interfaces, page 489 and the OSPF Area Setup, page 487 respectively.

List 20-4 OSPF/RIP Settings - OSPF Router Setup - section OSPF Router Configuration

Parameter	Description	
<b>ABR Type</b>	Defines Area Border Router (ABR) behaviour of the OSPF routing daemon. The following types are available for selection: <ul style="list-style-type: none"> <li>➤ Not an ABR</li> <li>➤ Cisco Type</li> <li>➤ IBM Type</li> <li>➤ Standard RFC 2328 Type</li> </ul>	
<b>Terminal Password</b>	Password to connect via telnet. OSPF router is reachable on TCP port 2604 (loopback only).	
<b>Privileged Terminal Password</b>	Password to enable configuration via telnet.	
<b>RFC1583 Compatibility</b>	Defines RFC 1583 compatibility behaviour.	
<b>Auto-Cost Ref Bwidth [MBit/s]</b>	The OSPF metric is calculated as reference bandwidth divided by bandwidth. The default setting is <b>10000</b> . <p><b>Attention:</b> This value is overwritten by explicit cost statements.</p> <p><b>Attention:</b> This setting should be used equally with all OSPF routers in an autonomous system. Otherwise, the metric calculation will be incorrect.</p>	
<b>Network Prefix</b>	Defines the interfaces on which OSPF runs and the networks which are propagated as OSPF Intra-Area or Inter-Area routes.	
<b>Advanced Settings</b>	<b>Support Opaque LSA</b>	Set to yes to enable Opaque LSA.
	<b>SPF Delay Timer</b>	Specifies the amount of time (sec) to wait before running an SPF after receiving a database change.
	<b>SPF Hold Timer</b>	Specifies the amount of time (sec) to wait between consecutive SPF runs.
	<b>Refresh Timer</b>	Valid values from 10 to 1800.
	<b>Default Metric</b>	Defines the default metric for the OSPF protocol. Use if other protocols are used for metric-translation, too.
<b>Admin Distance</b>	To determine which routing protocol to use if two protocols provide routing information for the same destination, the administrative distance is used as the first criterion. Higher distance values imply lower trust ratings. The admin distance setting is used to increase the metric of routes introduced to the system. For instance, an externally learned RIP route with metric 2 and Administrative Distance 100 is introduced with metric 102. This will effect that the OSPF route is favoured over the RIP route. <p><b>Note:</b> Remember that administrative distance is not advertised and thus only has local impact.</p>	

**List 20-5** OSPF/RIP Settings - OSPF Router Setup - section Router Distribution Configuration

Parameter	Description
<b>Default Route Distribution</b>	Click the <i>Edit ...</i> button to specify default route distribution settings:
<b>OSPF Metric</b>	Set the metric in the router's link state advertisement. The SPF algorithm uses this value to calculate the cost for each route. Routes with lower cost are preferred over routes with higher costs.
<b>OSPF External Metric</b>	Set external metrics type: ↗ <b>Type1</b> Type1 external routes have a cost that is the sum of the cost of this external route plus the cost to reach the ASBR. ↗ <b>Type2</b> The cost of Type2 external routes is defined alike the cost of Type1 routes but without the cost to reach the ASBR.
<b>Originate Always</b>	Enables the router to send the default route 0.0.0.0 to a neighbour. The neighbour can then use this route to reach the router if all other routes are not available.
<b>Route Maps</b>	Filter definitions. References OSPF/RIP Settings - Filter Setup - Route Map Filters - section Route Map Filters in 1.3.9 Filter Setup.
<b>Route Redistribution</b>	Click the <i>Insert ...</i> button to specify individual route redistribution settings:
<b>Route Types</b>	Available route type settings are: ↗ connected ↗ RIP
<b>OSPF Metric</b>	See OSPF Metric parameter description above.
<b>OSPF External Metric</b>	See OSPF External Metric parameter description above. If no external metric setting is needed, the value <b>NOT-SET</b> can be defined in this place.
<b>Route Maps</b>	Filter definitions. References OSPF/RIP Settings - Filter Setup - Route Map Filters - section Route Map Filters in 1.3.9 Filter Setup.

### 1.3.4 OSPF Area Setup

In this section, area specific parameters are set.

**List 20-6** OSPF/RIP Settings - section OSPF Area Configuration

Parameter	Description
<b>Enable Configuration</b>	Set to no to disable this area configuration.
<b>Area ID Format</b>	Defines which area format is used: ↗ Integer (default) ↗ Quad-IP
<b>Area ID [IP]</b>	Area ID as Quad-IP (for example 0.0.0.1)
<b>Area ID [Int]</b>	Area as number (for example 1)
<b>Authentication Type</b>	Defines authentication for the area (default: <b>Digest-MD5</b> )
<b>Simple Authentication Key</b>	Define here the OSPF area authentication credentials.
<b>Digest Authentication Key</b>	Define here the OSPF area authentication credentials.
<b>Special Type</b>	Stub areas do not import or originate external LSAs. NSSAs are the "OSPF Not-So-Stubby Area" where an ASBR can be located in a stub area (see RFC 3101) (default: <b>NONE</b> ).
<b>NSSA-ABR Translate Election</b>	This setting option is defined by RFC 3101.
<b>Disable Summary</b>	Disables summary LSAs.

**List 20-6** OSPF/RIP Settings - section OSPF Area Configuration

Parameter	Description
<b>Virtual Link ID (ABR)</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Sets the virtual link ID for this area.
<b>Virtual Link Params</b>	<b>Note:</b> This parameter is only available in <b>Advanced View</b> mode. Parameters for the virtual link. For a description see OSPF/RIP Settings - Network Interfaces Configuration - Parameter Template Configuration - section OSPF Parameters, 1.3.7.3 Section Parameter Template Configuration.
<b>Area Default Cost</b>	The area default cost is the cost for the default route injected into an attached stub area.
<b>Summary Range IP/Mask</b>	<b>Summary Range IP/Mask</b> Create summary ranges in the area to special actions on that range.  <b>Range Action</b> (default: <b>advertise</b> ): Special action for a range: ↗ advertise (default) ↗ non-advertise ↗ substitute  <b>Range Cost</b> Cost for a range.  <b>Advertised Range</b> Advertise configured range to.
<b>Area Export Filters</b>	Set an export ACL.
<b>Area Import Filters</b>	Set an import ACL.
<b>Area in Filters</b>	Set an import prefix list.
<b>Area out Filters</b>	Set an export prefix list.

### 1.3.5 RIP Router Setup

This tab only has to be configured when RIP has been activated in the General tab through setting the **Run RIP Router** parameter to **yes**.

Specification of global RIP settings such as version, timers and authentication, and definition of interfaces on which the RIP process shall run, is done in this place.

For interface specific tuning please use the Network Interfaces, page 489.

**List 20-7** OSPF/RIP Settings - RIP Router Setup - section RIP Router Configuration

Parameter	Description
<b>RIP Keychains</b>	<b>Key/Key String</b> To enable RIP authentication so-called key chains have to be introduced. A key chain can consist of several keys, where each key is identified by a number and a key string (password).
<b>RIP Version</b>	The netfence routing service allows usage of both standardised RIP versions RIPv1 or RIPv2. The following values are thus available for selection: ↗ <b>Version_1</b> (classful) ↗ <b>Version_2</b> (classless)
<b>RIP Terminal Password</b>	Password to connect via telnet and query status information of the RIP router. The RIP router is reachable on TCP port 2604 (loopback only). This is mainly useful for debugging purposes. Note that remote connection to the RIP terminal is not possible.
<b>Privileged RIP Terminal Password</b>	Password to connect via telnet and change configuration of the RIP router (not recommended since changes made via the terminal are not persistent). Note that remote connection to the RIP terminal is not possible.
<b>Networks</b>	<b>Network Prefix/Device</b> Defines the interfaces on which the RIP daemon runs.

List 20-7 OSPF/RIP Settings - RIP Router Setup - section RIP Router Configuration

Parameter	Description
<b>Advanced Settings</b>	<b>Update Timer</b> Specifies the time span (sec) between the unsolicited sending of response messages to all neighbours containing the routing table. Default: <b>30</b>
	<b>Timeout Timer</b> Specifies the validity timeout (sec) of a route. The route is retained in the routing tables but is no longer valid. Default: <b>180</b>
	<b>Garbage Collect Timer</b> Specifies the time span (sec) after which an invalid route is removed from the routing table. Default: <b>120</b>
	<b>Administrative Distance</b> To determine which routing protocol to use if two protocols provide routing information for the same destination, the administrative distance is used as the first criterion. Higher distance values imply lower trust ratings, RIP default is <b>120</b> . The administrative distance setting is used to increase the metric of routes introduced to the system. For instance, an externally learned RIP route with metric 2 and Administrative Distance 100 is introduced with metric 102. This will effect that the OSPF route is favoured over the RIP route. <b>Note:</b> Remember that administrative distance is not advertised and thus only has local impact.
	<b>Default Metric</b> Defines the default metric for redistributed routes. Does not apply to connected routes. Default: <b>1</b>
	<b>Interface Default</b> Default interface policy for RIP. Possible values are: ↗ <b>passive</b> network is only advertised; no RIP Hello packets are sent out from this interface ↗ <b>active</b> (default)

List 20-8 OSPF/RIP Settings - RIP Router Setup - section Router Distribution Configuration

Parameter	Description
<b>Default Route Redistribution</b>	Select checkbox to redistribute default routes. A list of routes which should be redistributed can be specified.
<b>Route Redistribution</b>	<b>Route Types</b> The route type can be either <b>connected</b> or <b>OSPF</b> . In the first case, netfence routes, which have the flag <b>Propagate via OSPF</b> set to <b>Yes</b> , are redistributed. In the latter case routes learned via OSPF are redistributed. Note that direct routes on an active interface are always redistributed.
	<b>RIP Metric</b> Sets the metric for the selected type of routes.
	<b>Route Maps</b> Filter definitions. References <b>Route maps</b> in <b>FILTER</b> tab.

List 20-8 OSPF/RIP Settings - RIP Router Setup - section Router Distribution Configuration

Parameter	Description								
<b>Route Update Filtering</b>	Route Update Filtering is used to provide Access Control Mechanisms and mechanisms to fine-tune RIP metrics.								
	<table border="1"> <thead> <tr> <th>Metric Offsets</th> <th>Update Direction</th> <th rowspan="4">Configuring Metric Offsets adds an offset to incoming and outgoing metrics to routes learned via RIP.</th> </tr> </thead> <tbody> <tr> <td></td> <th>Enforced Metric</th> </tr> <tr> <td></td> <th>ACLs</th> </tr> <tr> <td></td> <th>Devices</th> </tr> </tbody> </table>	Metric Offsets	Update Direction	Configuring Metric Offsets adds an offset to incoming and outgoing metrics to routes learned via RIP.		Enforced Metric		ACLs	
Metric Offsets	Update Direction	Configuring Metric Offsets adds an offset to incoming and outgoing metrics to routes learned via RIP.							
	Enforced Metric								
	ACLs								
	Devices								
<b>Route In/Out Filters</b>	<table border="1"> <thead> <tr> <th>Update Direction</th> <th rowspan="5">Route Filters are used to control the advertising and learning of routes in routing updates. Filters with the parameter Update Direction set to "in" apply to routes processed in incoming routing updates. The filter is matched against the content of the update, not against the source or destination of the routing update packets.</th> </tr> </thead> <tbody> <tr> <th>Object Type</th> </tr> <tr> <th>ACLs</th> </tr> <tr> <th>IP Prefix List</th> </tr> <tr> <th>Devices</th> </tr> </tbody> </table>	Update Direction	Route Filters are used to control the advertising and learning of routes in routing updates. Filters with the parameter Update Direction set to "in" apply to routes processed in incoming routing updates. The filter is matched against the content of the update, not against the source or destination of the routing update packets.	Object Type	ACLs	IP Prefix List	Devices		
	Update Direction	Route Filters are used to control the advertising and learning of routes in routing updates. Filters with the parameter Update Direction set to "in" apply to routes processed in incoming routing updates. The filter is matched against the content of the update, not against the source or destination of the routing update packets.							
	Object Type								
	ACLs								
	IP Prefix List								
Devices									

### 1.3.6 RIP Preferences

List 20-9 OSPF/RIP Settings - RIP Preferences - section RIP Preferences Configuration

Parameter	Description
<b>Log Level</b>	Specifies the verbosity of the RIP routing service. Available values are: ↗ critical ↗ debugging ↗ emergencies ↗ errors ↗ informational (default) ↗ notifications ↗ warnings ↗ alerts
<b>Use Special Routing Table</b>	By setting this parameter to <b>yes</b> and selecting a table name below, routes learned by the RIP service are introduced into an own routing table. Note that the routing table is not automatically introduced, but has to be configured manually by introducing Policy Routes.
<b>Table Names</b>	A list of policy routing names can be specified here. Routes learned by the routing daemon are introduced into each of the enlisted routing tables.
<b>Multipath Handling</b>	↗ <b>ignore</b> multipath routes will be discarded <b>Attention:</b> RIP summarises routes to multipath routes automatically if more than one next hop to a prefix exists. Use setting "ignore" with caution. ↗ <b>assign-internal-preferences</b> multipath routes will be translated to several routes with different metrics (preferences) ↗ <b>accept-on-same-device</b> multipath routes will be introduced as multipath if all nexthops are reachable on the same interface ↗ <b>accept-all</b> (default) multipath routes will be introduced



### 1.3.7 Network Interfaces

In this section, interface specific parameters of the routing protocols are configured. This applies to OSPF and RIP.

#### 1.3.7.1 Section Network Interfaces Configuration

List 20-10 OSPF/RIP Setting - section Network Interface Configuration

Parameter	Description
<b>Load Interface Info</b>	If set to <b>yes</b> , the list of available interfaces is loaded after execution of <b>Send Changes</b> .
<b>Interfaces</b>	see list 20-11

List 20-11 OSPF/RIP Settings - Network Interfaces Configuration - Interfaces - section Shared Interface Configuration

Parameter	Description
<b>Interface Description</b>	Informational text field.
<b>Apply to Interface</b>	Specifies the network interface to which the following settings apply.
<b>Activate Config for</b>	Specifies the routing protocols for which the settings should be activated on this interface. Possible settings are OSPF, RIP or OSPF+RIP.
<b>Passive Interface</b>	On a passive interface the routing protocol does not send Hello packets. The network configured for this interface is still advertised. An interface is active by default (setting: <b>No</b> ).
<b>Parameter Template</b>	References templates for this interface.

List 20-12 OSPF/RIP Settings - Network Interfaces Configuration - Interfaces - section OSPF Specific Parameters

Parameter	Description						
<b>Network Type</b>	Type of network. Ethernet is normally <b>broadcast</b> . Sometimes there may be a need to use <b>point-to-point</b> for Ethernet-Links, for example when there is only a /30 subnet. Type <b>non-broadcast</b> is needed to propagate OSPF over a VPN tunnel.						
<b>Bandwidth [kBit/s]</b>	Bandwidth of the interface. Configuration is highly recommended since this information can not be determined automatically. This setting is used by OSPF to calculate the metric.						
<b>Interface Addresses</b>	<table border="1"> <thead> <tr> <th>Interface Addresses</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td></td> <td>By specifying an Interface Address the configuration only applies for a single OSPF network. This parameter can be useful in multinet environments. Otherwise the parameters applies to all OSPF networks on the given interface.</td> </tr> <tr> <td><b>Parameter Template for Address</b></td> <td>References templates for this interface.</td> </tr> </tbody> </table>	Interface Addresses	Description		By specifying an Interface Address the configuration only applies for a single OSPF network. This parameter can be useful in multinet environments. Otherwise the parameters applies to all OSPF networks on the given interface.	<b>Parameter Template for Address</b>	References templates for this interface.
Interface Addresses	Description						
	By specifying an Interface Address the configuration only applies for a single OSPF network. This parameter can be useful in multinet environments. Otherwise the parameters applies to all OSPF networks on the given interface.						
<b>Parameter Template for Address</b>	References templates for this interface.						

List 20-13 OSPF/RIP Settings - Network Interfaces Configuration - Interfaces - section RIP Specific Parameters

Parameter	Description
<b>Enable Split Horizon</b>	Split Horizon is a mechanism used by RIP to reduce the possibility of routing loops. By enabling this parameter (default: <b>yes</b> ), routes learned from a specific interface, are not re-advertised on this interface.
<b>Enable Poisoned Reverse</b>	This technology is an extension to Split Horizon. By enabling this setting (default: <b>no</b> ), routes learned from a specific interface are re-advertised on this interface but the metric is set to infinity (16).

#### 1.3.7.2 Section Available Interfaces

List 20-14 OSPF/RIP Settings - Network Interfaces Configuration - Available Interfaces - section Available Interfaces

Parameter	Description
	Displays a read-only list of the available network interfaces.

#### 1.3.7.3 Section Parameter Template Configuration

List 20-15 OSPF/RIP Settings - Network Interfaces Configuration - Parameter Template Configuration - section OSPF Parameters

Parameter	Description
<b>Authentication Type</b>	Authentication for neighbours on specified interface. Either no authentication (default: <b>null</b> ), <b>simple</b> authentication as specified in RFC1583 or the cryptographic authentication <b>digest-MD5</b> (RFC2328) can be used.
<b>Simple Authentication Key</b>	Password for simple authentication. This value only has to be specified with Authentication type set to <b>simple</b> .
<b>Digest Authentication Key</b>	Password for digest authentication. This value only has to be specified with Authentication type set to <b>digest-MD5</b> .
<b>Message Digest Key ID</b>	Key for digest authentication. This value only has to be specified with Authentication type set to <b>digest-MD5</b> .
<b>OSPF Priority</b>	Set to a higher value, the router will be more eligible to become a Designated Router or a Backup Designated Router. Set to <b>0</b> , the router is no longer eligible to become a Designated Router. Default: <b>1</b>
<b>OSPF Dead Interval</b>	Seconds for timer value used for Wait Timer and Inactivity Timer. This value must be the same for all routers attached to a common network.
<b>OSPF Hello Interval</b>	Time to wait between OSPF "hello" messages to neighbours (sec). This value must be the same for all routers attached to a common network.
<b>OSPF Retransmit Interval</b>	Minimum time waited between retransmissions (sec).
<b>OSPF Transmit Delay</b>	Sets number of seconds for <b>InfTransDelay</b> value. The InfTransDelay parameter defines the estimated time required to send a link-state update packet on the interface.

List 20-16 OSPF/RIP Settings - Network Interfaces Configuration - Parameter Template Configuration - section RIP Parameters

Parameter	Description
<b>Authentication Type</b>	Authentication for neighbours on specified interface. Either no authentication (default: <b>null</b> ), <b>text</b> authentication or the cryptographic authentication <b>digest-MD5</b> (RFC2082) can be used.
<b>RIP Key Chain</b>	The pull-down menu displays the configured key chains (see 1.3.5 RIP Router Setup) and allows selection of a key chain which is used for authentication.
<b>RIP Text Secret</b>	Specifies the text secret used for authentication purposes. Note that the value specified here always takes precedence over the <b>RIP Keychains</b> settings.
<b>Send Protocol</b>	Configures protocol types for transmission. Possible values are <b>Version_1</b> , <b>Version_2</b> or <b>Version_1+2</b> .
<b>Receive Protocol</b>	Configures protocol types for reception. Possible values are <b>Version_1</b> , <b>Version_2</b> or <b>Version_1+2</b> .

### 1.3.8 Neighbour Setup

For connectivity issues it is sometimes recommended to set the neighbours statically. Do this in the following section.

List 20-17 OSPF/RIP Settings - Neighbor Setup - section Neighbors

Parameter	Description
<b>Active</b>	Set to no to disable this neighbour configuration.
<b>Routing Protocols</b>	Specifies which routing protocols should be exchanged with this neighbour. Possible values are <b>OSPF</b> , <b>RIP</b> or <b>RIP+OSPF</b> .
<b>Neighbor IP</b>	IP address of the neighbour to exchange routing information with.

List 20-18 OSPF/RIP Settings - Neighbor Setup - section OSPF Parameters

Parameter	Description
<b>Neighbor Priority</b>	The Neighbor Priority parameter influences the Designated Router election. Set to a higher value, the router will be more eligible to become a Designated Router. Set to <b>0</b> , the router is no longer eligible to become a Designated Router or a Backup Designated Router. Default: <b>1</b>
<b>Dead Neighbor Poll Interval</b>	Seconds between two neighbour probings.

### 1.3.9 Filter Setup

A filter is needed for example when redistributing routes from one protocol to another. Available filters are ACLs and Prefix lists. Prefix lists are easier to use. See 1.3.9.1 Example for IP Prefix List Filter Usage for further information.

Route maps can be used to modify routing information. In route maps, the filter is applied to match the routes. Some set actions can be applied to the matching routes. Example: The RIP learned route 10.0.0.0/8 with metric 4 hops should have metric 6 instead. The match condition in the route map must be a filter matching 10.0.0.0/8 and the set condition must be metric 6.

When applying route filters in the RIP or OSPF section, only ACLs or Prefix-lists but no route maps are needed.

#### Note:

This dialogue is restricted to basic ACLs (1-99). Extended ACLs must be configured in Tab Text Based Configuration (page 491).

List 20-19 OSPF/RIP Settings - Filter Setup - section Access List Filters

Parameter	Description
	This section allows the definition of filters which can be referenced within the 1.3.4 OSPF Area Setup and within the RIP Route Update Filtering section (list 20-7, page 487).
<b>Name</b>	This is the ACL name.
<b>Description</b>	A short description of the ACL.
<b>Network Prefix</b>	Network/Netmask <b>Note:</b> Enter the address in phion Notation ( <b>Getting Started - 5.</b> phion Notation, page 25). The address will be converted to Cisco notation for the config file.
<b>Type</b>	Action for prefixitem <ul style="list-style-type: none"> <li>➤ permit (default)</li> <li>➤ deny</li> </ul>

List 20-20 OSPF/RIP Settings - Filter Setup - Route Map Filters - section Route Map Filters

Parameter	Description
	Route maps are used to control and modify routing information that is exchanged between routing domains.
<b>Name</b>	This is the Route Map Name.

List 20-21 OSPF/RIP Settings - Filter Setup - Route Map Filters - section Route Map Configuration

Parameter	Description
<b>Description</b>	A short description of the route map.

List 20-22 OSPF/RIP Settings - Filter Setup - Route Map Filters - section OSPF Specific Conditions

Parameter	Description
<b>Sequence Number</b>	Unique identifier for a route map entry.

List 20-22 OSPF/RIP Settings - Filter Setup - Route Map Filters - section OSPF Specific Conditions

Parameter	Description
<b>Type</b>	Action for route map: <ul style="list-style-type: none"> <li>➤ permit (default)</li> <li>➤ deny</li> </ul>
<b>Match Condition</b>	The route map entry matches when the route matches the configured criteria or filter: <ul style="list-style-type: none"> <li>➤ ACL (default)</li> <li>➤ PREFIXLIST</li> <li>➤ Gateway-IP</li> <li>➤ Interface-Name</li> </ul>
<b>ACL Name</b>	Name of ACL defined in the Access-Lists section above.
<b>IP Prefix List</b>	Name of IP prefix list defined in OSPF/RIP Settings - Filter Setup - IP Prefix List Filters - section IP Prefix List Filters List 20-24.
<b>Gateway IP</b>	IP of the Next Hop in the route.
<b>Out Interface Name</b>	See interfaces to gain available interface names.
<b>Set Action</b>	Defines action to set: <ul style="list-style-type: none"> <li>➤ Metric</li> <li>➤ Metric-Type</li> </ul>
<b>Set OSPF Metric</b>	Set metric for route map.
<b>Set OSPF External Metric</b>	Set external metric-type for route map.

List 20-23 OSPF/RIP Settings - Filter Setup - Route Map Filters - section RIP Specific Conditions

Parameter	Description
<b>Sequence Number</b>	Unique identifier for a route map entry.
<b>Type</b>	Action for route map: <ul style="list-style-type: none"> <li>➤ permit (default)</li> <li>➤ deny</li> </ul>
<b>Match Condition</b>	The route map entry matches when the route matches the configured criteria or filter: <ul style="list-style-type: none"> <li>➤ ACL (default)</li> <li>➤ PREFIXLIST</li> <li>➤ Gateway-IP</li> <li>➤ Interface-Name</li> <li>➤ Metric</li> </ul>
<b>ACL Name</b>	Name of ACL defined in the Access-Lists section above.
<b>IP Prefix List</b>	Name of IP prefix list defined in OSPF/RIP Settings - Filter Setup - IP Prefix List Filters - section IP Prefix List Filters List 20-24.
<b>Gateway IP</b>	IP of the Next Hop in the route.
<b>Interface Name</b>	See interfaces to gain available interface names.
<b>Set Action</b>	Defines action to set: <ul style="list-style-type: none"> <li>➤ Next-Hop</li> <li>➤ Metric</li> </ul>
<b>Set RIP Metric</b>	Set metric for route map.
<b>Set RIP Next-Hop IP</b>	Set next-hop IP address.

List 20-24 OSPF/RIP Settings - Filter Setup - IP Prefix List Filters - section IP Prefix List Filters

Parameter	Description
	Prefix lists are easier to understand for route-filters than ACLs. See 1.3.9.1 Example for IP Prefix List Filter Usage below for information on prefix list usage.
<b>Name</b>	This is the name of the IP prefix list.

List 20-25 OSPF/RIP Settings - Filter Setup - IP Prefix List Filters - section IP Prefix List Configuration

Parameter	Description
<b>Description</b>	A short description of the IP prefix list.
<b>Sequence Number</b>	Unique identifier for a prefixlist item.
<b>Network Prefix</b>	Network/Netmask

**List 20-25** OSPF/RIP Settings - Filter Setup - IP Prefix List Filters - section IP Prefix List Configuration

Parameter	Description
<b>Type</b>	Action for prefixitem ↗ permit ↗ deny
<b>Extent Type</b>	Matching condition: ↗ none (default) ↗ greater-than ↗ less-than
<b>Prefix Length</b>	Minimum or maximum prefix length to be matched.

### 1.3.9.1 Example for IP Prefix List Filter Usage

The following examples show how a prefix list can be used.

**Table 20-2** Example for IP Prefix List Filter - prefix list

	Network Prefix	Type	Extent Type
Deny default route 0.0.0.0/0	0.0.0.0/0	deny	none
permit prefix 10.0.0.0/8	10.0.0.0/8	permit	none

The following examples show how to specify a group of prefixes.

**Table 20-3** Example for IP Prefix List Filter - group of prefixes

	Network Prefix	Type	Extent Type	
accept a mask length of up to 24 bits in routes with the prefix 192.168/8	192.168.0.0/8	permit	less-than	24-Bit
deny mask lengths greater than 25 bits in routes with a prefix of 192/8	192.168.0.0/8	deny	greater-than	25-Bit
permit mask lengths from 8 to 24 bits in all address spaces	0.0.0.0/0	permit	greater-than	8-Bit
	0.0.0.0/0	permit	less-than	24-Bit
deny mask lengths greater than 25 bits in all address spaces	0.0.0.0/0	deny	greater-than	25-Bit
deny all mask lengths within the network 10/8	10.0.0.0/8	deny	less-than	32-Bit
deny all masks with a length greater than or equal to 25 bits within the network 192.168.1/24	192.168.1.0/24	deny	greater-than	25-Bit
permit all routes	0.0.0.0/0	permit	less-than	32-Bit

### 1.3.10 GUI as Text

**Note:**

This parameter set is only available in **Advanced View** mode.

The configuration done with the GUI is displayed here in quagga/Cisco commands.

**List 20-26** OSPF/RIP Settings - GUI as Text - section Text Equivalent of GUI

Parameter	Description
<b>Show as Text</b>	Set this to yes to show created OSPF syntax configuration after Send Changes.
<b>OSPF Text</b>	Created OSPF syntax configuration. Shown, if Show as Text is set to yes.

**List 20-26** OSPF/RIP Settings - GUI as Text - section Text Equivalent of GUI

Parameter	Description
<b>RIP Text</b>	Created RIP syntax configuration. Shown, if Show as Text is set to yes.

### 1.3.11 Text Based Configuration

Configure dynamic routing here, if you do not want to configure it with the GUI. Already done GUI configuration will be replaced. Syntax as used for quagga or Cisco applies.

**List 20-27** OSPF/RIP Settings - Text Based Configuration - section Free Format OSPF Configuration / Free Format RIP Configuration

Parameter	Description
<b>Use Free Format</b>	Set this to yes to use free OSPF/RIP syntax configuration.
<b>Free Format Text</b>	OSPF/RIP syntax configuration. This field applies when parameter Use Free OSPF format is set to yes.

## 1.4 Routing Configuration

**Attention:**

Network routes which are required for an OSPF/RIP network prefix must NOT be a subset of another route (see below for an explanation).

**Table 20-4** Configuration example

Configuration Entity	Values
OSPF network prefix	10.0.66.0/8
Server IP	10.0.66.98
Box network route	10.0.66.0/8 via dev eth1
<b>Additional box network route</b>	<b>10.0.0.0/24 via dev eth0</b>

In the configuration example (table 20-4), the required box network route "10.0.66.0/8 via dev eth1" is completely included in the additional box network route (**bold**). This will lead to a mismatch in the OSPF configuration. OSPF will neither detect eth0 nor eth1 as OSPF enabled and therefore not work.

## 1.5 HA Operation

The OSPF/RIP service synchronises externally learned routes with its HA partner. Routes cannot be introduced on the partner, while this is "passive" because network routes required to do so are missing. The external routes HA information is thus stored in a file and introduced on the HA system during startup of the OSPF/RIP service.

Take over and startup of the OSPF/RIP service usually take a few seconds. The HA routes are introduced as protocol "**extha**" (number 245). These routes are then either replaced by newly learned external OSPF or RIP routes (protocols "**ospfext**" or "**ripext**") or removed with the HA garbage collection after five minutes.

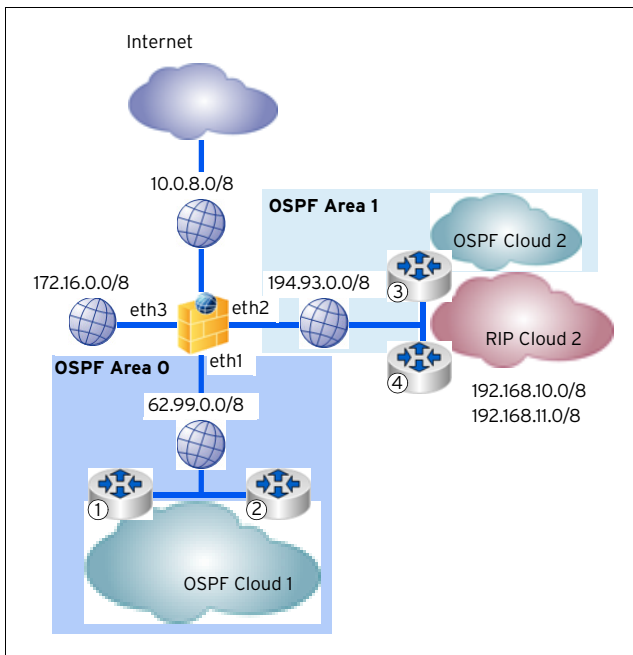
## 2. Example for OSPF and RIP Configuration

### 2.1 Network Setup

The following description is meant to point out a convenient way for OSPF and RIP configuration on a netfence gateway. The example assumes that a netfence is added to a network already configured for OSPF.

Four routers are appointed to learn routes from OSPF and RIP "Clouds". Router 1 and router 2 are both attached to LAN segment 62.99.0.0/8 and belong to OSPF Area 0. Router 3 is attached to LAN segment 194.93.0.0/8 serving as OSPF router in OSPF Area 1 and as RIP router for RIP Cloud 2. Router 4 is a sole RIP router attached to LAN segment 194.93.0.0/8. Two further networks 192.168.10.0/8 and 192.168.11.0/8 live in Rip Cloud 2.

Fig. 20-1 Example setup for OSPF and RIP configuration



- Router 1  
OSPF learned networks from OSPF Cloud 1:  
62.99.0.0/8

- Router 2  
OSPF learned networks from OSPF Cloud 1:  
62.99.0.0/8
- Router 3  
RIP and OSPF learned networks from OSPF and RIP Cloud 2  
194.93.0.0/8  
192.168.10.0/8  
192.168.11.0/8
- Router 4  
RIP learned networks from RIP Cloud 2  
194.93.0.0/8

### 2.2 Configuration Steps

The instruction is broken down into the segments listed below:

- OSPF basic setup (see 2.2.1)
- Redistribution of connected networks to OSPF (see 2.2.2)
- Injecting the default route to OSPF (see 2.2.3)
- OSPF Multipath routing (see 2.2.4)
- OSPF Link Authentication (see 2.2.5)
- OSPF Route Summarisation (see 2.2.6)
- RIP basic setup (see 2.2.7)
- Redistribution between RIP and OSPF (see 2.2.8)

#### 2.2.1 OSPF Basic Setup

The network is already configured for OSPF. Several destinations are reachable through multiple paths. The newly installed netfence gateway should participate in the routing and load-sharing shall be used.

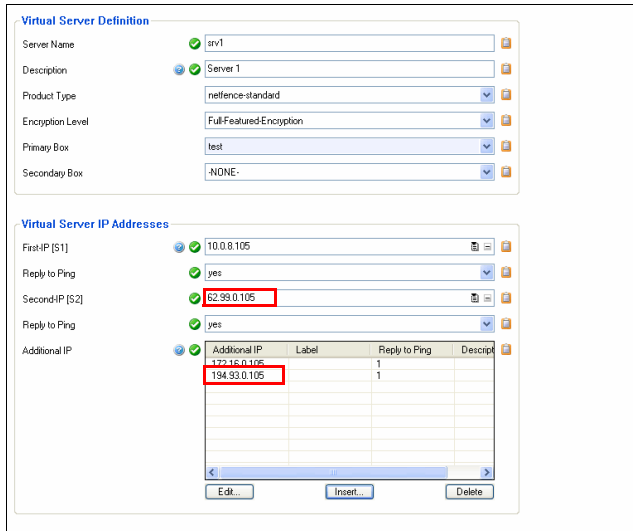
##### Step 1 Install the OSPF/RIP service

For a description how to install the service, see 1.2 Installation, page 485.

**Step 2 Add the network interfaces speaking OSPF to the Server Properties**

OSPF is spoken on two interfaces linking to the following networks: eth1 (62.99.0.0/8) and eth2 (194.93.0.0/8).

Fig. 20-2 Configuring of addresses in the Server Properties

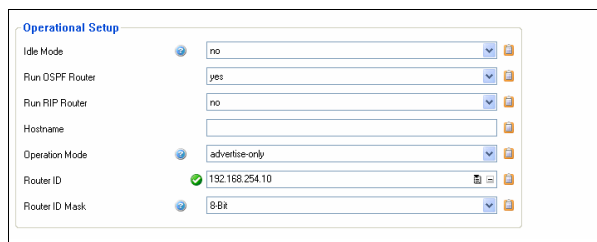


**Step 3 Configure OSPF Routing Settings**

**Operational Setup**

The netfence gateway is configured to operate as "normal" router. The operation mode is set to "active-passive" (that is *advertise-learn*). By this means, all routes are learned and forwarded. Setting a **Router ID** is mandatory. It is important for easily identifying LSAs during troubleshooting.

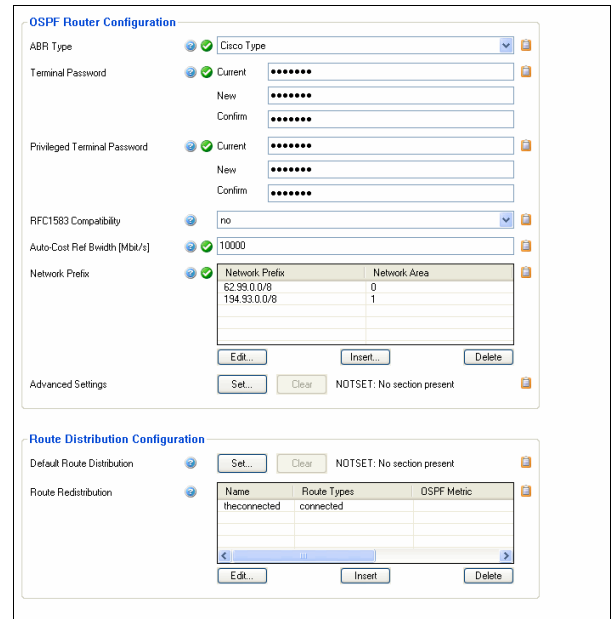
Fig. 20-3 OSPF Routing Settings - Operational Setup



**OSPF Router Setup**

Specify a **Terminal Password** and a **Privileged Terminal Password**. These passwords are needed to to access the routing engine directly via telnet. Setting **Auto-Cost Ref Bandwidth** to 10000 causes a more granular cost in LAN environments. The cost is calculated as ref-bandwidth divided by intf-bandwidth (Mbit/s). In the example, a 1 Gbit link would have a cost of 10 (10000/1000).

Fig. 20-4 OSPF Routing Settings - OSPF Router Setup



Specify the interfaces where OSPF should be enabled and where adjacencies should be built through the **Network Prefix** parameter. In the example, the netfence is made an Area Border Router (ABR) with interfaces in **Area 0** and **Area 1**. The network 62.99.0.0/8 is part of Area 0; the network 194.93.0.0/8 is part of Area 1.

**Step 4 Send Changes and Activate the configuration**

The basic OSPF setup is complete. The routes learned through OSPF can now be viewed in the netfence gateway's routing table.

Fig. 20-5 Routing table displaying routes learned through OSPF

Table / Sic Filter	State	Type	Device	Sic IP	Pref	Gateway	Name
192.168.10.0/8	up	gateway-ospfext	eth2	-	1010	194.93.0.254	
192.168.11.0/8	up	gateway-ospfext	eth2	-	1010	194.93.0.254	
192.168.12.0/8	up	gateway-ospfext	eth2	-	1010	194.93.0.254	
192.168.254.1/0	up	gateway-ospfext	eth1	-	1001	62.99.0.254	
192.168.254.2/0	up	gateway-ospfext	eth1	-	1001	62.99.0.253	
192.168.254.3/0	up	gateway-ospfext	eth2	-	1001	194.93.0.254	
194.93.0.0/8	up	device-boot	eth2	194.93.0.105	0	-	ext2
212.86.0.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
212.86.1.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
213.50.0.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
213.50.1.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
214.51.2.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
221.73.0.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
221.73.1.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
28.235.0.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
38.232.0.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
38.232.1.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
56.47.0.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
56.47.1.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
62.99.0.0/8	up	device-boot	eth1	62.99.0.105	0	-	ext1
79.23.0.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	
79.23.1.0/8	up	gateway-ospfext	eth1	-	1010	62.99.0.254	

A further way to see more detailed information regarding the OSPF service is to connect to the quagga engine itself with a telnet to localhost:2604 at the Command Line Interface. This mode can also be used for debugging purposes. If needed, see [www.quagga.net](http://www.quagga.net) for information about the Quagga Routing Suite.

Figure 20-6 shows the output of the commands `sh ip ospf neigh` and `sh ip ospf route`.

Fig. 20-6 Quagga engine output

```
[root@NF1:~]# telnet localhost 2604
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is quagga (version 0.96.5).
Copyright 1996-2002 Kunihiro Ishiguro.

User Access Verification

Password:
NF1> en
Password:
NF1# sh ip ospf neigh

Neighbor ID      Pri   State           Dead Time   Address
Interface        RXmtL RqstL DBsmL
192.168.254.3    1     Full/DR         00:00:35   194.93.0.254
eth2:194.93.0.105 0     0 0             00:00:35   194.93.0.105
192.168.254.2    1     Full/DR         00:00:33   62.99.0.253
eth1:62.99.0.105 0     0 0             00:00:33   62.99.0.105
192.168.254.1    1     Full/Backup     00:00:35   62.99.0.254
eth1:62.99.0.105 0     0 0             00:00:35   62.99.0.105
NF1# sh ip ospf route
===== OSPF network routing table =====
N   62.99.0.0/24          [1000] area: 0.0.0.0
    directly attached to eth1
N   192.168.1.0/24       [1010] area: 0.0.0.0
    via 62.99.0.253, eth1
D IA 192.168.10.0/23    Discard entry
N   192.168.10.0/24     [1010] area: 0.0.0.1
    via 194.93.0.254, eth2
N   192.168.11.0/24     [1010] area: 0.0.0.1
    via 194.93.0.254, eth2
N   192.168.12.0/24     [1010] area: 0.0.0.1
    via 194.93.0.254, eth2
N   192.168.254.1/32    [1001] area: 0.0.0.0
    via 62.99.0.254, eth1
N   192.168.254.2/32    [1001] area: 0.0.0.0
    via 62.99.0.253, eth1
N   192.168.254.3/32    [1001] area: 0.0.0.1
    via 194.93.0.254, eth2
N   194.93.0.0/24       [1000] area: 0.0.0.1
    directly attached to eth2

===== OSPF router routing table =====
R   192.168.254.1       [1000] area: 0.0.0.0, ABR, ASBR
    via 62.99.0.254, eth1
R   192.168.254.2       [1000] area: 0.0.0.0, ABR
    via 62.99.0.253, eth1
R   192.168.254.3       [1000] area: 0.0.0.1, ABR, ASBR
    via 194.93.0.254, eth2

===== OSPF external routing table =====
N E1 10.0.84.0/24      [1010] tag: 0
    via 62.99.0.254, eth1
N E1 28.235.0.0/24    [1010] tag: 0
    via 62.99.0.254, eth1
N E1 38.232.0.0/24    [1010] tag: 0
    via 62.99.0.254, eth1
N E1 38.232.1.0/24    [1010] tag: 0
    via 62.99.0.254, eth1
N E1 56.47.0.0/24     [1010] tag: 0
    via 62.99.0.254, eth1
N E1 56.47.1.0/24     [1010] tag: 0
    via 62.99.0.254, eth1
N E1 79.29.0.0/24     [1010] tag: 0
    via 62.99.0.254, eth1
N E1 79.29.1.0/24     [1010] tag: 0
    via 62.99.0.254, eth1
N E1 123.43.0.0/24    [1010] tag: 0
    via 62.99.0.254, eth1
N E1 123.43.1.0/24    [1010] tag: 0
    via 62.99.0.254, eth1
N E1 134.46.0.0/24    [1010] tag: 0
    via 62.99.0.254, eth1
N E1 134.46.1.0/24    [1010] tag: 0
    via 62.99.0.254, eth1
```

## 2.2.2 Redistribution of Connected Networks to OSPF

Proceed as follows to configure redistribution of connected networks:

### Step 5 Activate OSPF advertising

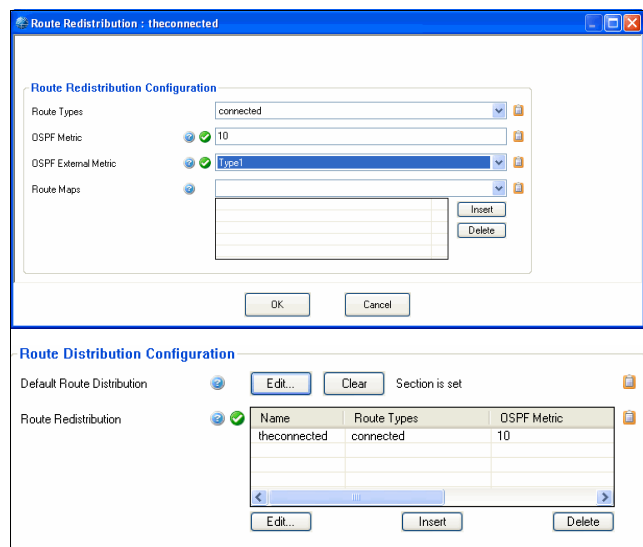
Browse to **Config** > **Box** > **Network** > **Networks** and set parameter **Advertise Route** to *yes*.

### Step 6 Configure Route Redistribution

Route Redistribution is configured in the OSPF Router tab within the OSPF Routing Settings configuration.

In the example, the following values are specified for the available parameters:

Fig. 20-7 Configuring Route Redistribution



With these configuration settings, all networks connected to the netfence gateway will be redistributed to OSPF with a cost of 10 and Metric-type External 1.

## 2.2.3 Injecting the Default Route to OSPF

### Step 7 Activate OSPF advertising

Static Routes as well as only advertised via OSPF when the **Advertise Route** option is set in the network configuration. If not already done, browse to **Config** > **Box** > **Network** > **Networks** and set parameter **Advertise Route** to *yes*.

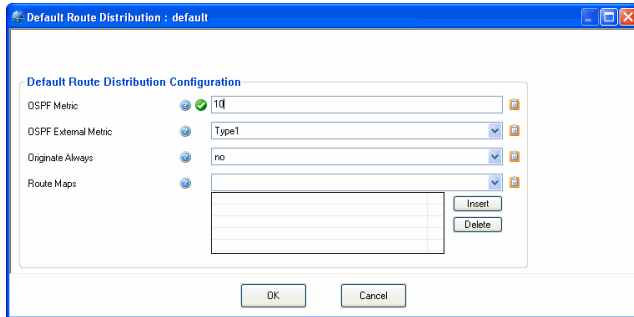


### Step 8 Configure Default Route Redistribution

Default Route Redistribution is configured in the OSPF Router tab within the OSPF Routing Settings configuration.

In the example, the following values are specified for the available parameters:

Fig. 20-8 Configuring Default Route Redistribution



With these configuration settings, the default route (if configured) will be redistributed to OSPF with a cost of 10 and Metric-type External 1. If a default route should always be distributed unless configured or not, set parameter **Originate Always** to yes.

## 2.2.4 OSPF Multipath Routing

Multipath routing is configured in the OSPF Routing Settings' **OSPF Preferences** view.

Three options are available for Multipath Handling:

- **ignore**  
No Multipath routing is used; learned Multipath routes are ignored.
- **assign internal preferences**  
The metric of every equal cost route is translated to different values - load-sharing is not used. Additional routes are only used as backup.
- **accept on same device**  
Multipath routing is enabled but it is only available when the routes are learned on the same interface.

The example configuration uses the setting **accept on same device**.

## 2.2.5 OSPF Link Authentication

Two methods for OSPF authentication exist:

- Authentication in an Area
- Authentication on a Link

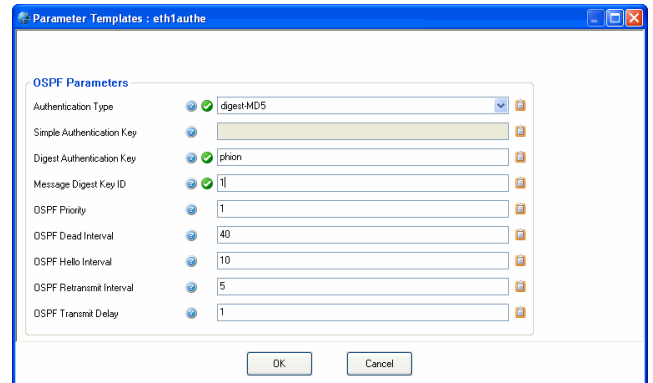
Area authentication is configured within the **OSPF Area Setup**. For Link Authentication first a parameter template has to be created, and then a reference to this template has to be established. The example uses Link Authentication.

Authentication configuration is done in the **Network Interfaces** section of the OSPF Routing configuration. Proceed as follows to configure Link Authentication:

### Step 9 Configure a parameter template

Open the **Network Interfaces** section and click the **Insert ...** button in the **Parameter Template Configuration** section to create a new parameter template. The following values are defined in the example: MD5 Authentication usage with key ID "1" and authentication key "phion".

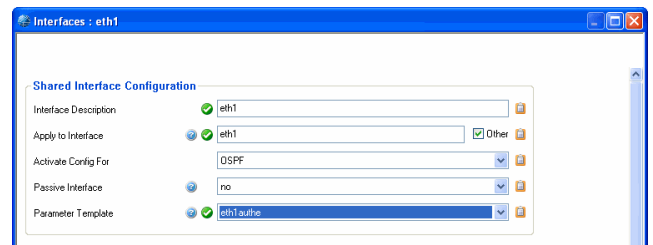
Fig. 20-9 Configuring a parameter template



### Step 10 Create a reference to the parameter template

Click the **Insert ...** button in **Network Interface > Interfaces** (**Network Interfaces** view) to configure link authentication on an interface. The example defines the following values:

Fig. 20-10 Creating a link to the parameter template



#### Note:

All other routers on this interface must have the same settings. Otherwise, adjacency cannot be established.

## 2.2.6 OSPF Route Summarisation

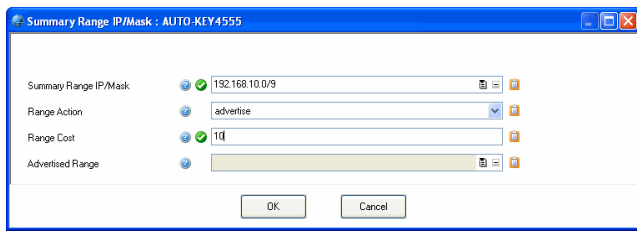
In large networks is it useful to summarise routes on Area or Autonomous system borders. In the example setup, two networks live in Area 1: 192.168.10.0/8 and 192.168.11.0/8. The aim is to summarise these two networks to 192.168.10.0/9.

The configuration for summarisation of areas is done in the **OSPF Area Setup**.

Click the **Insert ...** button to create new configuration settings for Area 1. Set the value for **Area ID [Int]** to "1". Create a new entry for parameter **Summary Range IP/Mask** by clicking **Insert ...**

A new window opens allowing for configuration of the following values:

Fig. 20-11 Configuring route summarisation



Range 192.168.10.0/9 is now going to be advertised as summary route with cost 10. A router in Area 0 is going to create an entry in its routing table alike the following one:

Fig. 20-12 Entry in routing table

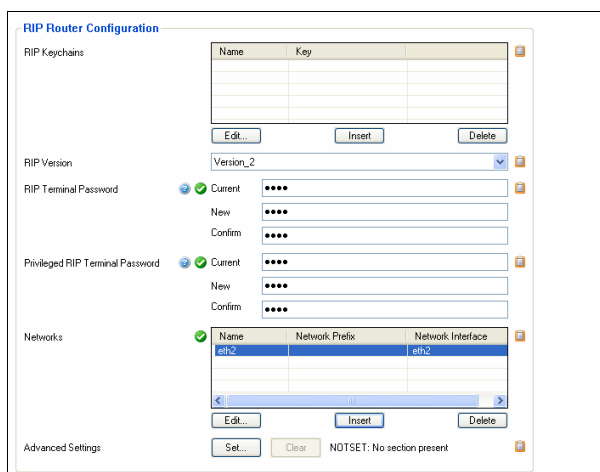
```
SW2#sh ip route 192.168.10.0
Routing entry for 192.168.10.0/23, supernet
Known via "ospf 1", distance 110, metric 1020, type inter area
Last update from 62.99.0.105 on Vlan111, 00:03:46 ago
Routing Descriptor Blocks:
* 62.99.0.105, from 192.168.254.10, 00:03:46 ago, via Vlan111
Route metric is 1020, traffic share count is 1
```

## 2.2.7 RIP Basic Setup

Basic RIP settings have to be configured in the **Operational Setup**, the **RIP Preferences** and the **RIP Router Setup**. In the example setup, RIP Version 2 is used and multipath routes are discarded. Therefore, the following configuration settings apply:

- **Operational Setup**  
RIP is activated by setting parameter **Run RIP Router** to **yes**.
- **RIP Preferences**  
Parameter **Multipath Handling** is set to **ignore**.
- **RIP Router Setup**  
**RIP Version 2** is enabled on **Network Device** eth2 in the **Networks** section.  
Redistribution of connected networks to RIP is configured in the **Route Redistribution** section. In the example, all connected networks are redistributed to RIP with a hopcount of 2.

Fig. 20-13 Configuring RIP settings - RIP Router Setup



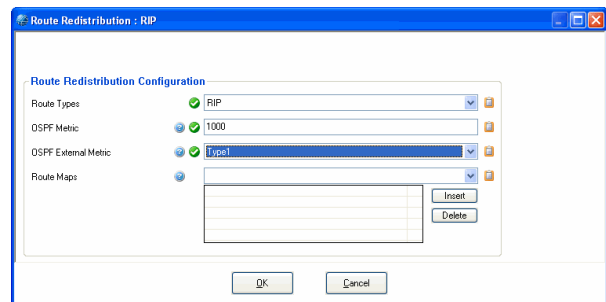
## 2.2.8 Redistribution between RIP and OSPF

To implement redistribution between RIP and OSPF the following minimum settings have to be configured:

### ➤ OSPF Router Setup

To redistribute routes learned by RIP insert a new entry in the **Route Redistribution Configuration** section.

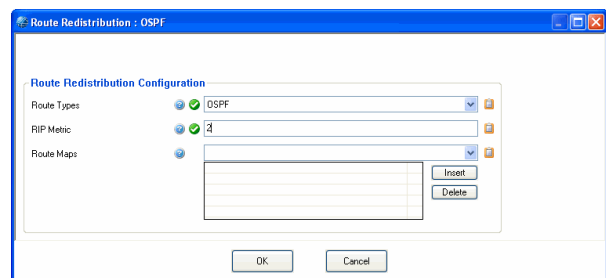
Fig. 20-14 Configuring route redistribution



### ➤ RIP Router Setup

To redistribute routes learned by OSPF insert a new entry in the **Route Redistribution Configuration** section.

Fig. 20-15 Configuring route redistribution



# Licensing

<b>1.</b>	<b>Understanding phion Licensing</b>	
1.1	Module-dependent Licensing .....	498
1.2	Quantity-dependent Licensing .....	498
1.3	User-counting .....	498
<b>2.</b>	<b>phion Licensing Examples</b>	
2.1	Example Setup .....	499
2.2	Example 1 .....	499
2.3	Example 2 .....	499
<b>3.</b>	<b>Licenses Overview</b>	
3.1	Licences Format .....	500
3.2	Licences Types .....	500
3.2.1	Box Licences for Self-managed Gateways .....	500
3.2.2	management centre Licences .....	501
3.2.3	"Floating" Box Licences .....	502
3.2.4	VPN-Pool Licences .....	502
3.2.5	Avira Virus Scanner Licences .....	502
<b>4.</b>	<b>System Behaviour without or with Invalid Licences</b>	
4.1	Evaluation Mode .....	503
4.2	Valid Mode .....	503
4.3	Grace Mode .....	504
4.3.1	On Self-managed Gateways and management centres .....	504
4.3.2	On MC-administered Boxes .....	504
<b>5.</b>	<b>License Activation</b>	
5.1	Get the License Key .....	506
5.2	Activate the License Key(s) .....	506
5.2.1	Activating the License on a Self-managed Netfence Gateway .....	506
5.2.2	Activating the Licences on the MC .....	507
5.3	Emergency Strategies .....	508
5.3.1	Self-managed netfence Gateways .....	508
5.3.2	management centre .....	508
<b>6.</b>	<b>Protected IP Count Policies</b>	
6.1	Policy No. 1: No Counting .....	509
6.2	Policy No. 2: Rule Explicit .....	509
6.3	Policy No. 3: Redirected Destination .....	509
6.4	Policy No. 4: Site-to-site Tunnel .....	509
6.5	Policy No. 5: General Case .....	510

# 1. Understanding phion Licensing

Licences for netfence products are designed so that they correspond as closely as possible to the intended use of the product. We generally try to interpret the licence parameters in such a way as to accommodate the customer's need as much as possible.

## 1.1 Module-dependent Licensing

Licences include the list of modules that may be active on a netfence system. For example, the sectorwall and contegrity licences do not include the VPN module, whereas it is included in netfence sintegra and gateway licences. In this way it is possible to implement different product types using identical software.

## 1.2 Quantity-dependent Licensing

Some modules are not merely switched on and off by licences but in addition their usage is metered.

## 1.3 User-counting

### ➤ Firewall

The number of firewall users is defined as follows:

The current number of firewall users is defined as the number of IP addresses that have used the firewall engine with permission within the last hour. The algorithm is explained in detail below.

### ➤ VPN

The VPN connector itself is not licensed, but its access to the VPN server is licensed. The netfence VPN server differentiates between 2 types of access:

- named user
- concurrent use

Named users are appointed by the VPN server's internal CA. The concurrent use method is used for users who do not access the internal CA for authentication. VPN licences include the number of maximum possible users.

Certificates issued by the VPN server's internal CA reduce the maximum number of users who are able to simultaneously gain access using other authentication methods.

### ➤ URL filter

The URL filter counts the incoming user names or IP addresses and, like the Firewall, saves them for one hour. If the number of licensed users is exceeded, non-licensed users will either be blocked or allowed to pass, depending on how the system is configured. The URL filter users are to be licensed per system.

### ➤ Antivirus

The exact number of users is calculated from all users whose traffic is checked for viruses. For this, all e-mail users, web users and FTP users from the entire CPA are added together.

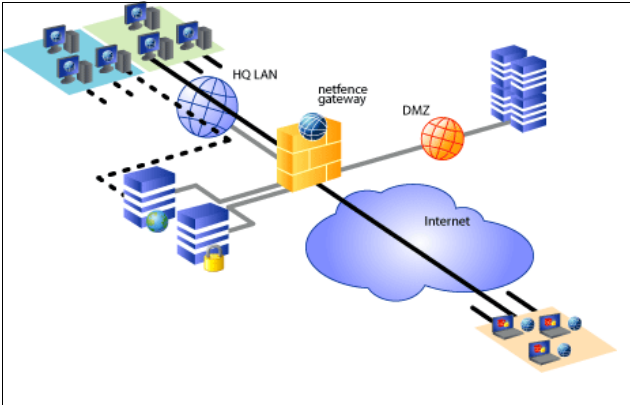
Virus scanner licences are **independent of the number of systems** and can be used simultaneously on any number of systems.

The virus scanner licences come with an expiry date. After the licence has expired, NO further viruses will be detected. Extend your licence in plenty of time.

## 2. phion Licensing Examples

### 2.1 Example Setup

Fig. 21-1 Example setup



### 2.2 Example 1

A network with 200 IP addresses is protected by a netfence gateway. Only 40 workstations have transparent access to the Internet through the firewall. 130 workstations have web access using the built-in http-proxy of the netfence gateway. There are 4 servers in the DMZ. 5 VPN clients connect remotely to the VPN server.

The optimum license for this deployment would be an NF-50 (not an NF 250).

**Explanation:**

The 40 clients and 4 servers are counted as protected IPs, 130 workstations access a local service (proxy) and are thus not counted. The 5 VPN clients need VPN-Pool licenses, which are included in the nf-50 license.

### 2.3 Example 2

In addition to 7 nomadic users using Secure Connectors with certificates, 11 individual contractors need VPN access to some machines for support reasons and authenticate themselves by using a user name/password scheme but only one to three at a time.

The correct VPN-Pool license would be a 10-client license.

**Explanation:**

The 7 nomadic users will obtain client access certificates issued by the VPN server. The three remaining client-access licenses are unused, so three clients at a time can connect using a purely external authentication scheme.

## 3. Licenses Overview

### 3.1 Licenses Format

All phion licenses are x.509 certificates issued and signed by the phion Certificate Authority. They are distributed as **.lic** files and may be viewed with an arbitrary text editor.

Because all netfence products have the phion public key built into the product, they can easily validate the certificates and extract the license information.

phion issues different types of licenses, which are described below.

### 3.2 Licences Types

phion licenses are divided into the following types:

- **node-locked licenses** (see 3.2.1 Box Licenses for Self-managed Gateways and 3.2.2 management centre Licenses)
- **pool/floating licenses** (see 3.2.3 "Floating" Box Licenses)

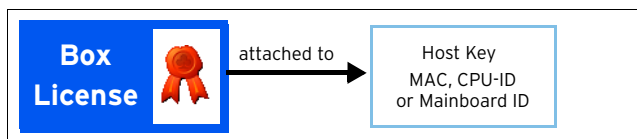
Node-locked licenses are issued to self-managed gateways (Box License) and management centres (MC Box License and/or Master License) and are bound to a hardware ID of the system.

Pool licenses are attached to the Master License and assigned to the MC-administered boxes dynamically. When assigned, the license is granted a specific time-to-live, the so-called "float"-time. Licenses that are assigned to boxes by a management centre are therefore also referred to as "floating" licenses.

#### 3.2.1 Box Licenses for Self-managed Gateways

Single box licenses are associated with a hardware ID of the machine they are running on. Typically either the MAC address of a network card, the main board ID or the CPU ID is used as the key for the license. The box license contains information on what kind of service can be started on this machine and to what extent it can be used (Firewall, VPN server, management centre, ...).

**Fig. 21-2** Principle of a node-locked license on a self-managed netfence gateway



As box licenses for self-managed gateways are bound to a hardware ID (a host key) they are referred to as so-called **node-locked licenses**. The table below lists the host key types, which can be used for node-locking:

- CPU-ID (available only for Pentium III and higher and only if activated in BIOS)
- Motherboard ID
- MAC addresses of the network adapters.

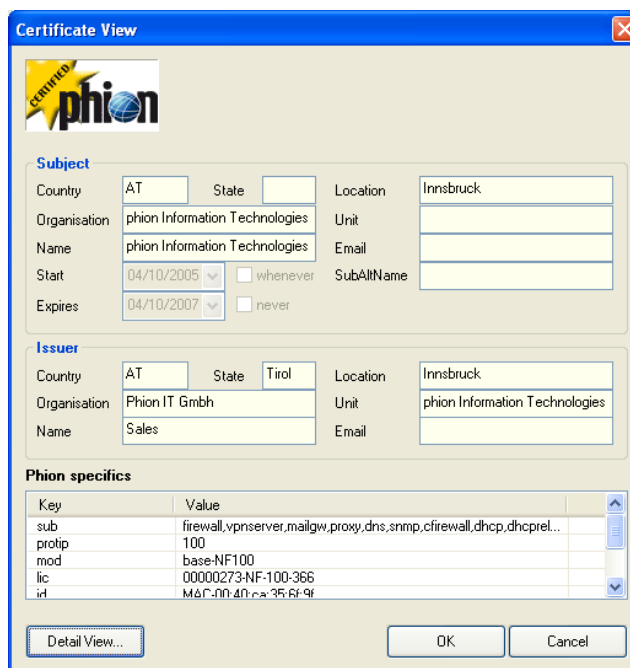
**Table 21-1** Host key examples

Key (Examples)	Comment
CPU-0000-068A-0003-C4DD-B165-B468	Valid CPU ID, invalid CPU IDs end with 0000-0000
BBS-8123FHGZOSCP	Valid Motherboard ID, several vendors do not provide an ID
MAC-00:90:27:43:48:ac MAC-00:90:27:0c:5f:1a MAC-00:02:a5:77:4f:7d	MAC addresses of network interfaces

Several vendors exist who do not provide unique IDs for CPUs and motherboards. Even network adapters exist, which do not provide a MAC address to the operating system. It is recommended to provide the phion licensing centre with all available host keys when requesting a license to avoid unnecessary delays.

After the box license file has been imported into the self-managed gateway (see 5.2 Activate the License Key(s), page 506), you will be able to view the certificate graphically (figure 21-3).

**Fig. 21-3** Certificate file as shown after box import and activation



**Certificate View**

**Subject**

Country	AT	State		Location	Innsbruck
Organisation	phion Information Technologies			Unit	
Name	phion Information Technologies			Email	
Start	04/10/2005	<input type="checkbox"/> whenever		SubAltName	
Expires	04/10/2007	<input type="checkbox"/> never			

**Issuer**

Country	AT	State	Tirol	Location	Innsbruck
Organisation	Phion IT GmbH			Unit	phion Information Technologies
Name	Sales			Email	

**Phion specifics**

Key	Value
sub	firewall.vpnserver.mailgw.proxy.dns.snmp.cfirwall.dhcp.dhcrel...
protip	100
mod	base-NF100
lic	00000273-NF-100-366
irt	M&C-00:40:ca:35:6f:9f

Buttons: Detail View..., OK, Cancel



Important license details are listed in the *Phion specifics* section:

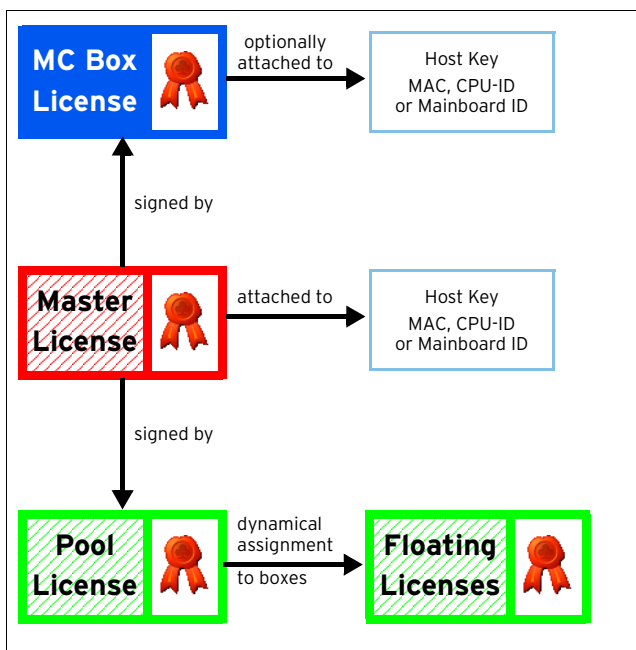
**Table 21-2** Important phion specifics in a node-locked license for a self-managed gateway

Key	Description
sub	This field lists the services the netfence gateway has been licensed for.
protip	This is the number of protected IPs the gateway has been licensed for.
mod	This field contains the license model, that means the product variant designed for a specific number of users covered by the license (for example base-NF100).
lic	This is the name of the license file as issued by the phion licensing centre (for example 00000273-NF-100-366). <b>Note:</b> Pass this name to the phion licensing centre in case license reissue becomes necessary (for example after new installation on another hardware due to crash recovery).
id	This is the host key the license has been bound to when it was issued.
grace	This is the time span for which the license remains valid in case it is installed on a system it has not been issued for (for example in case of crash recovery). See 4.3 Grace Mode, page 504 for further information on how to interpret grace time. <b>Attention:</b> The grace time of phion licenses is typically 15 days. All services will be deactivated after grace time has expired.

### 3.2.2 management centre Licenses

Analogous to box licenses for self-managed gateways, management centre licenses are attached to the hardware of the machine the management centre (MC) is running on. The MC (Master) License enables the administrator to generate and activate the Main Identity of the management centre (see 5.2.2 Activating the Licenses on the MC, page 507). This Main Identity will be used for all further communication between the MC and the netfence gateways.

**Fig. 21-4** Licenses interrelationship between MC and MC-administered boxes



### 3.2.2.1 MC Box License

Important license details of the MC Box License are listed in the *Phion specifics* section:

**Table 21-3** Important phion specifics in a node-locked box license for a management centre

Key	Description
sub	This field lists the services the management centre has been licensed for.
ranges	This is the number of ranges that may be created on the MC.
protip	This is the number of protected IPs MC has been licensed for.
mod	This field contains the license model, that means the product variant designed for a specific number of users covered by the license (for example base-MCED).
lic	This is the name of the license file as issued by the phion licensing centre (00000273-NF-100-366). <b>Note:</b> If the box license file is attached to a host key pass this name to the phion licensing centre in case license reissue becomes necessary (for example after MC installation on another hardware due to crash recovery).
id	This is the host key the license has been bound to when it was issued.
grace	This is the time span for which the license remains valid in case it is installed on a system it has not been issued for (for example in case of crash recovery). See 4.3 Grace Mode, page 504 for further information on how to interpret grace time. <b>Attention:</b> The grace time of phion licenses is typically 15 days. All services will be deactivated after grace time has expired.

### 3.2.2.2 MC Master License

Important license details of the MC Master License are listed in the *Phion specifics* section:

**Table 21-4** Important phion specifics in a node-locked master license for a management centre

Key	Description
ranges	This is the number of ranges that may be created on the MC.
mod	This field contains the license model. The master license is flagged with the model type <i>master</i> .
master	This is the name of the MC Identifier.
lic	This is the name of the master license file (for example LIC-00000273-MASTER-468). <b>Note:</b> Pass this name to the phion licensing centre in case license reissue becomes necessary (for example after MC installation on another hardware after crash recovery).
id	This is the host key the license has been bound to when it was issued.
grace	This is the time span for which the license remains valid in case it is installed on a system it has not been issued for (for example in case of crash recovery). See 4.3 Grace Mode, page 504 for further information on how to interpret grace time. <b>Attention:</b> The grace time of phion licenses is typically 15 days. All services will be deactivated after grace time has expired.

### 3.2.3 "Floating" Box Licenses

In deployments in which a management centre controls one or more netfence gateways, the license for the gateways can be attached to the MC license and dynamically assigned to the managed nodes.

You will be equipped with a management centre (Master) license and with one or multiple pool licenses, which have to be installed on the boxes the MC administers.

On a management centre, floating licenses can be assigned to boxes by choosing **Import from Pool License** instead of **Import from File** (3.2 Installing the Licenses, page 394). Pool licenses are not node-locked but they are instead conjoint to the Master License Key on the management centre. Boxes are thus obliged to verify their licenses with the MC.

Again, important license details are listed in the **Phion specifics** section:

**Table 21-5** Important phion specifics in a pool license issued for multiple MC-administered boxes

Key	Description
sub	This field lists the services the netfence gateways have been licensed for.
protip	This is the number of protected IPs the gateways have been licensed for.
num	This is the number of gateways that have been licensed.
mod	This field contains the license model, that means the product variant designed for a specific number of users covered by the license (base-NF500).
master	This is the name of the MC Identifier.
lic	This is the name of the box pool license file as issued by the phion licensing centre (for example 00000273-NF-500-469).
id	This is the name of the master license file this pool license has been signed by (for example LIC-00000273-MASTER-468).
grace	This is the time span for which the license remains valid in case the box cannot connect to its management centre for purpose of license verification. See 4.3 Grace Mode, page 504 for further information on how to interpret grace time. <b>Attention:</b> The grace time of phion licenses is typically 15 days. All services will be deactivated after grace time has expired.

### 3.2.4 VPN-Pool Licenses

VPN-Pool licenses are either attached to a hardware ID of the machine running the VPN Server or to the MC license, respectively. They contain information as to how many client access licenses (split into Secure Connector and Smart Connector) can be issued by the VPN server. The clients use these certificates to access the VPN server. In deployments using authentication methods that are not based on the internal CA (external PKI and/or user/password methods), the number of client access certificates not yet issued also specifies the maximum number of concurrent VPN client connections.

However, it is not possible to have overlay pool licenses, that means to have one 100 user license flexibly dividable.

In the VPN Pool License as well, important license details are listed in the **Phion Specifics** section:

**Table 21-6** Important phion specifics in a VPN pool license

Key	Description
smart	This field defines the type of the license. Secure Connector licenses are flagged with <b>0</b> , Smart Connector licenses are flagged with <b>1</b> .
seq	This is the sequence number of the license. One VPN client license is included into every purchased netfence product. This client license is installed by default (license file name <b>fwsingle</b> ) and defined by sequence number <b>1</b> . Every additionally installed license will be numbered consecutively.
num	This is the number of licensed VPN clients.
mod	This field contains the license model, that is <b>vpnpool</b> for a VPN pool license.
master	This is the name of the MC Identifier (in case the license has been issued for MC-administered boxes).
lic	This is the name of the VPN pool license file as issued by the phion licensing centre (for example 00000283-VPN-SECURE-400). <b>Note:</b> In case the VPN license is installed on a self-managed netfence gateway, pass this name to the phion licensing centre if license reissue becomes necessary (for example after new box installation on another hardware due to crash recovery).
id	This value is defined by the parent the VPN pool license file has been signed by. On self-managed netfence gateways this field will contain the hardware host key the license has been bound to when it was issued. in case the license has been issued for MC-administered boxes, the id field will contain the name of the master license file this pool license has been signed by prefixed with the word "float" (for example float-LIC-00000273-MASTER-468).
grace	This is the time span for which the license remains valid in case it is either installed on a system it has not been issued for (for example in case of crash recovery on another hardware), or in case the box cannot connect to its management centre for purpose of license verification. See 4.3 Grace Mode, page 504 for further information on how to interpret grace time. <b>Attention:</b> The grace time of phion licenses is typically 15 days. All services will be deactivated after grace time has expired.


For instructions how to import the VPN Pool License into the VPN server see **VPN - 2.6.1 Phion VPN CA Tab**, page 212.

### 3.2.5 Avira Virus Scanner Licenses

As the The AntiVir service is a tight integration of the AVIRA AntiVir WebGate and AVIRA AntiVir MailGate products into the netfence gateway, Avira Virus Scanner licenses are issued in two components:

- a .lic file typically named 0000nnnn-**VIRSCAN**-nnn.lic
- a .key file

Import the .lic file into **Box Licenses** (accessible via  **Config** >  **Box**).

Import the .key file into the fields **AVIRA license** in the  **Virus Scanner Settings (Anti-Virus - 2.1 Basic Setup**, page 368).

In case the Avira Virus Scanner license is installed on a self-managed netfence gateway, pass the name of the .lic file to the phion licensing centre if license reissue becomes necessary (for example after new box installation on another hardware due to crash recovery).

## 4. System Behaviour without or with Invalid Licences

The license status of a system is of major importance for its functionality. License states are depicted graphically in several monitoring areas of the graphical administration tool phion.a:

- **phion.a start screen (Getting Started - 3.2.1 Start Screen, page 18)**  
The background colour of the license icon changes to yellow when the system enters grace mode and to red when grace mode has expired.
- **Licenses tab (Control Centre - 2.5 Licenses Tab, page 37)**  
The background colour of the icon in the tab heading changes to yellow when the system enters grace mode and to red when grace mode has expired.

The phion license system generally distinguishes between three license modes:

- Evaluation Mode (see 4.1 Evaluation Mode)
- Valid Mode (see 4.2 Valid Mode)
- Grace Mode (see 4.3 Grace Mode)

### 4.1 Evaluation Mode

Even without a valid license the netfence gateway provides the most relevant features. Nevertheless the system is not intended to serve any other purpose than evaluation.

Take into consideration that evaluation systems comprise the following characteristics:

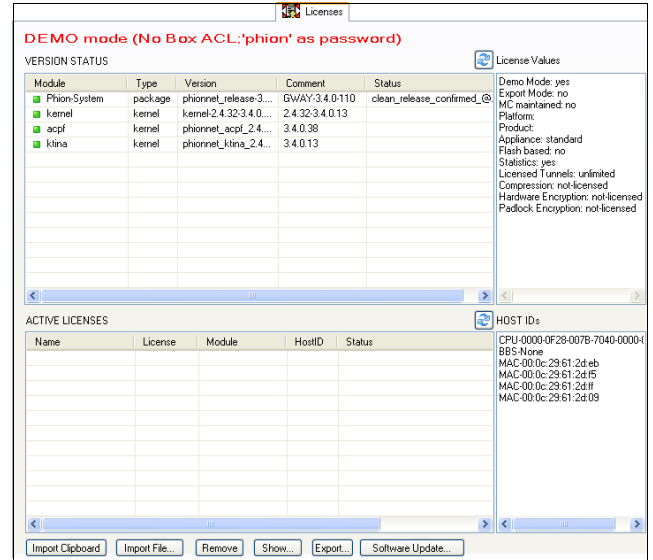
- Only weak encryption & authentication methods (DES, RSA-512) are implemented.
- Full root access to phion processes is granted with password *phion*.
- Box access control lists have no effect.

This means that any computer with network access to a management IP on your evaluation system is able to manage it.

**Attention:**  
Running the system in evaluation mode is completely insecure and can have severe impacts on your network. DO NOT evaluate the netfence gateway on security sensitive points.

The **Control > Licenses** tab illustrates DEMO mode systems in the following way:

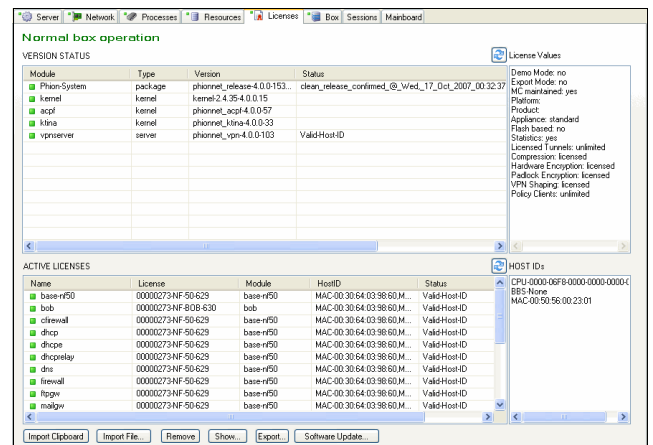
**Fig. 21-5** License view of the control window without valid license activated



### 4.2 Valid Mode

As soon as the license key is activated, all restrictions of the evaluation mode disappear. A fully functional system is titled with "Normal box operation".

**Fig. 21-6** License view of the control window with valid licenses activated

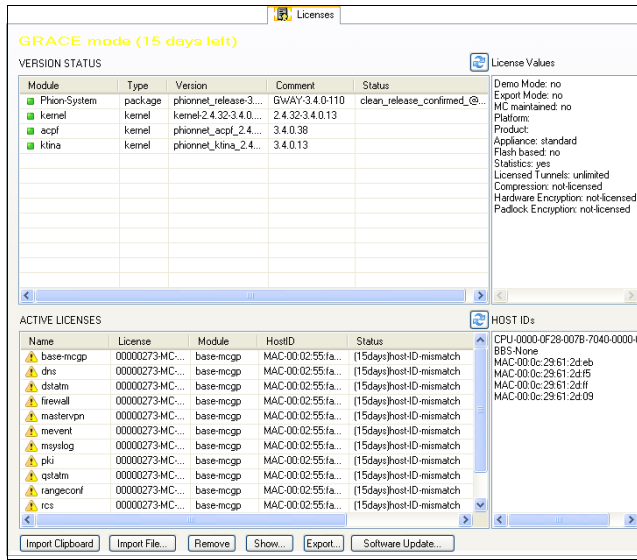


## 4.3 Grace Mode

### 4.3.1 On Self-managed Gateways and management centres

In case of a hardware failure and subsequent transfer of service to another machine, a license strictly bound to an unchangeable hardware criterion results in a loss of service. For this reason, almost every license issued by phion has a so-called Grace Period (typically 15 days). During this time, the netfence gateway works according to the parameters defined in the license, even if the hardware ID the license is attached to does not match the actual hardware. Should this happen, please contact your phion partner immediately to request a license reissue.

Fig. 21-7 License view of the control window with an invalid license activated on an MC.



**Note:**  
The MC has just been reinstalled on a hardware not matching the license. 15 days are left until services will be deactivated due to a "host-ID-mismatch".

**Note:**  
Even while in grace mode, an MC will renew floating box licenses when requested by its administered boxes. Nevertheless, do not delay requesting a license reissue.

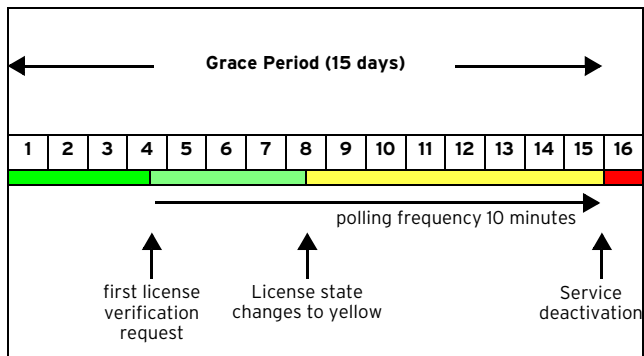
### 4.3.2 On MC-administered Boxes

Because the management centre renews floating box licenses attached to managed nodes periodically, a netfence system might switch to Grace Mode if the management centre is not available for a period longer than a quarter of the grace period.

Reconnecting the management centre or re-establishing communication between the managed netfence system and the management centre resolves this issue.

Have a look at the following chart to understand the calculation of grace time for floating box licenses. A typical grace period of 15 days is assumed:

Fig. 21-8 Grace time for floating box licenses

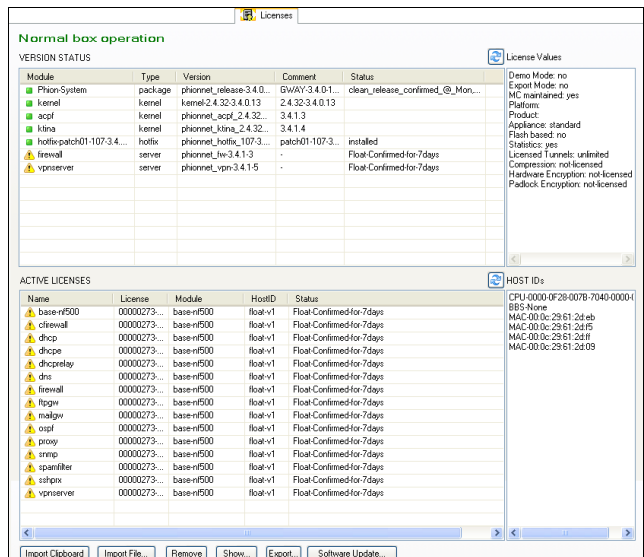


The box makes the first attempt to verify its license after a quarter of the grace period has expired. If it succeeds the license is renewed, granted a float time of 15 days and the cycle starts from the beginning.

If it fails, the box starts polling in sequences of 10 minutes. After half of the grace period has expired, the license's status colour changes to yellow. If the box has not succeeded in validating its license until grace time expires all services on the box are deactivated, and only access to configuration and control GUI is possible further on. Other management interfaces are not accessible until the license is validated again or another valid license is activated.

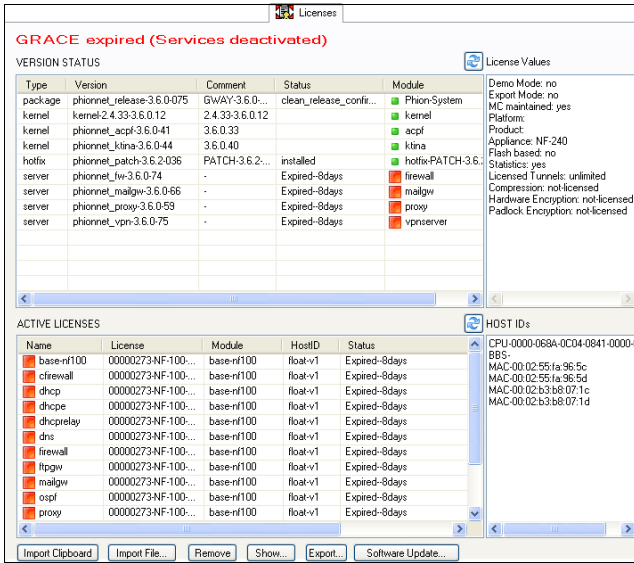
Floating box licenses that have not been renewed after a quarter of the grace period has expired will be displayed in the **Control > Licenses** tab in the following way:

Fig. 21-9 License view of the control window with floating licenses that will expire in 7 days



Their colour changes to red when they are deactivated:

Fig. 21-10 License view of the control window with deactivated services



**Attention:**

When license verification fails because the MC is unavailable, the box license status changes into grace mode for a defined period, until finally the system is considered as unlicensed and all services are deactivated. Step into action immediately when systems change into grace mode.







## 5.3 Emergency Strategies

In case of a hardware failure, which makes it impossible to run the system with the same host-key again, the following steps are recommended.

### Attention:

Make sure you have understood how Grace Mode works, when temporarily setting up an emergency rescue system (see 4.3 Grace Mode, page 504).

### 5.3.1 Self-managed netfence Gateways

- Reinstall the gateway with PAR file on another hardware. The system will change into grace mode immediately but nevertheless remain fully functional until grace time expires.
- Contact your phion partner to request a box license reissue (for this the original box license file name is needed).
- If VPN clients are connecting to your system request a VPN pool license reissue (for this the original VPN pool license file name is needed).
- If you are using the Avira Virus Scanner service request a reissue of the VIRSCAN .lic-file (for this the original VIRSCAN license file name is needed).
- Replace the invalid licenses with the reissued ones.

### 5.3.2 management centre

- Reinstall the MC with PAR file on another hardware. The system will change into grace mode immediately but nevertheless remain fully functional until grace time expires.
- Contact your phion partner to request an MC box license and Master License reissue (the original Master license file name is needed for license reissue).
- Replace the invalid licenses with the reissued ones.

### Note:

Other license files do not have to be reissued as they bind to the Master License and not to a host-key.

## 6. Protected IP Count Policies

netfence gateways are licensed based on the number of IP addresses accessing the Internet and being protected by the gateway. Especially in today's complex security environments classification of networks as „trusted“ or „untrusted“ is not always feasible, and thus license enforcement needs to rely on a more granular classification.

**Note:**

Please note that in the following the available count algorithms for protected IPs are described. Note the importance of the order. The most important step is No. 2, which simply states that if the counting algorithm does not count in a way you want, you can reverse its direction.

### 6.1 Policy No. 1: No Counting

**NOT** taken into account (neither source nor destination address):

- Source OR destination address is a **Personal VPN** address
- Source AND destination addresses are a **site-to-site tunnel** addresses (**VPN relaying** - star topology)
- Destination is a **Broadcast** or **Multicast** address
- Rule results in a **Block** or **Deny** action

Any communication directed to the services running on the netfence gateway itself as well is not counted:

- Caching proxy
- Mail gateway
- DNS server/forwarder
- DHCP server

### 6.2 Policy No. 2: Rule Explicit

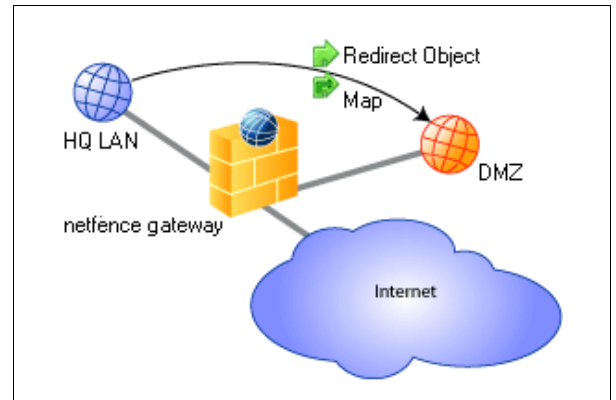
These policies are available within the Advanced Rule Parameters (**Firewall** - 2.3.3 Advanced Rule Parameters, page 154, **Policy**, page 155):

- Source is chosen as protected IP address if the rule explicitly requests it (**Count Source IP**).
- Destination is chosen as protected IP address if the rule explicitly requests it (**Count Destination IP**).
- Source and destination are interchanged if the rule matches on reverse

### 6.3 Policy No. 3: Redirected Destination

- If a redirection of the destination IP is performed in the firewall (Redirect or Map) the translated destination IP address is counted as protected.

Fig. 21-14 Policy for redirected destination



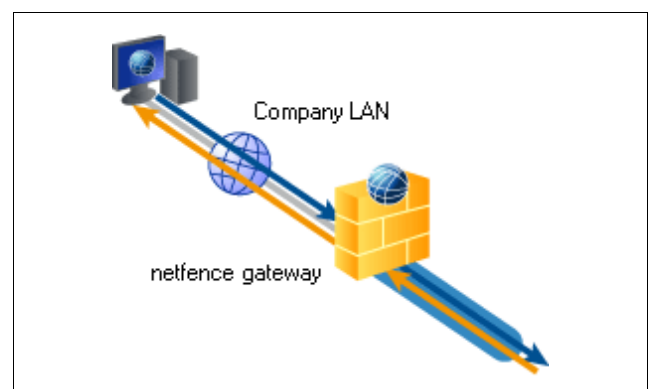
### 6.4 Policy No. 4: Site-to-site Tunnel

- Source is chosen as protected IP address if destination is routed via tunnel
- Destination is chosen as protected IP address if source originates from tunnel

**Note:**

If both options apply neither source nor destination is counted.

Fig. 21-15 Policy for site-to-site tunnels



## 6.5 Policy No. 5: General Case

The protected IP address chosen is either the source or destination address based on a comparison of the classification of incoming and outgoing interfaces.

**Table 21-8** Classification of incoming and outgoing interfaces

		Outgoing			
		Internal	DMZ	Unspecified	External
Incoming	Internal	Src	Src	Src	Src
	DMZ	Dst	Src	Src	Src
	Unspecified	Dst	Dst	Src	Src
	External	Dst	Dst	Dst	Src

**Note:**

The valid preference is the following: Internal - DMZ - Unspecified - External.

# System Information

<b>1.</b>	<b>Overview</b>	
1.1	General .....	512
<b>2.</b>	<b>phion Networking Layer</b>	
2.1	Configuration Files .....	513
2.2	Activation Scripts .....	514
<b>3.</b>	<b>phion Operative Layer</b>	
3.1	Directory Structure .....	515
3.1.1	Static Data .....	515
3.1.2	Dynamic Data .....	515
<b>4.</b>	<b>phion Ports</b>	
4.1	Ports Overview .....	515
<b>5.</b>	<b>List of Default Events</b>	
5.1	General .....	516
5.2	Operational Events .....	517
5.3	Security Events .....	519

# 1. Overview

## 1.1 General

### Attention:

The underlying Linux system is especially designed to serve as a base for the phion firewall. Direct interfering on the command line is not necessary for normal operation. Such operations should be carried out only by authorised personnel with excellent knowledge of Linux systems as well as the special phion implementation.

The phion system basically consists of three parts:

**Table 22-1** Basic overview of the phion Linux system and its licensing concepts.

Layer	Description	Licensing
Basic Linux	Standard Linux system with the modified phion kernel, whose source is of course part of the distribution	<b>Except for the FW engine</b> , mostly under GPL or other Open Source Licenses.
phion networking	Handles all steps dealing with networking	phion Public License. Can be used freely for all purposes except commercial redistribution.
phion operative	Operative phion Software; consists of box services (logging, statistics, control) and server (for example VPN, mail gateway, DNS, ...)	Proprietary phion License

This part of the documentation does not cover the administration of the Basic Linux layer. If you want to learn more about Linux systems in general, we want to refer to a number of excellent books and to a continually growing number of information sites on the internet. However, the phion Linux base does not serve as an operating system for general purpose. It does not include a number of packages which are necessary for most applications. We did not include those packages because of security reasons and we cannot give support for modifying the Linux system on the phion CD.



## 2. phion Networking Layer

The phion networking layer is installed by the `phionetc_box` package. It is called `phionetc_box`, because almost all relevant files live in the directory `/etc/phion`.

The main purpose of the package is to control every part of the system which communicates over the network. Beside the phion software modules there are other packages like `openssh` or `ntp`, which get their configuration and are started by phion scripts.

### 2.1 Configuration Files

There are three configuration files steering and controlling the networking behaviour of the system:

- `/etc/phion/options`
- `/etc/phion/boxadm.conf`
- `/etc/phion/boxnet.conf`

The `options` file is the only one, which is not edited through the GUI `phion.a`.

Template of the `options` file:

**Fig. 22-1** Example - `options` file

```
#####
## Systemwide phion-options
## File is sourced by several start scripts
##

# start networking at all?
BOX_NETWORK="Y"

# Number of retries to bring up all
# devices, sometimes useful for token ring
# devices
NET_RETRY=0

# should the phion subsystem be started ?
PHION_START="Y"

#for some historical reason: should the
# NetDB subsystem be started? #CAUTION:
# Activate only if you know very well what
# you are doing.
NETDB_START="N"

# for advanced Servers
START_ORA="N" #Y/N start ORACLE on BOOT
START_ADABAS="N" #Y/N start ADABAS on BOOT
```

- `#BOX_NETWORK`  
If set to `N`, literally nothing will happen when trying to start networking in the phion way.
- `NET_RETRY`  
Number of entries to establish a network link. This may be useful for unreliable token ring networks.
- `PHION_START`  
If set to `N`, the phion operative layer will not be started at all. Use this if you want to have a box without proprietary phion software running.
- `NETDB_START`  
Only of use if you have a box with a NetDB database system on it.
- `START_ORA` and `START_ADABAS`  
Only of use for a Master configuration server with an Oracle or ADABAS D database.

The `boxadm.conf` file holds all information, which does not need a network restart to be activated. Additionally it holds information for phion box services, too.

An example of an operative configuration file:

**Fig. 22-2** Example - `boxadm.conf` file

```
ACLLIST[] = 10.0.0.8/3 10.0.0.231
ACTBOXSERVICES = y
DNSSERVER[] = 10.1.103.179 10.1.100.204
DOMAIN = m086
ENABLESHOSTS = y
MAINADMIN = n
MASTER[] = 10.1.17.42
RID = 86
RMASTER[] = 10.1.17.42
RPASSWD = $1$someMD5encryption
SPASSWD = $1$someMD5encryption
STARTNTP = y
STATISTICS = y
SYNC = y
TMASTER[] = 10.1.16.21
TZONE = Europe/Vienna
UTC = y

[boxtuning]
FILEMAX = 32768
IDETUNING = y
INODEMAX = 65536
SYSTUNING = n
```

For explanation of the parameters see **Configuration Service** - 5.1 Box Settings - Advanced Configuration, page 100.

**Attention:**

Be extremely cautious in changing these files on the command line.

The boxnet.conf file holds all information which deals with network connections. These are the hostname and the network interfaces, IP addresses and routing information.

Again, let us have a look on a sample file:

**Fig. 22-3** Example - boxnet.conf file

```

HOSTNAME = sega           [addroute_QA]
                          DEST = 10.0.0.244
[addnet_dmz]             DEV = eth0
BIND = n                 FOREIGN = y
CRIT = y                  MASK = 8
DEV = eth1                SRC = 10.0.0.8
IP = 192.168.32.1        TARGET = 192.168.10.0
IPCHAINS = y             TYPE = gw
MASK = 8
PING = y

[addroute_default]
]
DEST =
195.23.11.6
DEV =
FOREIGN = y
MASK = 32
PREF =
REACHIP[] =
SRC =
TARGET = 0.0.0.0
TYPE = gw

[boxnet]
DEV = eth0
IP = 10.0.0.8
MASK = 8

[cards_eeepro]
MOD = eeepro100.o
MODOPTIONS[] =
NUM = 1
TYPE = eth

[cards_realtek]
MOD = rtl18139.o
MODOPTIONS[] =

```

For explanation of the parameters see **Configuration Service** - 5.1 Box Settings - Advanced Configuration, page 100.

## 2.2 Activation Scripts

There are two scripts which are intended to be started from the command line:

➤ /etc/rc.d/init.d/phion (which is actually a link to /etc/phion/rc.d/phionrc)

➤ /etc/phion/bin/activate

All other scripts should not be started on the command line but are invoked by the 2 scripts above.

For more information see User Documentation Command Line Interface.

### 3. phion Operative Layer

#### 3.1 Directory Structure

##### 3.1.1 Static Data

The whole operative data resides in `/opt/phion`.

**Note:**

It is not recommended to change anything below this directory.

The full configuration of a phion box is held under `/opt/phion/config/active`. The configuration files may be modified manually by a phion support engineer or by a specially trained system engineer. If you are not absolutely sure about what you are doing, do not change anything in this place.

##### 3.1.2 Dynamic Data

Log files and statistics data reside in `/var/phion`.

This directory has the following substructure.

- `/var/phion/logs`  
All log files are stored here. You can read it with any editor.

**Attention:**

DO NOT write to it, DO NOT rename it, DO NOT put any files in here. Every manual action can result in strange behaviour of the log GUI.

- `/var/phion/stat`  
Root directory for the statistics data structure. The data files are Berkeley DB files in binary form. They can be viewed with the `showstat` utility (`/opt/phion/bin/`).

**Attention:**

Again: Do NOT change anything in this directories manually.

- `/var/phion/logcache`  
Home of the **Log Access Files** (\*.laf). These are Berkeley DB files for fast access to large log files.
- `/var/phion/run/<module>`  
Services may store operational data in these directories.

Intervention on command line is generally not intended on the phion operative layer. Nevertheless there is one powerful tool to steer the processes. It can be used to gather comprehensive information about system state, routing, servers, processes. Furthermore it is able to start / stop / block / disable servers and box processes. It is called `phionctrl` and resides in `/opt/phion/bin`. For more information see the User Documentation Command Line Interface.

### 4. phion Ports

The following table enlists the ports of a netfence gateway that are required for communication.

#### 4.1 Ports Overview

**Table 22-2** Ports overview

Port	Protocol	Type	Daemon
22	TCP	service	sshd
691 & 443	TCP/UDP	service	vpn
688	TCP	service	firewall
801	TCP	box	controld
802	TCP	box	phibsd
803	TCP	box	logd
805	TCP	box	distd
806	TCP	service	qstatd
807	TCP	box	qstatd
807	UDP	box	cstatd
808	TCP/UDP	box	event
808	TCP/UDP	service	mevent
809	TCP	box	boxconfig
810	TCP	service	masterconfig
811	TCP	service	map/status

**Table 22-2** Ports overview

Port	Protocol	Type	Daemon
814	TCP	service	vpnserv
815	TCP	service	mailgateway
816	TCP	service	DHCP
817	UDP	service	trans7
818	TCP	service	PKI

# 5. List of Default Events

## 5.1 General

Events with identical Event-ID may be generated by multiple processes. Each process, which is responsible for event generation is characterised by an assigned Class and Layer-ID allowing for rough categorisation.

The following Class- and Layer-IDs apply for categorisation:

### Layer IDs:

Table 22-3 Layer-IDs overview

Layer-ID	Layer Title	Description
1	Boot Layer	Events that are generated during system boot-up
2	Box Layer	Events that are generated by a box service (controld, logd, ...)
3	Server/Service Layer	Events that are generated by a server/service process

### Class IDs:

Table 22-4 Class-IDs overview

Class-ID	Class Title	Description
1	Operative	Events that are related to the operative service of the system
2	Resources	Events that are related to system resources
3	Security	Events that are related to system security

Because Class- and Layer-IDs are not attributable to exactly one Class or Layer, Class and Layer descriptions are not included in the list below. They can be learned from the Event Monitor GUI.

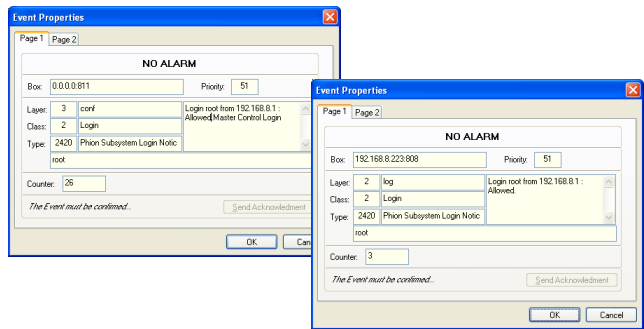
The example below shows a snapshot from the Event Monitor GUI. Entries with identical Event-IDs are highlighted. Have a look at the corresponding different entries in the Layer Desc column.

Fig. 22-4 Event Monitor GUI

Event Time	Event	Desc	Count	from Box	Layer desc	Class desc
2006.10.17/14:44:56	2 event 1 Login 2044 root	Login root from 192.168.8.1 : Login into unlicensed service				
2006.10.17/15:55:11	Authentication Failure Notice	root	1	Phobos_border_10	DAM_gwdb	login
2006.10.18/09:09:47	Phion Subsystem Login Notice	root	3	MC	event	login
2006.10.18/09:09:43	Phion Subsystem Login Notice	root	26	MC	conf	login
2006.10.17/16:58:04	Phion Subsystem Login Notice	root	3	Phobos_border_10	log	login
2006.10.17/16:58:03	Phion Subsystem Login Notice	root	3	Phobos_border_10	boxconfig	login
2006.10.17/16:04:03	Phion Subsystem Login Notice	root	3	Phobos_border_10	phiond	login
2006.10.17/16:04:02	Phion Subsystem Login Notice	root	4	Phobos_border_10	quest	login
2006.10.17/15:58:12	Phion Subsystem Login Notice	root	7	Triton_border_10	phiona	login
2006.10.17/14:49:57	Phion Subsystem Login Notice	root	2	Phobos_border_10	control	login
2006.10.03/15:08:09	Phion Subsystem Login Notice	root	6	Triton_border_10	control	login
2006.10.04/09:04:27	Emergency Server Stop	boardSRV	1	Phobos_border_10	control	controld
2006.10.04/09:04:30	Emergency Server Start	boardSRV	2	Triton_border_10	control	controld
2006.10.17/18:52:49	GRACE Mode Expired	Base License	293	Triton_border_10	control	controld
2006.10.17/18:44:19	GRACE Mode Expired	Base License	298	Phobos_border_10	control	controld
2006.10.17/16:04:02	No Valid License for Service	root	2	Phobos_border_10	box	login
2006.10.17/14:50:50	No Valid License for Service	root	1	Phobos_border_10	boxconfig	login
2006.10.17/14:45:26	No Valid License for Service	root	1	Phobos_border_10	log	login
2006.10.17/14:45:55	No Valid License for Service	root	1	Phobos_border_10	quest	login
2006.10.03/15:08:09	Block Server	boardSRV	1	Triton_border_10	control	control session

A double-click on the event entries framed in red discloses that the first entry with Layer Description **conf** has Layer-ID 3 and Class-ID 2 assigned, whereas the second entry with Layer Description **log** has Layer-ID 2 and Class-ID 2 assigned.

Fig. 22-5 Event Properties windows



The following events are defined on a netfence gateway/management centre:

**Note:** Events flagged with "not available" in the **Relevance** field of the following table are not utilised in netfence gateway 4.2.

## 5.2 Operational Events

Table 22-5 Operational Events overview

Event-ID	Description	Relevance	Severity	Notification	Persistent
10	Disk Space Low	On at least one partition between 70 and 90 % of available disk space are in use. Disk usage is graphically depicted in the Box Control > Resources Tab (see page 36). Low disk space is characterised by a yellow status bar.	Warning	1	yes
11	Disk Space Critical	On at least one partition more than 90 % of available disk space are in use. Disk usage is graphically depicted in the Box Control > Resources Tab (see page 36). Critical disk space is characterised by a red status bar.	Error	1	yes
20	Memory Low	At least 70 or up to 90 % of available memory are in use. Memory usage is graphically depicted in the Box Control > Processes Tab (see page 36). Low memory availability is characterised by a yellow status bar.	Warning	1	yes
21	Memory Critical	More than 90 % of available memory are in use. Memory usage is graphically depicted in the Box Control > Processes Tab (see page 36). Critical memory availability is characterised by a red status bar.	Error	1	yes
30	High System Load	The "Warning" <b>Infrastructure Services - Control - CPU-Load Monitoring - section CPU-Load Warning Thresholds</b> have been exceeded. Thresholds may be configured in Config > Box > Box Services > Control > CPU-LOAD tab (page 118).	Warning	1	yes
31	Excessive System Load	The "Critical" <b>Infrastructure Services - Control - CPU-Load Monitoring - section CPU-Load Warning Thresholds</b> have been exceeded. Thresholds may be configured in Config > Box > Box Services > Control > CPU-LOAD tab (page 118).	Error	1	yes
34	Critical System Condition	The Watchdog repair binary could not be executed flawlessly (see 5.1.10 Watchdog, page 108, and parameter <b>Run S.M.A.R.T.</b> , page 110).	Error	1	yes
48	Device Mismatch		Error	1	no
49	Device Activation Failed	A network interface could not be activated.	Error	1	no
50	Device Down	A network interface has been disabled.	Error	1	yes
51	IP Address Added	The control daemon has added a server IP to the network configuration (for example after manual configuration changes, enabling a server, ...).	Information	1	no
52	IP Address Removed	The control daemon has removed a hitherto existing server IP address from the network configuration (for example after manual configuration changes, blocking or disabling a server, ...).	Information	1	no
54	IP Property Change Failed	not available	Error	1	no
55	Assigned IP Address Changed	An IP address, which has been assigned to the system by an DHCP server has changed.	Information	1	no
56	Duplicate DHCP IP	An DHCP server assigned IP address living on the system has additionally been detected in the network.	Warning	1	no
57	Dyn DNS Update Succeeded	Update of a configured DynDNS account (for example DHCP network or ISDN network configuration) has succeeded/failed.	Information	1	no
58	Dyn DNS Update Failed		Warning	1	no
60	Route Added	A route has been added to the active network configuration, for example because an xDLS connection has been activated or a gateway has become available.	Information	1	no
61	Route Deleted	A route has been deleted from the system, for example because a gateway has become unavailable.	Information	1	no
62	Route Changed	The state or a parameter of a route has changed.	Information	1	no
63	Route Enabled	A route has been activated, because for example a server IP has been added to the configuration.	Information	1	no
64	Route Disabled	A route has been disabled, because for example a server IP has been deleted from the configuration.	Information	1	no
65	Route Reactivated	See also Event-ID 66 Route Deactivated. A gateway route has been reactivated because the initial state has been restored.	Information	1	no
66	Route Deactivated	A gateway route has been deactivated because a former gateway IP has become a local IP on a netfence system. This event might occur on secondary HA boxes, when the server IP of the primary box (former gateway IP for the secondary box) changes to the secondary box after HA takeover.	Information	1	no
70	Flash RAM auto detection	The Storage Architecture option available in the Box Configuration file might have been misconfigured (see <b>Storage Architecture</b> , page 52).	Error	1	no
90	Module Error		Error	1	no
100	Missing Configuration File	A server or service configuration file cannot be retrieved, that means it might have been deleted.	Error	1	no
110	Missing Sysctrl	not available	Error	1	yes
120	Missing Executable	A binary needed at start-up could not be found (for example acpctrl for setting parameters, ...).	Error	1	yes
131	Resource Missing	A resource needed for full system functionality is missing, for example a configured network interface is not available.	Error	1	no
135	Resource Limit Pending	Less than 50 % of maximum command value remain (see 2.2.3.7 SMS Control, <b>Successive Command Maximum</b> , page 58).	Warning	1	yes

Table 22-5 Operational Events overview

Event-ID	Description	Relevance	Severity	Notification	Persistent
136	Resource Limit Exceeded	The number of concurrent connections allowed to connect to a service or a configured maximum limit has reached a critical value or has been exceeded (for example, see <b>Mail Gateway</b> - 3.2.7 Reporting, page 256, <b>Parallel Connection Limit</b> , page 256, <b>Spooling Limit</b> , page 256, and <b>DHCP</b> - 2.2.2 Global Settings, page 283, Leases Low / Leases Critical, page 283).  The maximum command counter has been reached or has been exceeded (see 2.2.3.7 SMS Control, <b>Successive Command Maximum</b> , page 58).	Warning	1	yes
150	Corrupted Data File	The utility dstats has identified a corrupt data file ( <b>Configuration Service</b> - 5.2.5 Statistics, page 118).	Error	1	no
400	Time Discontinuity Detected	The statistics daemon has detected a time shift, that means a deviation from former time settings (for example date/time settings have been changed manually, hardware clock settings are wrong after reboot).	Warning	1	no
500	Invalid License	The license that is installed on the system is invalid, for example the Hardware ID of the system does not match with the ID the license has been issued for or the validity period has been exceeded.	Error	1	yes
501	No License Found		Error	1	yes
505	License Limit Exceeded	The license limit of IPs protected by the firewall has been exceeded ( <b>Firewall</b> - 6.5.2 Protected IPs, page 176).	Error	1	no
510	Invalid Argument	The Watchdog repair binary could not be executed flawlessly (see 5.1.10 Watchdog, page 108).	Error	1	no
600	HA Partner Unreachable	Connectivity between a netfence gateway and its high availability partner is disrupted.	Error	1	yes
610	Reporter SSH Host Key Mismatch	This event is only applicable on management centres. Statistics transfer from MC to a netfence reporter has failed because the SSH Host Keys did not match. Refer to the netfence reporter documentation (available in a separate document) for details.	Error	1	yes
620	Box Unreachable	Connectivity between MC and one of its administered boxes is disrupted. This event is only generated on the MC.	Warning	1	yes
622	Box Reachable Again	Connectivity between MC and one of its administered boxes has been restored. This event is only generated on the MC.	Information	1	no
666	Process Core Found	The core-search utility has found a core dump of a netfence process and has moved it to <code>/var/phion/crash</code> .	Warning	1	no
2000	Start Server	A server has been started either by the system or manually.	Information	1	no
2001	Start Service	A service has been started either by the system or manually.	Information	1	no
2002	Start Box Service	A box-service has been started either by the system or manually.	Information	1	no
2010	Stop Server	A server has been stopped either by the system or manually.	Information	1	no
2011	Stop Service	A service has been stopped either by the system or manually.	Information	1	no
2012	Stop Box Service	A box-service has been stopped either by the system or manually.	Information	1	no
2020	Restart Server	A server has been restarted either by the system or manually.	Information	1	no
2021	Restart Service	A service has been restarted either by the system or manually.	Information	1	no
2022	Restart Box Service	A box-service has been restarted either by the system or manually.	Information	1	no
2030	Block Server	A server has been blocked manually.	Warning	1	no
2031	Block Service	A service has been blocked manually.	Warning	1	no
2032	Block Box Service	A box-service has been blocked manually.	Warning	1	no
2040	Deactivate Server		Warning	1	no
2041	Deactivate Service		Warning	1	no
2042	Deactivate Box Service		Warning	1	no
2044	No Valid License for Service		Warning	1	yes
2045	Entering GRACE Mode	A system with a formerly valid license has changed into grace mode, either because the host-key the license has been issued for does not match with the system's host key or because the MC-administered box could not validate its license with the MC.	Warning	1	no
2046	Entering DEMO Mode	The system has been installed without importing a valid license or a valid box license has been removed from it.	Error	1	no
2047	GRACE Mode Expired	Grace mode has expired and all services have been deactivated.	Error	1	no
2050	Reactivate Server		Warning	1	no
2051	Reactivate Service		Warning	1	no
2052	Reactivate Box Service		Warning	1	no
2054	Subprocess Kill Requested	A sub-process has been killed manually.	Information	1	no
2056	Connection Kill Requested		Information	1	no
2058	Session Kill Requested		Information	1	no
2060	Emergency Server Start	A server has started because the HA partner is not available.	Warning	1	no
2061	Emergency Server Stop	A server has stopped because the HA partner server is in state active.	Warning	1	no
2070	Daemon Startup Failed	A daemon's startup/shutdown has failed/succeeded. The daemon responsible for the event will be included in the event message. Eventing notifications may be configured per daemon (for example NTPd - see page 57, SSH - see page 106). They will only be generated for controlled startup/shutdown sequences and not for manual process terminations.	Warning	1	no
2071	Daemon Startup Succeeded		Information	1	no
2072	Daemon Shutdown Failed		Information	1	no
2073	Daemon Shutdown Succeeded		Information	1	no
2080	Time Synchronisation Failed	NTP sync with the configured NTP server has failed. NTP synchronisation settings are defined in Config > Box > Settings > TIME/NTP tab (see page 56).	Warning	1	no



Table 22-5 Operational Events overview

Event-ID	Description	Relevance	Severity	Notification	Persistent
2081	Time Synchronisation Succeeded	NTP sync with the configured NTP server has succeeded. NTP synchronisation settings are defined in Config > Box > Settings > TIME/NTP tab (see page 56).	Information	1	no
2082	Time Synchronisation Denied	NTP sync with the configured NTP server has been denied. NTP synchronisation settings are defined in Config > Box > Settings > TIME/NTP tab (see page 56).	Error	1	no
2102	Network Restart Requested	A network restart has been triggered manually using phion.a.	Information	1	no
2103	Activate New Network Configuration	A new network configuration has been activated manually using phion.a.	Information	1	no
2104	Phion Subsystem Start	The phion Subsystem (network and phion processes) has been started.	Information	1	no
2105	Phion Subsystem Stop	The phion Subsystem (network and phion processes) has been stopped.	Information	1	no
2120	Mail DSN Message Sent	A DSN ( <b>D</b> elivery <b>S</b> tatus <b>N</b> otification) message has been generated and sent by the mail gateway (for example due to undeliverable mail). Further DSN generation conditions are configurable in the Limits configuration section of the mail gateway ( <b>Mail Gateway</b> - 3.2.6 Limits, page 255).	Information	1	no
2210	Network Subsystem Restart	The network subsystem (routes, IP addresses, network interface drivers) has been restarted.	Information	1	no
2212	Unclean Network Subsystem Activation	An error has occurred during network subsystem activation.	Warning	1	no
2220	Network Subsystem Shutdown	The network subsystem (routes, IP addresses, network interface drivers) has been shut down.	Information	1	no
2222	Unclean Network Subsystem Shutdown	An error has occurred during network subsystem shutdown.	Information	1	no
2230	Network Subsystem Check	The network subsystem configuration has been checked for consistency.	Information	1	no
2232	Network Subsystem Check	The network subsystem configuration has been checked for consistency.	Information	1	no
2234	Network Subsystem Check Failed	An error has been discovered during network subsystem configuration check.	Warning	1	no
2240	Link Activation Failed	Activation of a dynamic link (for example xDSL, UMTS, DHCP) has failed. The reason for activation failure is provided in the event message.	Error	1	no
2242	Sublink Activation Failed		Error	1	no
2250	PCMCIA Bus Reset	Resetting the PCMCIA bus to recover from potential modem lockup by power cycling it.	Error	1	no
2380	Flawed Configuration Data Activation	The rule file containing the domain settings of the mail gateway service is either missing or a corrupt rule file has been loaded. This event is only reported when parameter <b>Bad Rulefile Loaded</b> (see page 256) is set to <b>yes</b> .	Error	1	no
2500	FW Forwarding Loop Suppressed	These events are triggered when the FW server IP is addressed directly and no proper rule set is defined. They are only generated when parameter settings <b>Local Redirection / Local Routing Loop</b> , see page 130 are set to <b>yes</b> .	Information	1	yes
2502	FW Local Redirection Suppressed		Information	1	yes
2511	FW Worker Limit Exceeded		Error	1	yes
3000	VPN Server Tunnel Terminated	A VPN tunnel has been terminated manually.	Information	1	no
3001	VPN Alternative Tunnel Activated	A VPN alternative tunnel will be activated, when the active partner of the tunnel changes his Bind-IP address (for example provider failure).	Warning	1	no
3002	VPN Server Tunnel Activated	A VPN Site-to-Site tunnel has been activated.	Information	1	no

### 5.3 Security Events

Table 22-6 Security Events overview

Event-ID	Description	Relevance	Severity	Notification	Persistent
53	Duplicate IP Detected	An IP address living on the system has additionally been detected in the network.	Warning	2	yes
140	Mail Size Limit Exceeded	The size of an e-mail has exceeded the configured limit (see parameter <b>Mail Data Size Limit</b> , page 256). This event is only reported when parameter <b>Mail Data Size Limit</b> (see page 256) is set to <b>yes</b> .	Notice	2	no
300	User ID (UID) Invalid		Security	3	no
304	Reserved Login ID Used		Security	3	no
2099	CTRL-ALT-DEL	A system reboot has been triggered manually at the physical console by pressing the keys CTRL-ALT-DEL simultaneously.	Warning	2	no
2100	Reboot Requested	A system reboot has been triggered manually using phion.a.	Warning	2	no
2101	System Halt Requested	A system shutdown has been triggered manually.	Warning	2	no
2400	Config Node Change Notice	A configuration file has been edited in the management centre configuration tree. "Config node change" events are only reported if event notification has been configured for configuration file changes ( <b>phion management centre</b> - 6.7 Defining Node Properties, page 420). The following events apply: ↗ <b>Normal Event</b> - Event-ID 2400 ↗ <b>Notice Event</b> - Event-ID 2401 ↗ <b>Alert Event</b> - Event-ID 2402	Notice	2	no
2401	Config Node Change Warning		Warning	2	no
2402	Config Node Change Alert		Security	3	no

Table 22-6 Security Events overview

Event-ID	Description	Relevance	Severity	Notification	Persistent
2420	Phion Subsystem Login Notice	An application has been granted administrative access to the system. phion applications generate "phion Subsystem Login" notifications every time a user has successfully logged into an application that interacts with the graphical administration tool phion.a (for example control, event, statistics, config). The severity level for notifications regarding access to box services is configurable in Config > Box > Box Misc. > Access Notification tab, see page 105; Notifications for other services may be customised per service (list 3-92, page 98).	Notice	2	no
2421	Phion Subsystem Login Warning		Warning	2	no
2422	Phion Subsystem Login Alert		Security	3	no
2510	FW Global Connection Limit Exceeded	The number of total sessions allowed for a request has been exceeded (see <b>Max. Session Slots</b> , page 127).	Security	3	yes
2600	DHCP Lease Deleted	not available	Notice	2	no
3011	CRL Collection Failed	Collection of the Certificate Revocation List (CRL) has failed. Paths to CRLs are defined in the VPN settings > Root Certificates tab > Certificate Revocation tab (VPN - 2.3.3 Root Certificates Tab, page 208). Polling for CRL retrieval is defined through parameter <b>CRL Poll Time</b> (see page 207).	Security	3	no
3012	VPN Client Version	not available	Warning	2	no
3013	Antivir Pattern Update Failed	Update to the recent AntiVirus definitions has not succeeded.	Security	3	no
4000	FW Port Scan Detected	The number of blocked requests has exceeded the <b>Port Scan Threshold</b> within the configured <b>Port Scan Detection Interval</b> . Limit values can be customised in the Firewall Settings > Reporting tab (see page 129).	Notice	2	no
4002	FW Flood Ping Protection Activated	The <b>Min Delay</b> time for pinging defined in a Firewall Service Object (Firewall > Service Objects > <b>Min Delay</b> , see page 144) has been under-run and the connection has thus been blocked by the FW.	Warning	2	no
4004	FW Activating Perimeter Defence (inbound mode)	The <b>Inbound Threshold (%)</b> value specified in the Local Firewall settings (see page 128) has been exceeded. This event is only reported when parameter <b>Pending Accepts Critical</b> (see page 130) is set to <b>yes</b> .	Security	3	no
4006	FW Pending TCP Connection Limit Reached	The number of pending TCP sessions per source IP exceeds the allowed maximum. Requests initiating further pending sessions will be blocked. The threshold is configurable in the Firewall Forwarding Settings > Firewall tab (see page 131, parameter <b>Max. Pending Forward Accepts/Src</b> ). This event is only reported when parameter <b>Accept Limit Exceeded</b> (see page 129) is set to <b>yes</b> .	Security	3	no
4008	FW UDP Connection per Source Limit Exceeded	The maximum number of UDP sessions per source IP has been exceeded. The thresholds can be configured in the Local Firewall Settings > Session Limits tab (parameter <b>Max Local-In UDP/Src</b> , see page 127) and in the Firewall Forwarding Settings > Firewall tab (parameter <b>Max. Forwarding UDP/Src</b> , see page 131). This event is only reported when parameter <b>UDP/Src Limit Exceeded</b> (see page 129) is set to <b>yes</b> .	Warning	2	no
4009	FW UDP Connection Limit Exceeded	The maximum number of UDP sessions has been exceeded. The threshold can be configured in the Local Firewall Settings > Session Limits tab (parameter <b>Max UDP (%)</b> , see page 127) This event is only reported when parameter <b>UDP/Src Limit Exceeded</b> (see page 129) is set to <b>yes</b> .	Security	3	no
4010	FW Oversized SYN Packet Dumped	An oversized SYN packet has been dropped by the firewall (see <b>Oversized SYN Packet</b> , page 130). This event is only reported when parameter <b>Oversized SYN Packet</b> (see page 130) is set to <b>yes</b> .	Notice	2	no
4012	FW Large ICMP Packet Dumped	An ICMP-ECHO packet larger than the configured <b>Max Ping Size</b> (see page 144) has been dropped by the firewall. This event is only reported when parameter <b>Large ICMP Packet</b> (see page 130) is set to <b>yes</b> .	Notice	2	no
4014	FW IP Spoofing Attempt Detected	An IP spoofing attempt has been discovered. This event is only reported when parameter <b>IP Spoofing</b> (see page 130) is set to <b>yes</b> .	Notice	2	no
4015	FW Potential IP Spoofing Attempt	A SYN flooding attack has been identified (see 2.3.3.3 Accept Policies, page 157). This event is only reported when parameter <b>IP Spoofing</b> (see page 130) is set to <b>yes</b> .	Notice	2	no
4016	FW Rule Connection Limit Exceeded	The maximum number of concurrent connections allowed per rule has been exceeded. The maximum value is defined by parameter <b>Max. Number of Sessions</b> (see page 155). This event is only reported when parameter <b>Rule Limit Exceeded</b> (see page 129) is set to <b>yes</b> .	Warning	2	no
4018	FW Rule Connection per Source Limit Exceeded	The maximum number of concurrent connections allowed per rule and source has been exceeded. The maximum value is defined by parameter <b>Max. Number of Sessions per Source</b> (see page 155). This event is only reported when parameter <b>Source/Rule Limit Exceeded</b> (see page 129) is set to <b>yes</b> .	Warning	2	no
4020	FW Rule Notice	A firewall rule equipped with event generation has been processed. The severity level of the generated event is defined by the rule (see parameter <b>Eventing</b> , page 155).	Notice	2	no
4021	FW Rule Warning		Warning	2	no
4022	FW Rule Alert		Security	3	no
4024	FW Global Connection per Source Limit Exceeded	The maximum number of concurrent connections allowed per source has been exceeded. The maximum value is defined by parameters <b>Max Local-In Session/Src</b> in the Local Firewall Settings (see page 127) and <b>Max. Forwarding Session/Src</b> in the Forwarding Firewall Settings (see page 131). This event is only reported when parameter <b>Session/Src Limit Exceeded</b> (see page 129) is set to <b>yes</b> .	Warning	2	no
4026	FW ICMP-ECHO Connection per Source Limit Exceeded	The maximum number of concurrent ICMP-ECHO connections allowed per source has been exceeded. The maximum value is defined by parameters <b>Max Local-In Echo/Src</b> in the Local Firewall Settings (see page 127) and <b>Max. Forwarding Echo/Src</b> in the Forwarding Firewall Settings (see page 131). This event is only reported when parameter <b>Echo/Src Limit Exceeded</b> (see page 129) is set to <b>yes</b> .	Warning	2	no

Table 22-6 Security Events overview

Event-ID	Description	Relevance	Severity	Notification	Persistent
4027	FW ICMP-ECHO Connection Limit Exceeded	The maximum number of ICMP-ECHO connections has been exceeded. The threshold can be configured in the Local Firewall Settings > Session Limits tab (parameter <b>Max Echo (%)</b> , see page 127) This event is only reported when parameter <b>Echo Limit Exceeded</b> (see page 129) is set to <b>yes</b> .	Warning	2	no
4028	FW OTHER-IP Connection per Source Limit Exceeded	The maximum number of concurrent OTHER-IP connections (all IP protocols except TCP, UDP and ICMP) allowed per source has been exceeded. The maximum value is defined by parameters <b>Max Local-In Other/Src</b> in the Local Firewall Settings (see page 128) and <b>Max. Forwarding Other/Src</b> in the Forwarding Firewall Settings (see page 131). This event is only reported when parameter <b>Other/Src Limit Exceeded</b> (see page 130) is set to <b>yes</b> .	Warning	2	no
4029	FW OTHER-IP Session Limit Exceeded	The maximum number of OTHER-IP sessions (all IP protocols except TCP, UDP and ICMP) has been exceeded. The threshold can be configured in the Local Firewall Settings > Session Limits tab (parameter <b>Max Other (%)</b> , see page 127). This event is only reported when parameter <b>Other Limit Exceeded</b> (see page 130) is set to <b>yes</b> .	Warning	2	no
4050	FW ARP MAC Address Changed	not available	Notice	2	no
4051	FW ARP Ambiguous Duplicate Reply	not available	Notice	2	no
4052	FW ARP Request Device Mismatch	not available	Notice	2	no
4053	FW ARP Reverse Routing Interface Mismatch	not available	Notice	2	no
4100	User Unknown	A system login has been attempted with an unknown login ID (see Config > Box > Box Misc. > Access Notification tab, page 105, and List 3-92 Service Configuration - Notification - section Access Notification, page 98).	Warning	2	no
4110	Authentication Failure Notice	A login attempt with a valid login ID has failed (see Config > Box > Box Misc. > Access Notification tab, page 105, and List 3-92 Service Configuration - Notification - section Access Notification, page 98).	Notice	2	no
4111	Authentication Failure Warning	A login attempt with a valid login ID has failed the second time (see Config > Box > Box Misc. > Access Notification tab, page 105, and List 3-92 Service Configuration - Notification - section Access Notification, page 98).  The ACL does not match (see 2.2.3.7 SMS Control, <b>Allowed Phone Numbers</b> , page 58).	Warning	2	no
4112	Authentication Failure Alert	A login attempt with a valid login ID has failed at least three times (see Config > Box > Box Misc. > Access Notification tab, page 105, and List 3-92 Service Configuration - Notification - section Access Notification, page 98).  Password authentication failure and/or unsuccessful command match (see 2.2.3.7 SMS Control, section <b>Administrative Settings - SMS Control - section Command Codes</b> , page 58).	Security	3	no
4120	Session Opened Notice		Notice	2	no
4121	Session Opened Warning	A traced user has initiated an SSH connection ( <b>SSH Gateway</b> - 1. SSH Proxy, page 364, Recorded Users, page 366).	Warning	2	no
4122	Session Opened Alert		Security	3	no
4124	Remote Command Execution Notice	Remote command execution has been triggered remotely by the management centre (in MC Control Centre > Box Execution tab) or by an authorised user. Note that copying files with SCP also generates this event.	Notice	2	no
4125	Remote Command Execution Warning		Warning	2	no
4126	Remote Command Execution Alert	Successful authentication and command is accepted (see 2.2.3.7 SMS Control, section <b>Administrative Settings - SMS Control - section Command Codes</b> , page 58).	Security	3	no
4130	System Login Notice	The quality of these event notifications is determined by the settings made in Config > Box > Box Misc. > Access Notification tab, see page 105. The following notifications apply with default settings: Notice (not assigned), Warning (successful SSH and remote SSH login), Alert (successful console login). Login failure triggers events 4110, 4111, and 4112 (see above).	Notice	2	no
4131	System Login Warning		Warning	2	no
4132	System Login Alert		Security	3	no
4160	Log Data Deleted		Notice	2	no
4162	Statistics Data Deleted		Notice	2	no
4163	Statistics Collection Failed		Notice	2	no
4200	CTRL-ALT-DEL		Warning	2	no
4202	System Reboot	The system has been rebooted. Manual reboot will trigger this event as well as the Watchdog repair binary (see 5.1.10 Watchdog, page 108).	Warning	2	no
4204	System Shutdown	The system has been shut down.	Warning	2	no
4206	Runlevel Changed	The runlevel of the operating system has changed. Runlevels change during system boot.	Notice	2	no
4210	Single User Mode	The system has been booted in Single User mode using the boot option "phion single".	Warning	2	no
4212	Problems During Bootup		Warning	2	no
4214	Incomplete Previous Boot	The previous system bootup could not be completed.	Warning	2	no
4220	System Boot	The system is starting the bootup process.	Notice	2	no
4222	Emergency System Boot		Warning	2	no
4240	Bootloader Configuration Change		Notice	2	no
4242	Two Phase Kernel Update		Notice	2	no
4244	Automatic Kernel Update		Notice	2	no



Table 22-6 Security Events overview

Event-ID	Description	Relevance	Severity	Notification	Persistent
4246	Kernel Update Rejected		Warning	2	no
4248	Custom Bootloader or Kernel Update		Notice	2	no
4250	Bootloader Test Activation Failure		Notice	2	no
4252	Bootloader Activation Failed		Warning	2	no
4254	Bootloader Disaster Recovery		Warning	2	no
4256	Bootloader Reconfigured		Notice	2	no
4258	Kernel Update		Warning	2	no
4260	Pending Kernel Update		Warning	2	no
4261	Activate Pending Kernel Update		Warning	2	no
4262	Bootloader Reconfiguration Failed		Warning	2	no
4264	Kernel Update Failed		Warning	2	no
4300	Empty ACL Encountered		Security	3	no
4302	Overlong ACL Encountered		Security	3	no
4304	Password Update Failure		Security	3	no
4306	Password Updated	The password of user 'phion' or 'root' has changed.	Warning	2	no
4307	Key Updated	The root public RSA key has changed.	Warning	2	no
4400	Release Update Triggered	Software update has been triggered manually.	Notice	2	no
4402	Subsystem Release Update Succeeded		Notice	2	no
4404	Subsystem Release Update Cancelled	A software update has been cancelled.	Notice	2	no
4406	Subsystem Release Update Aborted		Warning	2	no
4408	Release Update Failed		Security	3	no
4410	Release Inconsistencies Detected	Incorrect RPM packages have been installed, for example hotfixes intended for another netfence release version, or phion files have been modified, for example by manually editing a phion script.	Warning	2	no
4412	Active Kernel not in RPM-DB	The Linux Kernel in use has not been added to the RPM database.	Notice	2	no
4500	Mail Data Discarded	An e-mail has been discarded from the mail queue ( <b>Mail Gateway</b> - 5.3 Mail Queue Tab, page 263, <b>Discard Mail</b> , page 264. This event is only reported when parameter <b>Admin Reception Commands</b> (see page 256) is set to <b>yes</b> .	Notice	2	no
4504	Mail Operation Changed	An e-mail has been allowed or blocked manually ( <b>Mail Gateway</b> - 5.6 Processes Tab, page 266, <b>Allow Mail Reception/Block Mail Reception</b> , page 266. This event is only reported when parameter <b>Admin Discard Mail Cmd</b> (see page 256) is set to <b>yes</b> .	Notice	2	no
4506	Mail Delivery Refused	E-mail delivery to a banned recipient has been refused. This event is only reported when parameter <b>Recipient Dropped</b> (see page 256) is set to <b>yes</b> .	Notice	2	no
4508	Mail Relaying Denied	Relaying of an e-mail has been denied according to content filter configuration. This event is only reported when parameter <b>Mail Denied</b> (see page 256) is set to <b>yes</b> .	Notice	2	no
4512	Mail Rule Notice	These are customised events with corresponding customised descriptions, which are triggered when Action type <b>Event</b> ( <b>Mail Gateway</b> - 3.2.4 Advanced Setup, page 250, Expert Settings section, page 251) is used in the Expert Settings configuration area. Event-ID <b>0</b> = Severity Notice Event-ID <b>1</b> = Severity Warning Event-ID <b>2</b> = Severity Security Events will only be reported when parameter <b>User Defined Rule Event</b> (see page 256) is set to <b>yes</b> (default).	Notice	2	no
4513	Mail Rule Warning		Warning	2	no
4514	Mail Rule Alert		Security	3	no
4600	Attempted Illegal Assignment		Security	3	no

# Appendix

<b>1.</b>	<b>How to ...</b> .....	<b>524</b>
1.1	How to gather Group Information .....	524
1.2	How to tune netfence for High Performance Environments .....	525
1.3	How to set up for SCEP .....	526
1.4	How to mount USB Flashdisk on phion netfence .....	527
1.5	How to set up a Generic VPN Tunnel (phion M Box to VPN Server) .....	528
1.6	How to make a phion M appliance centrally manageable .....	529
<b>2.</b>	<b>Parameter Defaults for netfence Appliances</b> .....	<b>530</b>
<b>3.</b>	<b>Index of Dialogue Sections</b> .....	<b>550</b>
<b>4.</b>	<b>Index of Dialogue Tabs</b> .....	<b>554</b>
<b>5.</b>	<b>Parameter List Directory</b> .....	<b>557</b>
<b>6.</b>	<b>Index of Configuration Parameters</b> .....	<b>566</b>
<b>7.</b>	<b>Table Directory</b> .....	<b>584</b>
<b>8.</b>	<b>Figure Directory</b> .....	<b>590</b>
<b>9.</b>	<b>Glossary</b> .....	<b>598</b>
<b>10.</b>	<b>Log of Changes</b> .....	<b>603</b>
<b>11.</b>	<b>phion Lizenzbedingungen / phion License Conditions</b> .....	<b>605</b>

# 1. How to ...



## 1.1 How to gather Group Information

Group information is/may be required for the following services:

- FTP - see **FTP Gateway**, page 351
- Proventia Web Filter - see **Proxy** - 3. ISS Proventia Web Filter, page 342
- VPN - see **VPN**, page 199
- Firewall Authentication - see **Firewall** - 10. Firewall Authentication, page 188

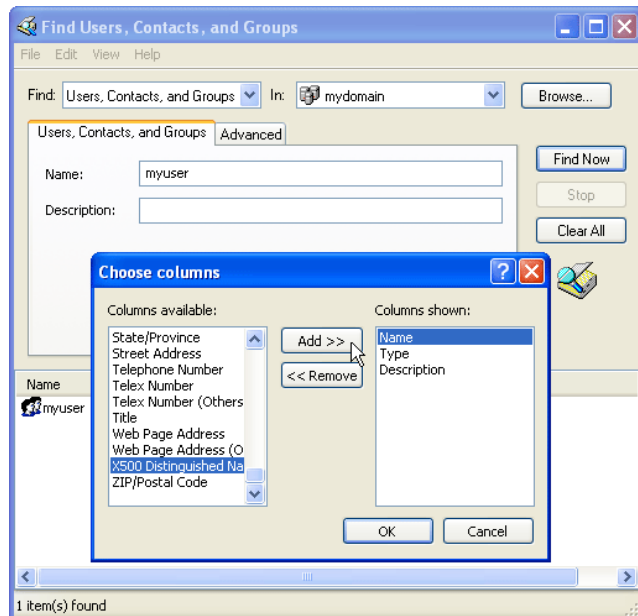
The **distinguished name** containing the group information is needed for external authentication using MSAD and LDAP.

### 1.1.1 MSAD

Open the management console by selecting  > **My Network Places** >  **Search Active Directory**. Select the searching domain. Enter the name of the user you are searching for and click the **Find Now** button.

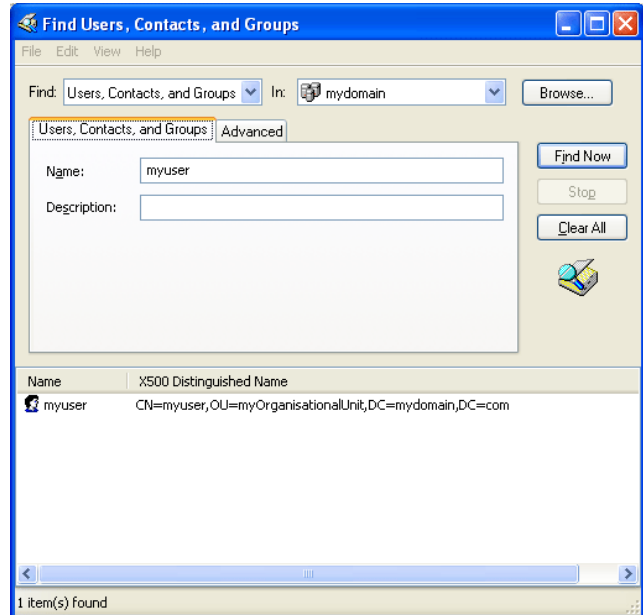
After you have found the user, enable the **X500 Distinguished Name** column in the view. Therefore, select **View** > **Choose columns ...** from the menu, select **X500 Distinguished Name** and click the **Add >>** button (figure 23-1).

Fig. 23-1 Adding a new column to the view



The search result now displays the **Distinguished Name**.

Fig. 23-2 Search result containing group information

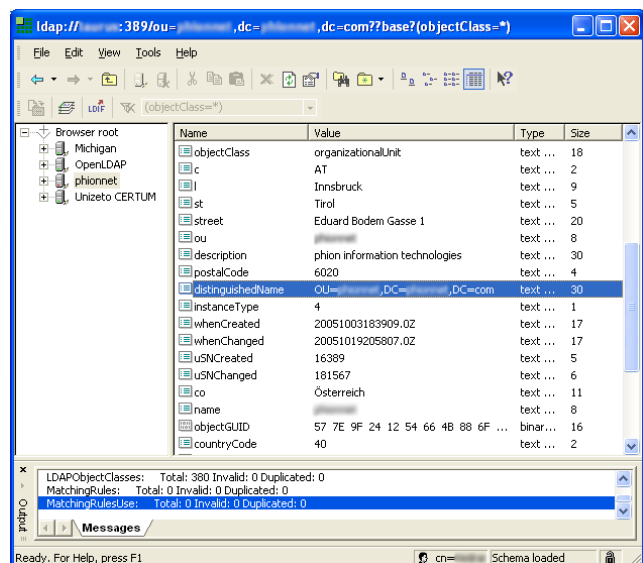


### 1.1.2 LDAP

You may gather distinguished names for the authentication scheme LDAP with an arbitrary LDAP browser.

Open this LDAP browser and connect to your domain controller to retrieve the distinguished name (figure 23-3).

Fig. 23-3 LDAP browser with marked distinguished name





## 1.2 How to tune netfence for High Performance Environments

### 1.2.1 General

In certain high load environments where

- over 50.000 concurrent sessions persist or
- where more than 5000 new sessions are generated per second
- in combination with a multi gigabit forwarding traffic flow

some tuning may be necessary to achieve an optimal outcome.

**Note:**

For an optimal result, install netfence version 4.0.3 or higher.

### 1.2.2 Procedures

**Note:**

These settings have to be made by experts.

#### 1.2.2.1 Interrupt Throttle Rate

If your hardware uses Intel Gigabit NICs the interrupt rate should be throttled to 10.000 interrupts. Otherwise the kernel tries to fetch packets from the NIC too often which slows down overall performance. This can be done using the module parameter:

```
InterruptThrottleRate=10000 for one NIC and
InterruptThrottleRate=10000,10000 for two NICs.
```

Add as much additional ,10000 parameters to reflect the total number of Intel Gigabit NICs in your system.

Module parameters can be set in **Box > Network > Interfaces > Network Interface Cards > Driver Options.**

#### 1.2.2.2 Processing Priority for "ksoftirqd"

Under heavy load, some packets cannot be handled via the hardware interrupt and are treated by the ksoftirqd daemon. The default priority is set in a way to treat other processes with a higher priority to ksoftirqd. To avoid this, run the following command:

```
renice -19 -p $(ps ax | grep ksoftirqd | grep
-v grep | awk '{print $1}')
```

This will set the priority to -19.

To make this configuration permanent, add the command to a box network **Special Needs** script (**Box > Network > Special Needs**) (**Configuration Service - 2.2.5.11 Special Needs**, page 80).

#### 1.2.2.3 NIC Receive Buffers

Increasing the number of receive buffer improves the performance when packet bursts occur.

The default value for Intel Gigabit NIC is 256. It can be increased by running the following command:

```
ethtool -g eth3 (Show settings)
ethtool -G eth3 rx 1024 (Set Value)
```

**Note:**

This is a per interface setting and has to be applied for each interface.

To make this configuration permanent, add the command to a box network **Special Needs** script (**Box > Network > Special Needs**) (**Configuration Service - 2.2.5.11 Special Needs**, page 80).

#### 1.2.2.4 NOATIME Mount

In a default netfence installation, file access times are tracked when a file is accessed. This issues a write command even if a file is opened for reading only and so additional I/O load is created. To avoid this, mount the partitions with the mount option noatime.

Edit the file `/etc/fstab` and replace the value `defaults` in the 4th column with `noatime` for the `/`, the `/boot` and the `/phion0` partition.

**Note:**

This modification will not be saved in the PAR file. After a new installation edit the `fstab` file again.

The partitions should be then defined like in this example:

```
LABEL=/ / ext3 noatime 1 1
LABEL=/boot /boot ext3 noatime 1 1
```

This is a permanent setting and will be preserved.

#### 1.2.2.5 ACPF Kernel Timer Mode

This timer is an interruptible kernel thread.

This way, for the case of many (more than 3000) concurrent sessions the timer handling is spread in smaller portions which may be interrupted by the packet handling soft-IRQs. The old timer model caused rather long (3 ms) blackout periods for soft-IRQs.

To check if you may take advantage of the new timer, look at the profiling information of the ACPF module:

```
# cat /proc/net/acpf_prof
      Id CPU Usage [%] count time[nsec]
  acpf_input      0.0      0      0
  acpf_output     0.0      0      0
  acpf_timer      0.0     10     6540
```

```
Packets In = 19
Bytes In = 18698
Packets Out = 36
Bytes Out = 37288
Drops = 0
Blocks = 0
Sessions = 2
SessionsNum = 9
creation load = 0
  lo : 0
  pqd0 : 0
  tap0 : 0
  tap1 : 0
  tap2 : 0
  tap3 : 0
```

```
eth0 : 0
```

The line `acpf_timer` displays the time consumed for the sessions to be handled in the `time[nsec]` tab. If the time is longer than one millisecond (= 1000000 ns), you may gain higher performance when you switch to the new timer model.

Run the following commands to switch the timer model:

```
acpfctrl tune timermode 1    (new model)
acpfctrl tune timermode 0    (old model)
```

To make this configuration permanent, add the command to a box network **Special Needs** script (**Box > Network > Special Needs**) (**Configuration Service - 2.2.5.11 Special Needs**, page 80).

### 1.2.2.6 Increasing the Routing Cache

If you have your netfence gateway handling traffic from big networks with a large number of IPs on both sides of the forwarding firewall, increase the routing cache to gain higher performance.

Increase the number of **Max Routing Cache Entries** to 200.000 (**Box > Advanced Configuration > System Settings > Routing Cache**) (**Configuration Service - 5.1.1.3 Routing Cache**, page 100).

#### Note:

200000 is a reference value. You may increase it if necessary.

### 1.2.2.7 Disable CPU Power Savings

To enable highest performance on modern server systems, the CPU power savings have to be turned off. Modify the servers bios settings accordingly.

## 1.2.3 Example

Example for a **Special needs** script (**Box > Network > Special Needs**):

```
renice -19 -p $(ps ax | grep softirqd | grep -v grep | awk '{print $1}')
ethtool -G port1 rx 1024
ethtool -G port2 rx 1024
ethtool -G port3 rx 1024
ethtool -G port4 rx 1024
acpfctrl tune timermode 1
```

## 1.3 How to set up for SCEP

#### Note:

This documentation covers the configuration and usage of the SCEP protocol within the netfence software. Although some configuration steps will be explained on the certificate authority side, the installation and operation of such a server is not part of this documentation.

The goal of SCEP (Simple Certificate Enrollment Protocol) is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology whenever possible. The protocol supports the following operations:

- CA and RA public key distribution
- Certificate enrollment
- Certificate query
- CRL query

The X.509 certificates retrieved through SCEP can be used currently only for site-to-site VPN. TINA and IPSec both support the use of SCEP certificates.

#### Note:

More information about the SCEP protocol can be found at <http://tools.ietf.org/html/draft-nourse-scep-17>.

### 1.3.1 Configuring SCEP

The following steps are required in order to use SCEP on a netfence gateway:

- Configuring the box administrative settings
- Configuring the VPN tunnel settings (with GTI)
- Configuring the VPN tunnel settings (without GTI)

#### 1.3.1.1 Configuring the Box Administrative Settings

- Select **Config > Box > Administrative Settings > SCEP > BOX SCEP Settings**.
- Set the parameter **Enable SCEP** to **yes**.
- Enter the **SCEP Settings** by clicking on **Set...** or **Edit...** See **Configuration Service - 2.2.3.8 SCEP**, page 58 for the description of the available parameters.

## 1.3.2 Configuring the VPN Tunnels

Once SCEP has been setup properly in the box administrative settings, the VPN tunnels can now be configured for using the X.509 certificates retrieved by the SCEP protocol. The use of such certificates is not different than any other certificate. Each tunnel can be configured for using SCEP certificates as an authentication method. This is true for both TINA and IPSec VPN tunnels.

### 1.3.2.1 Using the GTI

#### Importing the Root Certificate

First, the root certificate used by the CA for signing the SCEP certificates must be imported into the GTI.

- Right-click the group window of the GTI and select **GTI Editor Defaults...**
- Go to the **Root Certificates** tab, right-click the main window and import the root certificate(s) via **Import PEM from File...**

#### Selecting the authentication method

Just like any other VPN tunnel setting, the SCEP authentication method can be set at the GTI level, at any GTI group level, or individually per tunnel, under **Identification type**.

- TINA tunnel:
  - Click on the **TINA** tab
  - Set parameter **Accept Identification Type** to **Box SCEP Certificate (CA signed)**
  - Click **OK**
- IPSec tunnel:
  - Click on the **IPSec** tab
  - Set parameter **Identification Type** to **Box SCEP Certificate (CA signed)**
  - Click **OK**

### 1.3.2.2 Using the Legacy Method

#### Importing the root certificate

First, the root certificate used by the CA for signing the SCEP certificates must be imported into the VPN service.

- Go to the desired VPN service in the configuration tree and open the **VPN settings** configuration window.
- Select the **Root Certificates** tab, right-click the main window and import the root certificate(s) via **Import PEM from File...**

#### Selecting the authentication method

For each tunnel configured through the legacy method, the SCEP certificate can be used as authentication method:

- TINA tunnel:
  - Click on the **Identify** tab
  - Set parameter **Identification Type** to **Box SCEP Certificate (CA signed)**
  - Click **OK**
- IPSec tunnel:

- Click on the **Authentication** tab
- Set parameter **Identification Type** to **Box SCEP Certificate (CA signed)**
- Click **OK**

## 1.3.3 Operating SCEP

### 1.3.3.1 Interactive Functions

Unless the SCEP password policy was set to **Enter-Password-at-Box**, no further intervention is required for successful operation after SCEP has been correctly configured.

However, phiona offers a few options to interact with the SCEP subsystem in order to:

- Show SCEP status
- Re-initiate SCEP pending request
- Force SCEP update or retry
- Set the SCEP password

#### Box SCEP Status

The SCEP status and control menu are available via **Control > Box**, when connected to the desired netfence gateway. For the description of the available commands see **Control Centre - 2.6.6 Section BOX SCEP Status**, page 40.

#### Files location

The files hold by the SCEP subsystem are stored on the gateway in the directory `/opt/phion/certs/scep-*`

## 1.4 How to mount USB Flashdisk on phion netfence

### 1.4.1 Procedure

Enter the following commands:

- `mkdir /mnt/usb`
- `mount /dev/sda1 /mnt/usb`

#### Note:

Depending on the controller the command differs:

- IDE, CCISS: ... `/dev/sda1` ...
- SCSI, SAS, SATA, RAID: ... `/dev/sdb1` ...

Now the USB Flashdisk is ready for usage.

Before you remove the USB Flashdisk enter the following command:

- `umount /mnt/usb`

## 1.5 How to set up a Generic VPN Tunnel (phion M Box to VPN Server)

For customers without phion management centre (MC), management via phion.a has been improved in a way that a dedicated remote management tunnel to the peripheral gateway (phion M-series) is now available, even if the appliance is not centrally managed via MC.

### Step 1 Export box public key from phion M box

- Select **Config > Box > Identity** at the phion M box
- In section **Box Certificate** at parameter **Box Private Key** click **Ex/Import**
- Choose **Export Public to Clipboard**

#### Note:

For more information about the **Identity** view see **Configuration Service - 2.2.4 Identity**, page 60.

### Step 2 Configure site to site tunnel at the VPN server partner

- Select **Config > Box > Virtual Servers > <server> > Assigned Services > <vpnservice> > Site to Site** at the VPN server
- Click **Lock**
- Right-click the table and select **New TINA tunnel...**
- Enter a **Name** for the tunnel
- Set the **Direction** to **Passive**
- At tab **Identify** set the **Identification Type** to **Public Key**
- In section **Partner Identification** at parameter **Public Key** click **Ex/Import**
- Choose **Import from Clipboard**
- At parameter **Server Protocol Key** click **Ex/Import**
- Select one of the **New ... RSA Key**
- Click **Ex/Import**
- Choose **Export Public Key to Clipboard**
- At tab **Partner** choose 0.0.0.0/32 as **Peer IP Addresses** or enter the IP address of the single box and click **Add**

- At tab **Partner Networks** enter the VIP address as **Partner Network** and click **Add**

#### Note:

If not routed add the VIP address as ProxyARP.

- Select **Assigned Services > <service> (firewall) > Forwarding Rules > Proxy ARPs**
- Select **New...** from the context menu  
Complete the dialogue **Edit / Create a Proxy ARP Object**
- Be sure that checkbox **Standalone** is selected

- At tab **Local Networks** enter your desired networks and click **Add** (should match the networks at the box)
- At tab **Parameter** choose the desired bind-IP or the device for tunnel as **IP Address or Device used for Tunnel Address** and click **Add**

#### Note:

For more information about TINA tunnels see **VPN - 2.7.1 Configuring TINA Tunnels (Firewall-to-Firewall Tunnels)**, page 220.

### Step 3 Configure Remote Access at the phion M box

- Select **Config > Box > Network** at the single box
- Select the **Advanced View** and click **Management Access**
- Click **Lock**
- In section **Remote Management Tunnel** set parameter **Enable Tunnel** to **yes**
- Enter your **Virtual IP (VIP)**
- Click **Set...** at parameter **Tunnel Details**
- At parameter **VPN Server Key** click **Ex/Import** and choose **Import from Clipboard**
- At parameter **VPN Server** enter the partner vpnservice listen IP as point of entry
- Set parameter **VPN Port** to 691
- At parameter **Remote Networks** enter your desired networks (should match the networks at VPN server)

#### Note:

For more information about the **Management Access** view see **Configuration Service - 2.2.5.4 Management Access**, page 66.

## 1.6 How to make a phion M appliance centrally manageable

### 1.6.1 General

This step-by-step instruction describes the insertion of a readily configured phion M appliance into a phion management centre. If your phion M appliance is not configured yet, you might as well start by creating a phion M appliance from within the MC. Afterwards follow Step 4 to Step 7 respectively.

### 1.6.2 Prerequisites

- phion M appliance is up and running with a valid license
- phion management centre (MC) is up and running with a valid license
- One or multiple valid ADD-MC-M-MGMT license obtained from phion AG (one instance is needed for one phion M appliance)

### 1.6.3 Procedure

#### Step 1 Import licence

- Connect phiona.exe to the phion MC
- Select **Config** > **Multi-Range** > **Global Settings** > **Pool Licenses**
- Click **Lock**
- In the **Product Pool Licenses** section click **Import**, select **Import from File...** and browse for the ADD-MC-M-MGMT license
- Click **Send Changes** > **Activate**

#### Step 2 Create a PAR file

- Connect phiona.exe **directly** to the phion M appliance
- Select **Config**
- Right-click **Box** and select **Create PAR File...**
- Choose an adequate path and name, click **Save**

#### Step 3 Import the PAR File at the MC

- Connect phiona.exe to the phion MC
- Select **Config** > **Multi-Range** > <rangename> > <clustername>
- Right-click **Boxes** and select **Import Box from PAR ...**
- Browse for the previously created **PAR** file
- Insert a **Box Name**.
- Click **Activate** to activate the configuration changes

#### Step 4 Assign an instance

- In the config tree select **Box Licences** from the previously imported box
- Click **Lock**
- In the **License Configuration** section click **Import**, select **Import from Pool Licence** and select the ADD-MC-M-MGMT license
- Click **Send Changes** > **Activate**

#### Step 5 Create a PAR File

- Connect phiona.exe to the phion MC
- Select **Config** > **Multi-Range** > <rangename> > <clustername> > **Boxes**
- Right-click the box and select **Create PAR File for box...**
- Choose an adequate path and name, click **Save**

#### Step 6 Import PAR file

- Connect phiona.exe **directly** to the phion M appliance
- Select **Config**
- Right-click **Box** and select **Restore from PAR File...**
- Browse for the previously created **PAR** file, select it and click **Open**

#### Step 7 Reboot

- Reboot the phion M appliance

## 2. Parameter Defaults for netfence Appliances

### 2.1 netfence industrial

#### 2.1.1 Box Services > Firewall Settings

Table 23-1 netfence industrial - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Threshold [ %]	MAXCRIT	20
Session Limits	Max Echo [ %]	MAXECHO	30
Session Limits	Max Other [ %]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	32
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	128
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	256
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	128
Session Limits	Max UDP [ %]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	512
Memory Settings	Max. Acceptors	NUMACCEPTOR	1024
Memory Settings	Max. ARP Entries	NUMARPC	128
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	32
Memory Settings	Max. Fail Entries	NUMFC	512
Memory Settings	Max. Pending Inbounds	NUMINB	512
Memory Settings	Max. Block Entries	NUMPBC	512
Memory Settings	Max. Plugins	NUMPLUG	1024
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	32
Memory Settings	Max. SIP Calls	NUMSIPCALL	32
Memory Settings	Max. SIP Media	NUMSIPMEDIA	64
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	32
Memory Settings	Max. Session Slots	NUMSLOT	8192
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	1024
Memory Settings	Max. Drop Entries	NUMTBC	512

#### 2.1.2 Box > Tuning

Table 23-2 netfence industrial - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	4096
Arp	ARP Cache Size	NEIGHGC3	8192

#### 2.1.3 Box Services > Statistics

Table 23-3 netfence industrial - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	1

#### 2.1.4 Box Misc > Watchdog

Table 23-4 netfence industrial - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

#### 2.1.5 Box > Network

Table 23-5 netfence industrial - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NF-IND
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	1
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_LAN1]	LAN1
Networks	Devicename	[boxnet\$zdev_LAN2]	LAN2
Networks	Devicename	[boxnet\$zdev_LAN3]	LAN3
Networks	Devicename	[boxnet\$zdev_LAN4]	LAN4

#### 2.1.6 Box > Settings

Table 23-6 netfence industrial - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

#### 2.1.7 Box > Bootloader

Table 23-7 netfence industrial - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)



## 2.2 netfence sintegra XS

### 2.2.1 Box Services > Firewall Settings

**Table 23-8** netfence sintegra XS - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Threshold [%]	MAXCRIT	20
Session Limits	Max Echo [%]	MAXECHO	30
Session Limits	Max Other [%]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	32
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	128
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	256
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	128
Session Limits	Max UDP [%]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	512
Memory Settings	Max. Acceptors	NUMACCEPTOR	1024
Memory Settings	Max. ARP Entries	NUMARPC	128
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	32
Memory Settings	Max. Fail Entries	NUMFC	512
Memory Settings	Max. Pending Inbounds	NUMINB	512
Memory Settings	Max. Block Entries	NUMPBC	512
Memory Settings	Max. Plugins	NUMPLUG	1024
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	32
Memory Settings	Max. SIP Calls	NUMSIPCALL	32
Memory Settings	Max. SIP Media	NUMSIPMEDIA	64
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	32
Memory Settings	Max. Session Slots	NUMSLOT	8192
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	1024
Memory Settings	Max. Drop Entries	NUMTBC	512

### 2.2.2 Box > Tuning

**Table 23-9** netfence sintegra XS - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	4096
Arp	ARP Cache Size	NEIGHGC3	8192

### 2.2.3 Box Services > Statistics

**Table 23-10** netfence sintegra XS - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	1

### 2.2.4 Box Misc > Watchdog

**Table 23-11** netfence sintegra XS - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.3 netfence sintegra S

### 2.3.1 Box Services > Firewall Settings

**Table 23-12** netfence sintegra S - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Threshold [%]	MAXCRIT	20
Session Limits	Max Echo [%]	MAXECHO	30
Session Limits	Max Other [%]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	32
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	128
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	256
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	128
Session Limits	Max UDP [%]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	512
Memory Settings	Max. Acceptors	NUMACCEPTOR	1024
Memory Settings	Max. ARP Entries	NUMARPC	128
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	32
Memory Settings	Max. Fail Entries	NUMFC	512
Memory Settings	Max. Pending Inbounds	NUMINB	512
Memory Settings	Max. Block Entries	NUMPBC	512
Memory Settings	Max. Plugins	NUMPLUG	1024
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	32
Memory Settings	Max. SIP Calls	NUMSIPCALL	32
Memory Settings	Max. SIP Media	NUMSIPMEDIA	64
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	32
Memory Settings	Max. Session Slots	NUMSLOT	8192
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	1024
Memory Settings	Max. Drop Entries	NUMTBC	512

### 2.3.2 Box > Tuning

**Table 23-13** netfence sintegra S - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	4096
Arp	ARP Cache Size	NEIGHGC3	8192

### 2.3.3 Box Services > Statistics

**Table 23-14** netfence sintegra S - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.3.4 Box Misc > Watchdog

**Table 23-15** netfence sintegra S - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.4 netfence M5

### 2.4.1 Box Services > Statistics

**Table 23-16** netfence M5 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Treshold [ %]	MAXCRIT	20
Session Limits	Max Echo [ %]	MAXECHO	5
Session Limits	Max Other [ %]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	64
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	512
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	8192
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	512
Session Limits	Max UDP [ %]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	4096
Memory Settings	Max. Acceptors	NUMACCEPTOR	8192
Memory Settings	Max. ARP Entries	NUMARPC	4096
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	128
Memory Settings	Max. Fail Entries	NUMFC	4096
Memory Settings	Max. Pending Inbounds	NUMINB	16384
Memory Settings	Max. Block Entries	NUMPBC	4096
Memory Settings	Max. Plugins	NUMPLUG	8192
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	128
Memory Settings	Max. SIP Calls	NUMSIPCALL	1024
Memory Settings	Max. SIP Media	NUMSIPMEDIA	2048
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	1024
Memory Settings	Max. Session Slots	NUMSLOT	131072
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	8192
Memory Settings	Max. Drop Entries	NUMTBC	4096

### 2.4.2 Box > Tuning

**Table 23-17** netfence M5 - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	65536
Arp	ARP Cache Size	NEIGHGC3	16384

### 2.4.3 Box Services > Statistics

**Table 23-18** netfence M5 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.4.4 Box Misc > Watchdog

**Table 23-19** netfence M5 - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.5 netfence M3

### 2.5.1 Box Services > Firewall Settings

**Table 23-20** netfence M3 - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Treshold [ %]	MAXCRIT	20
Session Limits	Max Echo [ %]	MAXECHO	5
Session Limits	Max Other [ %]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	64
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	512
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	8192
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	512
Session Limits	Max UDP [ %]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	4096
Memory Settings	Max. Acceptors	NUMACCEPTOR	8192
Memory Settings	Max. ARP Entries	NUMARPC	4096
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	128
Memory Settings	Max. Fail Entries	NUMFC	4096
Memory Settings	Max. Pending Inbounds	NUMINB	16384
Memory Settings	Max. Block Entries	NUMPBC	4096
Memory Settings	Max. Plugins	NUMPLUG	8192
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	128
Memory Settings	Max. SIP Calls	NUMSIPCALL	512
Memory Settings	Max. SIP Media	NUMSIPMEDIA	1024
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	512
Memory Settings	Max. Session Slots	NUMSLOT	131072
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	8192
Memory Settings	Max. Drop Entries	NUMTBC	4096

### 2.5.2 Box > Tuning

**Table 23-21** netfence M3 - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	65536
Arp	ARP Cache Size	NEIGHGC3	8192

### 2.5.3 Box Services > Statistics

**Table 23-22** netfence M3 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.5.4 Box Misc > Watchdog

**Table 23-23** netfence M3 - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.6 netfence M1

### 2.6.1 Box Services > Firewall Settings

Table 23-24 netfence M1 - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Threshold [ %]	MAXCRIT	20
Session Limits	Max Echo [ %]	MAXECHO	5
Session Limits	Max Other [ %]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	64
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	512
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	8192
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	512
Session Limits	Max UDP [ %]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	2048
Memory Settings	Max. Acceptors	NUMACCEPTOR	8192
Memory Settings	Max. ARP Entries	NUMARPC	2048
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	128
Memory Settings	Max. Fail Entries	NUMFC	2048
Memory Settings	Max. Pending Inbounds	NUMINB	8192
Memory Settings	Max. Block Entries	NUMPBC	2048
Memory Settings	Max. Plugins	NUMPLUG	8192
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	128
Memory Settings	Max. SIP Calls	NUMSIPCALL	256
Memory Settings	Max. SIP Media	NUMSIPMEDIA	512
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	256
Memory Settings	Max. Session Slots	NUMSLOT	32768
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	8192
Memory Settings	Max. Drop Entries	NUMTBC	4096

### 2.6.2 Box > Tuning

Table 23-25 netfence M1 - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	32768
Arp	ARP Cache Size	NEIGHGC3	8192

### 2.6.3 Box Services > Statistics

Table 23-26 netfence M1 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.6.4 Box Misc > Watchdog

Table 23-27 netfence M1 - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.7 phion MR

### 2.7.1 Box Services > Firewall Settings

Table 23-28 phion MR - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Threshold [ %]	MAXCRIT	20
Session Limits	Max Echo [ %]	MAXECHO	30
Session Limits	Max Other [ %]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	32
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	128
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	256
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	128
Session Limits	Max UDP [ %]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	512
Memory Settings	Max. Acceptors	NUMACCEPTOR	1024
Memory Settings	Max. ARP Entries	NUMARPC	128
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	32
Memory Settings	Max. Fail Entries	NUMFC	512
Memory Settings	Max. Pending Inbounds	NUMINB	512
Memory Settings	Max. Block Entries	NUMPBC	512
Memory Settings	Max. Plugins	NUMPLUG	1024
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	32
Memory Settings	Max. SIP Calls	NUMSIPCALL	32
Memory Settings	Max. SIP Media	NUMSIPMEDIA	64
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	32
Memory Settings	Max. Session Slots	NUMSLOT	8192
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	1024
Memory Settings	Max. Drop Entries	NUMTBC	512

### 2.7.2 Box > Tuning

Table 23-29 phion MR - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	4096
Arp	ARP Cache Size	NEIGHGC3	8192

### 2.7.3 Box Services > Statistics

Table 23-30 phion MR - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	1

### 2.7.4 Box Misc > Watchdog

Table 23-31 phion MR - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.8 phion M5

### 2.8.1 Box Services > Statistics

Table 23-32 phion M5 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Threshold [ %]	MAXCRIT	20
Session Limits	Max Echo [ %]	MAXECHO	5
Session Limits	Max Other [ %]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	64
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	512
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	8192
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	512
Session Limits	Max UDP [ %]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	4096
Memory Settings	Max. Acceptors	NUMACCEPTOR	8192
Memory Settings	Max. ARP Entries	NUMARPC	4096
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	128
Memory Settings	Max. Fail Entries	NUMFC	4096
Memory Settings	Max. Pending Inbounds	NUMINB	16384
Memory Settings	Max. Block Entries	NUMPBC	4096
Memory Settings	Max. Plugins	NUMPLUG	8192
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	128
Memory Settings	Max. SIP Calls	NUMSIPCALL	1024
Memory Settings	Max. SIP Media	NUMSIPMEDIA	2048
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	1024
Memory Settings	Max. Session Slots	NUMSLOT	131072
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	8192
Memory Settings	Max. Drop Entries	NUMTBC	4096

### 2.8.2 Box > Tuning

Table 23-33 phion M5 - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	65536
Arp	ARP Cache Size	NEIGHGC3	16384

### 2.8.3 Box Services > Statistics

Table 23-34 phion M5 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.8.4 Box Misc > Watchdog

Table 23-35 phion M5 - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.9 phion M3

### 2.9.1 Box Services > Firewall Settings

Table 23-36 phion M3 - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Threshold [ %]	MAXCRIT	20
Session Limits	Max Echo [ %]	MAXECHO	5
Session Limits	Max Other [ %]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	64
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	512
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	8192
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	512
Session Limits	Max UDP [ %]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	4096
Memory Settings	Max. Acceptors	NUMACCEPTOR	8192
Memory Settings	Max. ARP Entries	NUMARPC	4096
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	128
Memory Settings	Max. Fail Entries	NUMFC	4096
Memory Settings	Max. Pending Inbounds	NUMINB	16384
Memory Settings	Max. Block Entries	NUMPBC	4096
Memory Settings	Max. Plugins	NUMPLUG	8192
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	128
Memory Settings	Max. SIP Calls	NUMSIPCALL	512
Memory Settings	Max. SIP Media	NUMSIPMEDIA	1024
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	512
Memory Settings	Max. Session Slots	NUMSLOT	131072
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	8192
Memory Settings	Max. Drop Entries	NUMTBC	4096

### 2.9.2 Box > Tuning

Table 23-37 phion M3 - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	65536
Arp	ARP Cache Size	NEIGHGC3	8192

### 2.9.3 Box Services > Statistics

Table 23-38 phion M3 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.9.4 Box Misc > Watchdog

Table 23-39 phion M3 - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.10 phion M1

### 2.10.1 Box Services > Firewall Settings

Table 23-40 phion M1 - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Treshold [%]	MAXCRIT	20
Session Limits	Max Echo [%]	MAXECHO	5
Session Limits	Max Other [%]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	64
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	512
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	8192
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	512
Session Limits	Max UDP [%]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	2048
Memory Settings	Max. Acceptors	NUMACCEPTOR	8192
Memory Settings	Max. ARP Entries	NUMARPC	2048
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	128
Memory Settings	Max. Fail Entries	NUMFC	2048
Memory Settings	Max. Pending Inbounds	NUMINB	8192
Memory Settings	Max. Block Entries	NUMPBC	2048
Memory Settings	Max. Plugins	NUMPLUG	8192
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	128
Memory Settings	Max. SIP Calls	NUMSIPCALL	256
Memory Settings	Max. SIP Media	NUMSIPMEDIA	512
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	256
Memory Settings	Max. Session Slots	NUMSLOT	32768
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	8192
Memory Settings	Max. Drop Entries	NUMTBC	4096

### 2.10.2 Box > Tuning

Table 23-41 phion M1 - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	32768
Arp	ARP Cache Size	NEIGHGC3	8192

### 2.10.3 Box Services > Statistics

Table 23-42 phion M1 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.10.4 Box Misc > Watchdog

Table 23-43 phion M1 - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.11 netfence sectorwall

### 2.11.1 Box Services > Firewall Settings

Table 23-44 netfence sectorwall - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Treshold [%]	MAXCRIT	20
Session Limits	Max Echo [%]	MAXECHO	5
Session Limits	Max Other [%]	MAXOTHER	10
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	64
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	512
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	8192
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	128
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	512
Session Limits	Max UDP [%]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	4096
Memory Settings	Max. Acceptors	NUMACCEPTOR	8192
Memory Settings	Max. ARP Entries	NUMARPC	4096
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	128
Memory Settings	Max. Fail Entries	NUMFC	4096
Memory Settings	Max. Pending Inbounds	NUMINB	32768
Memory Settings	Max. Block Entries	NUMPBC	4096
Memory Settings	Max. Plugins	NUMPLUG	8192
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	128
Memory Settings	Max. SIP Calls	NUMSIPCALL	1024
Memory Settings	Max. SIP Media	NUMSIPMEDIA	2048
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	1024
Memory Settings	Max. Session Slots	NUMSLOT	131072
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	8192
Memory Settings	Max. Drop Entries	NUMTBC	4096

### 2.11.2 Box > Tuning

Table 23-45 netfence sectorwall - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	65536
Arp	ARP Cache Size	NEIGHGC3	16384

### 2.11.3 Box Services > Statistics

Table 23-46 netfence sectorwall - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.11.4 Box Misc > Watchdog

Table 23-47 netfence sectorwall - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.12 netfence contegrity

### 2.12.1 Box Services > Firewall Settings

**Table 23-48** netfence contegrity - Box Services > Firewall Settings

Config Node	Config Label	Config Entry	Value
Session Limits	Inbound Treshold [ %]	MAXCRIT	20
Session Limits	Max Echo [ %]	MAXECHO	5
Session Limits	Max Other [ %]	MAXOTHER	5
Session Limits	Max Pending Local Accepts/Src	MAXREQLOCAL	64
Session Limits	Max Local-In Echo/Src	MAXSRCECHOLocal	64
Session Limits	Max Local-In Sessions/Src	MAXSRCLOCAL	8192
Session Limits	Max Local-In Other/Src	MAXSRCOTHERLOCAL	64
Session Limits	Max Local-In UDP/Src	MAXSRCUDPLocal	512
Session Limits	Max UDP [ %]	MAXUDP	30
Memory Settings	Max. Access Entries	NUMAC	1024
Memory Settings	Max. Acceptors	NUMACCEPTOR	8192
Memory Settings	Max. ARP Entries	NUMARPC	1024
Memory Settings	Max. Dynamic Rules	NUMDYNRULES	128
Memory Settings	Max. Fail Entries	NUMFC	1024
Memory Settings	Max. Pending Inbounds	NUMINB	16384
Memory Settings	Max. Block Entries	NUMPBC	1024
Memory Settings	Max. Plugins	NUMPLUG	8192
Memory Settings	Max. Multiple Redirect IPs	NUMREDIR	128
Memory Settings	Max. SIP Calls	NUMSIPCALL	32
Memory Settings	Max. SIP Media	NUMSIPMEDIA	64
Memory Settings	Max. SIP Transactions	NUMSIPTRANS	32
Memory Settings	Max. Session Slots	NUMSLOT	65536
Memory Settings	Dyn. Service Name Entries	NUMSRVPORT	8192
Memory Settings	Max. Drop Entries	NUMTBC	2048

### 2.12.2 Box > Tuning

**Table 23-49** netfence contegrity - Box > Tuning

Config Node	Config Label	Config Entry	Value
Routing Cache	Max Routing Cache Entries	RCMAXSIZE	16384
Arp	ARP Cache Size	NEIGHGC3	8192

### 2.12.3 Box Services > Statistics

**Table 23-50** netfence contegrity - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

### 2.12.4 Box Misc > Watchdog

**Table 23-51** netfence contegrity - Box Misc > Watchdog

Config Node	Config Label	Config Entry	Value
Watchdog	RUN S.M.A.R.T	SMARTD	yes
Watchdog	RUN WATCHDOG	RWDOG	yes

## 2.13 netfence standard

### 2.13.1 Box > Network

**Table 23-52** netfence standard - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NONE
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_eth0]	eth0
Networks	Devicename	[boxnet\$zdev_eth1]	eth1
Networks	Devicename	[boxnet\$zdev_eth2]	eth2
Networks	Devicename	[boxnet\$zdev_eth3]	eth3
Networks	Devicename	[boxnet\$zdev_eth4]	eth4
Networks	Devicename	[boxnet\$zdev_eth5]	eth5

### 2.13.2 Box > Settings

**Table 23-53** netfence standard - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	no
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.13.3 Box > Bootloader

**Table 23-54** netfence standard - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	none



## 2.14 nf-850

### 2.14.1 Box > Network

Table 23-55 nf-850 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NF-850
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	sk98lin.o
Devices	Network cards > Fallback Driver Options	AMODOPTS[]	empty string
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	y
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Driver Options	MODOPTS[]	Empty string
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_eth0]	eth0
Networks	Devicename	[boxnet\$zdev_eth1]	eth1
Networks	Devicename	[boxnet\$zdev_eth2]	eth2
Networks	Devicename	[boxnet\$zdev_eth3]	eth3

### 2.14.2 Box > Settings

Table 23-56 nf-850 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding / Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	yes
General	Serial Settings -> Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings -> Mgmt Baud Rate	SERIALBAUD	19200

### 2.14.3 Box > Bootloader

Table 23-57 nf-850 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.15 nf-780

### 2.15.1 Box > Network

Table 23-58 nf-780 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NF-780
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Fallback Driver Options	AMODOPTS[]	empty string
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Driver Options	MODOPTS[]	Empty string
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_eth0]	eth0
Networks	Devicename	[boxnet\$zdev_eth1]	eth1
Networks	Devicename	[boxnet\$zdev_eth2]	eth2
Networks	Devicename	[boxnet\$zdev_eth3]	eth3

### 2.15.2 Box > Settings

Table 23-59 nf-780 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding / Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.15.3 Box > Bootloader

Table 23-60 nf-780 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.16 nf-431

### 2.16.1 Box > Network

**Table 23-61** nf-431 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NF-431
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Fallback Driver Options	AMODOPTS[]	empty string
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Driver Options	MODOPTS[]	Empty string
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	6
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4
Networks	Devicename	[boxnet\$zdev_port5]	port5
Networks	Devicename	[boxnet\$zdev_port6]	port6

### 2.16.2 Box > Settings

**Table 23-62** nf-431 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.16.3 Box > Bootloader

**Table 23-63** nf-431 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.17 nf-421

### 2.17.1 Box > Network

**Table 23-64** nf-421 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NF-421
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Fallback Driver Options	AMODOPTS[]	empty string
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Driver Options	MODOPTS[]	Empty string
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	2
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4
Networks	Devicename	[boxnet\$zdev_port5]	port5
Networks	Devicename	[boxnet\$zdev_port6]	port6

### 2.17.2 Box > Settings

**Table 23-65** nf-421 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.17.3 Box > Bootloader

**Table 23-66** nf-421 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.18 nf-420

### 2.18.1 Box > Network

Table 23-67 nf-420 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NF-420
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Fallback Driver Options	AMODOPTS[]	empty string
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Driver Options	MODOPTS[]	Empty string
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	2
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4
Networks	Devicename	[boxnet\$zdev_port5]	port5
Networks	Devicename	[boxnet\$zdev_port6]	port6

### 2.18.2 Box > Settings

Table 23-68 nf-420 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.18.3 Box > Bootloader

Table 23-69 nf-420 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.19 nf-240

### 2.19.1 Box > Network

Table 23-70 nf-240 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NF-240
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4

### 2.19.2 Box > Settings

Table 23-71 nf-240 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.19.3 Box > Bootloader

Table 23-72 nf-240 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.20 nf-180

### 2.20.1 Box > Network

Table 23-73 nf-180 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	NF-180
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4

### 2.20.2 Box > Settings

Table 23-74 nf-180 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.20.3 Box > Bootloader

Table 23-75 nf-180 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.21 S5

### 2.21.1 Box > Network

Table 23-76 S5 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-S5
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_LAN1]	LAN1
Networks	Devicename	[boxnet\$zdev_LAN2]	LAN2
Networks	Devicename	[boxnet\$zdev_LAN3]	LAN3
Networks	Devicename	[boxnet\$zdev_LAN4]	LAN4

### 2.21.2 Box > Settings

Table 23-77 S5 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.21.3 Box > Bootloader

Table 23-78 S5 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.22 S6

### 2.22.1 Box > Network

Table 23-79 S6 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-S6
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	3
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ

### 2.22.2 Box > Settings

Table 23-80 S6 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.22.3 Box > Tuning

Table 23-81 S6 - Box > Tuning

Config Node	Config Label	Config Entry	Value
Flash	Size (%)	SIZEP	20
	Size Settings > Box Default > Resource	RESOURCE	box
	Size Settings > Box Default > Size (kB)	SIZE	16
	Size Settings > Server-Services-Default > Resource	RESOURCE	serverservice
	Size Settings > Server-Services-Default > Size (kB)	SIZE	16

### 2.22.4 Box Services > Statistics

Table 23-82 S6 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	1

### 2.22.5 Box > Bootloader

Table 23-83 S6 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.23 S25

### 2.23.1 Box > Network

Table 23-84 S25 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-S25
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4

### 2.23.2 Box > Settings

Table 23-85 S25 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.23.3 Box > Bootloader

Table 23-86 S25 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.24 S20

### 2.24.1 Box > Network

Table 23-87 S20 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-S20
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4

### 2.24.2 Box > Settings

Table 23-88 S20 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.24.3 Box > Bootloader

Table 23-89 S20 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.25 S16

### 2.25.1 Box > Network

Table 23-90 S16 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-S16
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	3
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ

### 2.25.2 Box > Settings

Table 23-91 S16 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.25.3 Box > Bootloader

Table 23-92 S16 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

### 2.25.4 Box Services > Statistics

Table 23-93 S16 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0



## 2.26 S15

### 2.26.1 Box > Network

Table 23-94 S15 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-S15
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_LAN1]	LAN1
Networks	Devicename	[boxnet\$zdev_LAN2]	LAN2
Networks	Devicename	[boxnet\$zdev_LAN3]	LAN3
Networks	Devicename	[boxnet\$zdev_LAN4]	LAN4

### 2.26.2 Box > Settings

Table 23-95 S15 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.26.3 Box > Bootloader

Table 23-96 S15 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.27 S10

### 2.27.1 Box > Network

Table 23-97 S10 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-S10
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	8139too.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	3
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_E0]	E0
Networks	Devicename	[boxnet\$zdev_E1]	E1
Networks	Devicename	[boxnet\$zdev_E2]	E2

### 2.27.2 Box > Settings

Table 23-98 S10 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.27.3 Box > Bootloader

Table 23-99 S10 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.28 M50

### 2.28.1 Box > Network

Table 23-100 M50 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M50
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_M]	M
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ

### 2.28.2 Box > Settings

Table 23-101 M50 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.28.3 Box > Bootloader

Table 23-102 M50 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

### 2.28.4 Box Services > Statistics

Table 23-103 M50 - Box Services > Statistics

Config Node	Config Label	Config Entry	Value
Statistics	Disc Write	DISCWRITE	0

## 2.29 M300

### 2.29.1 Box > Network

Table 23-104 M300 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M300
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	12
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4
Networks	Devicename	[boxnet\$zdev_port5]	port5
Networks	Devicename	[boxnet\$zdev_port6]	port6
Networks	Devicename	[boxnet\$zdev_port7]	port7
Networks	Devicename	[boxnet\$zdev_port8]	port8

### 2.29.2 Box > Settings

Table 23-105 M300 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.29.3 Box > Bootloader

Table 23-106 M300 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.30 M300a

### 2.30.1 Box > Network

Table 23-107 M300a - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M300a
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	8
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	8
Devices	Device Usage	[boxnet\$zgendeu_OK ]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4
Networks	Devicename	[boxnet\$zdev_port5]	port5
Networks	Devicename	[boxnet\$zdev_port6]	port6
Networks	Devicename	[boxnet\$zdev_port7]	port7
Networks	Devicename	[boxnet\$zdev_port8]	port8

### 2.30.2 Box > Settings

Table 23-108 M300a - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.30.3 Box > Bootloader

Table 23-109 M300a - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.31 M3000

### 2.31.1 Box > Network

Table 23-110 M3000 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M3000
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	8
Devices	Device Usage	[boxnet\$zgendeu_OK ]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4
Networks	Devicename	[boxnet\$zdev_port5]	port5
Networks	Devicename	[boxnet\$zdev_port6]	port6
Networks	Devicename	[boxnet\$zdev_port7]	port7
Networks	Devicename	[boxnet\$zdev_port8]	port8

### 2.31.2 Box > Settings

Table 23-111 M3000 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.31.3 Box > Bootloader

Table 23-112 M3000 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.32 M200

### 2.32.1 Box > Network

Table 23-113 M200 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M200
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	8
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4

### 2.32.2 Box > Settings

Table 23-114 M200 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.32.3 Box > Bootloader

Table 23-115 M200 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.33 M200a

### 2.33.1 Box > Network

Table 23-116 M200a - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M200a
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4

### 2.33.2 Box > Settings

Table 23-117 M200a - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.33.3 Box > Bootloader

Table 23-118 M200a - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.34 M2000

### 2.34.1 Box > Network

Table 23-119 M2000 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M2000
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4

### 2.34.2 Box > Settings

Table 23-120 M2000 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.34.3 Box > Bootloader

Table 23-121 M2000 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.35 M100

### 2.35.1 Box > Network

Table 23-122 M100 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M100
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	4
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT

### 2.35.2 Box > Settings

Table 23-123 M100 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.35.3 Box > Bootloader

Table 23-124 M100 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.36 M100a

### 2.36.1 Box > Network

Table 23-125 M100a - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M100a
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	2
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	2
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT

### 2.36.2 Box > Settings

Table 23-126 M100a - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.36.3 Box > Bootloader

Table 23-127 M100a - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.37 M1000

### 2.37.1 Box > Network

Table 23-128 M1000 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-M1000
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	2
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e100.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	2
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT

### 2.37.2 Box > Settings

Table 23-129 M1000 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.37.3 Box > Bootloader

Table 23-130 M1000 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)



## 2.38 L2000

### 2.38.1 Box > Network

Table 23-131 L2000 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-L2000
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	10
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_MGM]	MGM
Networks	Devicename	[boxnet\$zdev_port1]	port1
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4
Networks	Devicename	[boxnet\$zdev_port5]	port5
Networks	Devicename	[boxnet\$zdev_port6]	port6
Networks	Devicename	[boxnet\$zdev_port7]	port7
Networks	Devicename	[boxnet\$zdev_port8]	port8
Networks	Devicename	[boxnet\$zdev_port9]	port9
Networks	Devicename	[boxnet\$zdev_port10]	port10

### 2.38.2 Box > Settings

Table 23-132 L2000 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.38.3 Box > Bootloader

Table 23-133 L2000 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

## 2.39 L1000

### 2.39.1 Box > Network

Table 23-134 L1000 - Box > Network

Config Node	Config Label	Config Entry	Value
General	Verification	CHECKLESS	0 (Always)
Devices	Appliance Model	DEVMAP	HG-L1000
Devices	Network cards > Activate Driver	ACTSTATE	y
Devices	Network cards > Fallback Module Name	AMOD	NONE
Devices	Network cards > Driver Type	BLTIN	module
Devices	Network cards > Fallback Enabled	IFAMOD	n
Devices	Network cards > Operation Mode	MOD	e1000.o
Devices	Network cards > Ethernet MTU	MTU1	1500
Devices	Network cards > Number of Devices	NUM	10
Devices	Device Usage	[boxnet\$zgendeu_OK]	OK
Networks	Devicename	[boxnet\$zdev_HA]	HA
Networks	Devicename	[boxnet\$zdev_DMZ]	DMZ
Networks	Devicename	[boxnet\$zdev_EXT]	EXT
Networks	Devicename	[boxnet\$zdev_INT]	INT
Networks	Devicename	[boxnet\$zdev_port2]	port2
Networks	Devicename	[boxnet\$zdev_port3]	port3
Networks	Devicename	[boxnet\$zdev_port4]	port4
Networks	Devicename	[boxnet\$zdev_port5]	port5
Networks	Devicename	[boxnet\$zdev_port6]	port6

### 2.39.2 Box > Settings

Table 23-135 L1000 - Box > Settings

Config Node	Config Label	Config Entry	Value
Dns	Run Forwarding/Caching DNS	RUNBDNS	yes
General	Serial Access	SERIAL	y
General	Serial Settings > Access Types	SERIALTYPE	1 (ConsoleOnly(COM1))
General	Serial Settings > Mgmt Baud Rate	SERIALBAUD	19200

### 2.39.3 Box > Bootloader

Table 23-136 L1000 - Box > Bootloader

Config Node	Config Label	Config Entry	Value
Bootloader	Serial Console	SERIAL	0 (COM1)

### 3. Index of Dialogue Sections

#### A

Accepted Ciphers [VPN] .....	216,
[phion management centre] .....	467
Access Cache Settings [Firewall] .....	127
Access Control List [Configuration Service] .....	54
Access List Configuration [SSH Gateway] .....	366
Access List Filters [OSPF and RIP] .....	490
ACCESS NOTIFICATION [Configuration Service] .....	98
Access Options [SSH Gateway] .....	366
Access Rights Query [VPN] .....	233
ACL [VPN] .....	217
ACL Entries [Proxy] .....	329
ACL FileList [Proxy] .....	331
ACTIONS [Proxy] .....	331
ACTIVE LICENSES [Control Centre] .....	37
Additional Local Networks [Configuration Service] .....	62
Address Pool Configuration [DHCP] .....	273
Address Pools [DHCP] .....	274
Admin Restrictions [phion management centre] .....	419
Administrative Scope [phion management centre] .....	434
Administrative Level [phion management centre] .....	420
Advanced [Getting Started] .....	13,
[Proxy] .....	335,
[Anti-Virus] .....	369
Advanced Access Settings [Configuration Service] .....	54
Advanced DNS Settings [Configuration Service] .....	55
Affected Box Logdata [Configuration Service] .....	116
Affected Service Logdata [Configuration Service] .....	116
Allowed Host Configuration [SSH Gateway] .....	366
Allowed Relaying [Mail Gateway] .....	250
Application Access Authorization [VPN] .....	233
Application Tunneling Configuration [VPN] .....	233
Archive Scanning [Anti-Virus] .....	369
ARP Settings [Configuration Service] .....	100
Attachment Stripping [Mail Gateway] .....	253
Attributes [phion management centre] .....	468
Audit Info Transport [Firewall] .....	130
Audit Information Generation [Firewall] .....	129,
[Firewall] .....	130
Authentication [Configuration Service] .....	72,
[Configuration Service] .....	75,
[Configuration Service] .....	77,
[Proxy] .....	327
Authentication Level [Control Centre] .....	39
Authentication Method [Firewall] .....	190
Authentication Pattern [Firewall] .....	190
Auto Logout Setup [Configuration Service] .....	118
Available Interfaces [OSPF and RIP] .....	489
Available Server IPs [Configuration Service] .....	97

#### B

Band A [Configuration Service] .....	88
Band B [Configuration Service] .....	88
Band C [Configuration Service] .....	88
Band D [Configuration Service] .....	88
Band E [Configuration Service] .....	88
Band F [Configuration Service] .....	88
Band G [Configuration Service] .....	88
Bandwidth Protection [VPN] .....	225
Basic [Configuration Service] .....	112
Basic DNS Settings [Configuration Service] .....	55
BASIC OPTIONS [DHCP] .....	283
Basic Options [DHCP] .....	276
Basic Settings [Proxy] .....	325
Basic Setup [Anti-Virus] .....	368
BEHAVIOR [FTP Gateway] .....	353
Bind IPs [Configuration Service] .....	97
Blacklists [Mail Gateway] .....	254
BOB Settings [Firewall] .....	146
Box Certificate [Configuration Service] .....	60
Box public key [Getting Started] .....	14
BOX SCEP Settings [Configuration Service] .....	58
BOX SCEP Status [Control Centre] .....	40
Bridging [Firewall] .....	141

#### C

Cache Behaviour [Proxy] .....	326
-------------------------------	-----

Certificate [VPN] .....	208
Certificate Revocation [Proxy] .....	338,
[Proxy] .....	339
Certificate Verification [Proxy] .....	338
Channel Bonding Settings [Configuration Service] .....	75
Class Configuration [DHCP] .....	278
Client Description [DHCP] .....	275
Client Group Members [DHCP] .....	275
Client Match & Address Assignment [DHCP] .....	275
Cloning and Archiving [Mail Gateway] .....	251
Common [VPN] .....	217
Common Settings [Configuration Service] .....	104,
[Configuration Service] .....	108,
[VPN] .....	210
Compression [Getting Started] .....	22,
[Configuration Service] .....	75
Condition [Configuration Service] .....	87
Configuration Assignment [FTP Gateway] .....	353
Configuration Settings [Getting Started] .....	22
Configuration Update Setup [phion management centre] .....	413
Confirmed [Eventing] .....	312
Connect by Destination SSL Setup [phion management centre] .....	451
Connection Details [Configuration Service] .....	59,
[Configuration Service] .....	73,
[Configuration Service] .....	74
Connection Monitoring [Configuration Service] .....	67,
[Configuration Service] .....	73,
[Configuration Service] .....	74,
[Configuration Service] .....	76,
[Configuration Service] .....	78
Connection to MC [phion management centre] .....	472
Connection Tracing [Firewall] .....	129,
[Firewall] .....	131
Connection Type Setup [phion management centre] .....	451
Console Access [Configuration Service] .....	106
Contact Info [phion management centre] .....	416
Contact Information [phion management centre] .....	418
Cook Settings [Statistics] .....	300,
[phion management centre] .....	438
Corporate ID [VPN] .....	232
Counting / Eventing / Audit Trail [Firewall] .....	155
CPU-Load Error Thresholds [Configuration Service] .....	118
CPU-Load Warning Thresholds [Configuration Service] .....	118
CRL error handling [VPN] .....	208
Cryptography [Getting Started] .....	22
Custom Ciphers [VPN] .....	208

#### D

Data Leak Prevention [Proxy] .....	335
Data Origin [phion management centre] .....	450
Data Selection [phion management centre] .....	450
Data Tag Policy [phion management centre] .....	451
Data Transfer Setup [Configuration Service] .....	117
Default Mail [Eventing] .....	311
Default Server Certificate [VPN] .....	207
Default SNMP [Eventing] .....	311
Default User Specific [FTP Gateway] .....	354
Desktop Background [Getting Started] .....	22
Destination Address [Configuration Service] .....	117
Device Configuration [VPN] .....	207
Device Name [Configuration Service] .....	62
DNS [Getting Started] .....	11,
[Configuration Service] .....	73
DNS Authentication [DHCP] .....	278
DNS Update Configuration [DHCP] .....	278
DoS Protection [Mail Gateway] .....	255
Dynamic DNS Parameters [DHCP] .....	277
Dynamic Firewall Rule Activation Authorization [VPN] .....	233
Dynamic Firewall Rules [VPN] .....	233
Dynamic Network Connections [Control Centre] .....	39

#### E

Encoding Parameters [Configuration Service] .....	59
entegra Access Control Setup [VPN] .....	232
entegra Policy Service Options [DHCP] .....	276
Entries in Access Cache [Mail Gateway] .....	256
Entry [Firewall] .....	140,
[Firewall] .....	142

Event Settings [Mail Gateway] ..... 256  
 Eventing Settings [Firewall]..... 129  
 Excluded Entry [Firewall] ..... 140,  
 [Firewall] ..... 142  
 Expert Settings (use with care) [Mail Gateway]..... 251  
 Extended Domain Setup [Mail Gateway] ..... 248  
 EXTENDED OPTIONS [DHCP]..... 283  
 Extended Options [DHCP] ..... 276  
 Extended [Configuration Service]..... 112  
 External Group Condition [VPN]..... 219

**F**

Failover and Load Balancing [Firewall] ..... 146  
 File Specific Settings [Configuration Service] ..... 104  
 Flash Appliance Settings [Configuration Service]..... 101  
 Free Format OSPF Configuration [OSPF and RIP]..... 491  
 Free Format RIP Configuration [OSPF and RIP]..... 491  
 FW Authentication Server [Firewall] ..... 188

**G**

Garbage Collection [Configuration Service]..... 100  
 General [Firewall]..... 144,  
 [phion management centre] ..... 433  
 General IP Settings [Configuration Service]..... 100  
 General Service Settings [VPN] ..... 231,  
 [SSH Gateway]..... 365  
 General Settings [Configuration Service] ..... 106,  
 [phion management centre] ..... 459,  
 [phion management centre] ..... 467,  
 [phion management centre] ..... 468  
 Generic Application Tunneling Authorization [VPN]..... 233  
 Global Domain Parameters [Mail Gateway]..... 247  
 GLOBAL SETTINGS [DHCP] ..... 283  
 Global Settings [Statistics]..... 300,  
 [phion management centre] ..... 438  
 Graphics [phion management centre] ..... 471  
 Grey Listing [Mail Gateway]..... 253  
 Group Based Assignment [DHCP]..... 275  
 GUI AS TEXT [OSPF and RIP]..... 491

**H**

HA Monitoring Parameters [Configuration Service]..... 118  
 HA Synchronization Setup [phion management centre] .. 449  
 Header Settings [Configuration Service] ..... 102  
 Host Configuration [Mail Gateway]..... 247  
 HOST IDS [Control Centre]..... 37  
 HTML Tag Removal [Mail Gateway] ..... 255  
 HTTP Streaming [Anti-Virus]..... 369

**I**

ICMP Echo [Firewall] ..... 144  
 ICMP Gateway Monitoring Exemptions [Configuration Service]118  
 Identification [phion management centre]..... 416,  
 [phion management centre] ..... 418  
 Identification Settings [Configuration Service] ..... 52  
 IKE Parameters [VPN]..... 207  
 In Groups [phion management centre] ..... 468  
 Inbound (traffic received by the device) [Configuration Service]  
 85  
 Installation Mode Settings [Getting Started] ..... 14  
 Installation scripts [Getting Started] ..... 14  
 Installation-script files [Getting Started]..... 14  
 Integrity Check Settings [Configuration Service] ..... 80  
 Interface [DNS]..... 317,  
 [DNS] ..... 319  
 Interface Monitoring [Configuration Service]..... 95  
 IP Address & Networking [VPN] ..... 213  
 IP Monitoring [Configuration Service] ..... 95  
 IP Prefix List Configuration [OSPF and RIP]..... 490  
 IP Prefix List Filters [OSPF and RIP]..... 490  
 IP RANGES [DHCP] ..... 283  
 IPSec Phase I [VPN]..... 215  
 IPSec Phase II [VPN] ..... 215  
 ISDN Setup [Configuration Service]..... 74  
 ISS Proventia Cascaded Redirector [Proxy]..... 346  
 ISS Proventia Database Settings [Proxy] ..... 344  
 ISS Proventia Deny Message [Proxy]..... 346  
 ISS Proventia Exceptions [Proxy]..... 346  
 ISS Proventia General Settings [Proxy]..... 344  
 ISS Proventia Logging Settings [Proxy] ..... 346  
 ISS Proventia Proxy [Proxy] ..... 344

ISS Proventia Settings [Proxy]..... 345  
 ISS Proventia Statistics Settings [Proxy] ..... 347

**K**

Kernel Updates [Configuration Service]..... 102

**L**

L2TP Settings [VPN]..... 211  
 LAN Rule Policy [Firewall]..... 156  
 Layer2 Bridging [Firewall]..... 184  
 LDAP [Configuration Service]..... 113  
 LDAP Server [phion management centre] ..... 459  
 Lease Constraints [DHCP]..... 277  
 LEGACY [Proxy]..... 332  
 License Configuration [Configuration Service]..... 93  
 License Values [Control Centre]..... 37  
 Lifetime [VPN]..... 215  
 Limits and Operational Settings [Firewall]..... 129  
 Local Authentication [FTP Gateway]..... 354  
 Local Domain Settings [Mail Gateway] ..... 247  
 LOCAL PARAMETERS [phion management centre] ..... 449  
 Log Configuration [Configuration Service] ..... 119  
 Log Cycling Actions [Configuration Service] ..... 104  
 Log Data Tagging [Configuration Service]..... 117  
 Log File Selection [Configuration Service]..... 104  
 Log Settings [Configuration Service] ..... 101,  
 [Configuration Service] ..... 115,  
 [Proxy]..... 325  
 Logging [FTP Gateway] ..... 353  
 Login [VPN] ..... 209  
 Lookup [DNS]..... 318

**M**

Mail Gateway Limits [Mail Gateway] ..... 255  
 Mail Lookup [Configuration Service]..... 112  
 Main Routing Table [Configuration Service] ..... 68  
 Management Network [Configuration Service]..... 62  
 Management Traffic [Configuration Service]..... 88  
 Management Tunnel Configuration [Configuration Service] 67  
 MC Identification [phion management centre] ..... 412  
 MC IP Addresses [phion management centre]..... 412  
 MC SSH Access Keys [phion management centre]..... 413  
 Misc [Mail Gateway] ..... 255  
 Misc. Settings [Proxy]..... 325  
 Miscellaneous [Firewall]..... 155  
 Miscellaneous Parameters [DHCP]..... 277  
 Monitoring Parameters [Configuration Service]..... 117  
 Monitoring Policy [Configuration Service] ..... 110  
 Multi Subnet Configuration [DHCP]..... 274

**N**

Neighbors [OSPF and RIP]..... 489  
 Neighbour Settings [Proxy]..... 326  
 Network [VPN]..... 206  
 Network Configuration [Control Centre]..... 38  
 Network Interface Configuration [Configuration Service].  
 [OSPF and RIP] ..... 489  
 Network Routes [VPN]..... 217  
 NETWORK SETTINGS [Proxy]..... 325  
 Network Time Protocol [Getting Started]..... 11  
 Networks [VPN]..... 227  
 Non-Virus Detection [Anti-Virus]..... 369  
 Notification [Anti-Virus]..... 372  
 NTP Settings [Configuration Service] ..... 56

**O**

OCSP Server [VPN]..... 209  
 OCSP Server Identification [VPN] ..... 209  
 ONCRPC Servers / DCERPC Servers [Firewall] ..... 194  
 ONLINE TESTS [Mail Gateway] ..... 260  
 Operating System [Control Centre]..... 39  
 Operation Mode [Configuration Service] ..... 95  
 Operation Setup [OSPF and RIP] ..... 485  
 Operational Settings [Configuration Service] ..... 53,  
 [Mail Gateway]..... 250  
 Operational Setup [Configuration Service] ..... 115,  
 [phion management centre] ..... 447  
 Operative Settings [phion management centre]..... 435  
 Optimizations [Proxy]..... 335  
 Option Section [DHCP]..... 283

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Option Settings [Proxy].....	326
Options [Statistics] .....	297,
[Statistics].....	299
OSPF Area Configuration [OSPF and RIP].....	487
OSPF Parameters [OSPF and RIP] .....	489,
[OSPF and RIP].....	490
OSPF Preferences Configuration [OSPF and RIP] .....	485
OSPF Router Configuration [OSPF and RIP].....	486
OSPF Specific Conditions [OSPF and RIP].....	490
OSPF Specific Parameters [OSPF and RIP].....	489
OTHER DESTINATIONS [FTP Gateway] .....	354
Outbound (traffic being sent over the device) [Configuration Service].....	85
Outlook Web Access Authorization [VPN].....	232

**P**

Parameters [VPN] .....	228
Partner Identification [VPN].....	228
Password and Peer Restriction [VPN] .....	213
Password Parameters [phion management centre] .....	434
Peer Condition [VPN] .....	219
Performance [Configuration Service] .....	118
Phase 1 [VPN] .....	227,
[phion management centre] .....	468
Phase 1 (default) [VPN] .....	215
Phase 2 [VPN].....	215,
[VPN] .....	227
Phase2 [phion management centre] .....	468
PHIBS Authentication Settings [Firewall].....	189
PHIBS Specific Authentication Scheme [Proxy].....	328
Phion [VPN].....	216
phion Login [Getting Started] .....	13
Plain Data Reception [phion management centre] .....	448
Policy Based Routing [Configuration Service] .....	69
Policy Definition [Configuration Service].....	88
Policy Service [VPN] .....	207
Policy Source Matching [Configuration Service] .....	70
Policy Table Contents [Configuration Service].....	70
POP3 Setup [Mail Gateway] .....	249
PPPOE Connection Details [Configuration Service] .....	72
PPTP Connection Details [Configuration Service].....	71
PPTP Settings [VPN].....	211
Preauthentication [VPN].....	218
Protocol Version 1 Options [Configuration Service] .....	107
Protocol Version 2 Options [Configuration Service].....	107
PROVENTIA LIMIT HANDLING [Proxy].....	347
Proxy [VPN].....	209,
[VPN] .....	210
PUBLIC KEYS [Getting Started].....	24

**Q**

Quarantine Bridging [Firewall].....	184
Quarantine Class 1 Rule Policy [Firewall] .....	156
Quarantine Class 2 Rule Policy [Firewall] .....	156
Quarantine Class 3Rule Policy [Firewall].....	156
Quarantine Policy [Firewall].....	156

**R**

RAM Partition [Configuration Service].....	101
Recorded Conditions [Firewall] .....	130
Redirector Settings [Proxy] .....	335,
[Proxy] .....	344
Registry Entry [VPN] .....	219
Relay Streams [phion management centre] .....	452
Relaying Setup [phion management centre].....	450
Release Check [Configuration Service] .....	108
Remote Execution Setup [phion management centre]... ..	413
Remote Management Tunnel [Configuration Service] .....	67
Reporting [Anti-Virus].....	369
Resource Protection [Firewall] .....	155
RIP Parameters [OSPF and RIP] .....	489
RIP Preferences Configuration [OSPF and RIP].....	488
RIP Router Configuration [OSPF and RIP].....	487
RIP SETTINGS [OSPF and RIP].....	486
RIP Specific Conditions [OSPF and RIP].....	490
RIP Specific Parameters [OSPF and RIP].....	489
Role Name [phion management centre] .....	414
Root Login [Getting Started] .....	13
Root Password [Configuration Service].....	54
Route Map Configuration [OSPF and RIP].....	490
Route Map Filters [OSPF and RIP].....	490

Router Distribution Configuration [OSPF and RIP].....	487,
[OSPF and RIP].....	488
Routing [Configuration Service] .....	72,
[Configuration Service] .....	74,
[Configuration Service] .....	75,
[Configuration Service] .....	77
Routing Cache Settings [Configuration Service] .....	100
RPC Settings [Firewall].....	194
Rule Mismatch Policy [Firewall] .....	154
Rule Settings [Firewall].....	156
RULES [Mail Gateway] .....	261

**S**

Scanner Location [Anti-Virus].....	371
SCEP HTTP Proxy Settings [Configuration Service] .....	59
SCEP HTTP Server Authentication [Configuration Service] .....	59
SCEP Server [Configuration Service].....	59
SCEP X509 Request [Configuration Service].....	59
SCEP X509 Request Password [Configuration Service]... ..	59
Security [DNS].....	318,
[DNS] .....	319
Security Options [SSH Gateway].....	366
Serial Access [Configuration Service] .....	54
Serial Console [Configuration Service] .....	67
Server [VPN].....	217
Server Configuration [VPN].....	207
Server Scripts [Configuration Service] .....	96
Server Specific Firewall Settings [Firewall] .....	131
SERVER STATUS [Control Centre].....	29
Server/Service [phion management centre] .....	468
Service Availability [DHCP] .....	273
Service Definition [Configuration Service] .....	97
Service Identification [VPN].....	231,
[SSH Gateway] .....	365
Service Password [Configuration Service] .....	54
SERVICE STATUS [Control Centre] .....	29
Session Limits and Memory Settings [Firewall] .....	127
Session Password Setup [Configuration Service] .....	118
Shared Interface Configuration [OSPF and RIP] .....	489
Show Short/Long Date [Getting Started] .....	22
SNMP [Proxy].....	327
Software Packages [Getting Started] .....	13
Spam Detection [Mail Gateway] .....	253
Spamfilter Settings [Mail Gateway] .....	260
SPECIAL CLIENTS [DHCP] .....	283
SPECIAL DESTINATIONS [FTP Gateway].....	354
Special Destinations [FTP Gateway].....	353
Specific Settings [phion management centre].....	416,
[phion management centre] .....	418
SSH Colours [Getting Started].....	22
SSH KEYS [Getting Started].....	24
SSH Private Key [Configuration Service] .....	60
SSL Client Authentication [phion management centre]... ..	449
SSL Settings [Proxy] .....	338
SSL Tunnel Configuration [VPN].....	233
Statistic Cooking [Statistics] .....	300
Statistic Settings [Mail Gateway] .....	256
Statistics Cooking [phion management centre].....	438
Statistics Settings [Configuration Service].....	97
Status Map Setup [phion management centre].....	413
Stream Configuration [Configuration Service].....	117
Stream to Destination Setup [phion management centre] .....	451
SUBNET SETTINGS [DHCP] .....	273
System [Getting Started] .....	22
System Identification & Authentication [Configuration Service] .....	116

**T**

TCP & UDP [Firewall].....	144
TCP Policy [Firewall].....	154
Template Description [DHCP] .....	276,
[DHCP] .....	277
TEST CONNECTION [Firewall].....	163
TEST RESULT [Firewall].....	164
TI Traffic Prioritization [VPN].....	225
TI Transport Classification [VPN].....	224
TI Transport Selection [VPN].....	224
Time [Eventing] .....	312
Time Control [Control Centre].....	39
Time Interval [Statistics] .....	298
Time Restrictions [FTP Gateway].....	354
TIME SETTINGS [Proxy] .....	345

Time Settings [Configuration Service] ..... 56  
 Timeout Settings [Configuration Service] ..... 115  
 Timeouts [Getting Started] ..... 22  
 Top Level Logdata [Configuration Service] ..... 116  
 Top List [Statistics] ..... 299  
 TRAINING OPTIONS [Mail Gateway] ..... 261  
 Trust Chain Configuration [phion management centre]... 412  
 Tuning Parameters [phion management centre] ..... 448  
 Tunnel Configuration [Configuration Service] ..... 79  
 Tunnel Details [Configuration Service] ..... 67  
 Tunnels [phion management centre] ..... 468  
 Type Time [Statistics] ..... 300,  
     [phion management centre] ..... 439  
 Type Top [Statistics] ..... 301,  
     [phion management centre] ..... 439

**U**

UMTS (3G) Setup [Configuration Service] ..... 76  
 UMTS Connection Details [Configuration Service] ..... 76  
 Updates [Anti-Virus] ..... 368  
 URI [VPN] ..... 208  
 Usage [VPN] ..... 208  
 USER AUTHENTICATION [Mail Gateway] ..... 251  
 User Authentication [VPN] ..... 231,  
     [SSH Gateway] ..... 365  
 User Scripts [Configuration Service] ..... 80  
 User Session Handling [SSH Gateway] ..... 365

**V**

VERSION STATUS [Control Centre] ..... 37  
 Virtual LAN Configuration [Configuration Service] ..... 65  
 Virtual Server Definition [Configuration Service] ..... 95,  
     [Configuration Service] ..... 96  
 Virtual Server Identity [Configuration Service] ..... 96  
 Virtual Server IP Addresses [Configuration Service] ..... 95  
 Virtual Server/GTI Networks [Configuration Service] .... 96  
 Virus Protection [Mail Gateway] ..... 253,  
     [Anti-Virus] ..... 371  
 Virus Scanner [Proxy] ..... 335,  
     [Anti-Virus] ..... 370  
 Virus Scanning [FTP Gateway] ..... 353  
 Volumes [Getting Started] ..... 12  
 VPN Envelope Policy [VPN] ..... 226,  
     [phion management centre] ..... 467  
 VPN Traffic Intelligence (TI) Settings [Firewall] ..... 146  
 VPN User Pattern [Firewall] ..... 190  
 VPN World Settings [Configuration Service] ..... 53  
 VPN World Setup [phion management centre] ..... 413

**W**

Watchdog Monitored Entities [Configuration Service] .... 111  
 Watchdog Operational Setup [Configuration Service] .... 110  
 Watchdog Repair Policy [Configuration Service] ..... 110  
 Web Resource Access Authorization [VPN] ..... 232  
 Web Resource Configuration [VPN] ..... 232  
 WebDAV Resource Access Authorization [VPN] ..... 232  
 WebDAV Resource Configuration [VPN] ..... 232  
 WHITE/BLACK LISTS [Mail Gateway] ..... 260

**X**

X509 Certificate Conditions [VPN] ..... 219  
 X509 Certificate Pattern [Firewall] ..... 190  
 X509 Client Security [VPN] ..... 217  
 xDSL Setup [Configuration Service] ..... 70



## 4. Index of Dialogue Tabs

### A

Accepted Ciphers [phion management centre] .....	467
ACCESS [Configuration Service] .....	91
Access [Firewall] .....	173,
[VPN] .....	230,
[Mail Gateway] .....	265
Access Control [Proxy] .....	327,
[Proxy] .....	328
Access Limitations [Configuration Service] .....	58
Access Lists [SSH Gateway] .....	366
Account Description [Configuration Service] .....	91
Active [VPN] .....	229
Active Certificate [VPN] .....	214
Additional Schemes [Configuration Service] .....	115
Admin & MC Settings [Getting Started] .....	23
Administrative Sessions [Configuration Service] .....	118
Administrator [phion management centre] .....	433
Administrator Access Control [Configuration Service] .....	91
Administrator Authorization [Configuration Service] .....	91
Admins [phion management centre] .....	433
Advanced [Proxy] .....	335,
[phion management centre] .....	469
Advanced Setup [Mail Gateway] .....	250
Advanced System Access [Configuration Service] .....	54
AFS-Database (AFSDB) [DNS] .....	322
Alias (CNAME) [DNS] .....	322
Archive Scanning [Anti-Virus] .....	369
ARP Settings [Configuration Service] .....	100
ARPs [Control Centre] .....	32
Attachments [Mail Gateway] .....	266
Audit and Reporting [Firewall] .....	129
Authentication [Firewall] .....	131,
[VPN] .....	228,
[FTP Gateway] .....	354
Authentication & Login [SSH Gateway] .....	365
AuthUser [Firewall] .....	176

### B

Base configuration [VPN] .....	227
Basic [Eventing] .....	311
Basic Setup [Configuration Service] .....	115,
[Mail Gateway] .....	246,
[Anti-Virus] .....	368,
[phion management centre] .....	447
Basics [phion management centre] .....	469
Box [Control Centre] .....	38,
[phion management centre] .....	431
Box Execution [phion management centre] .....	401
Boxes [Getting Started] .....	21,
[phion management centre] .....	403
Bridging [Firewall] .....	131
Bridging ARPs [Firewall] .....	177

### C

Cache Filter [Firewall] .....	173
Cache Selection [Firewall] .....	173
Cascaded Redirector [Proxy] .....	346
Certificate details [VPN] .....	208
Certificate revocation [VPN] .....	208
CERTIFICATES [phion management centre] .....	412
Certificates & Private Keys [Getting Started] .....	23
Classes [DHCP] .....	278
Client [Getting Started] .....	22
Client Action [Eventing] .....	310
Client to Site [VPN] .....	229
Cluster [phion management centre] .....	431
Command Codes [Configuration Service] .....	58
Common [VPN] .....	216
Configuration Updates [phion management centre] .....	398
Connections [Firewall] .....	145
Content Filter [Mail Gateway] .....	253
Content Inspection [Proxy] .....	335
CPU-Load Monitoring [Configuration Service] .....	118

### D

Default Permissions [SSH Gateway] .....	366
Deny Message [Proxy] .....	346
Details [phion management centre] .....	434
DHCP Option Templates [DHCP] .....	276
DNS [Configuration Service] .....	55
Dynamic [Firewall] .....	176
Dynamic DNS [DHCP] .....	278
Dynamic Rules [Firewall] .....	176
Dynamic Services [Firewall] .....	177

### E

Events [Eventing] .....	306
EXCEPTIONS [Proxy] .....	346
Explicit Groups [Configuration Service] .....	115
Extended Domain Setup [Mail Gateway] .....	247
External CA [VPN] .....	215

### F

Favourites [phion management centre] .....	398
File Updates [phion management centre] .....	400
Filter Settings [Proxy] .....	345
Filter Setup [OSPF and RIP] .....	490
FILTERS [Configuration Service] .....	116
Firewall [Firewall] .....	131
Floating Licenses [phion management centre] .....	400

### G

GENERAL [Configuration Service] .....	105,
[DHCP] .....	273,
[phion management centre] .....	413
General [Configuration Service] .....	95,
[VPN] .....	210,
[DNS] .....	318,
[Proxy] .....	325,
[SSH Gateway] .....	365
General Settings [phion management centre] .....	460
Global Limits [Firewall] .....	126
Grey Listing [Mail Gateway] .....	267
GTI Networks [Configuration Service] .....	96
GUI as Text [DHCP] .....	279,
[OSPF and RIP] .....	491

### H

H.323 [Firewall] .....	131
HA Synchronization [phion management centre] .....	449
Host (A) [DNS] .....	320,
[DNS] .....	322
Host Information (HINFO) [DNS] .....	321,
[DNS] .....	322

### I

I/O Settings [Configuration Service] .....	101
ICMP [Firewall] .....	158
Identification [phion management centre] .....	412
Identify [VPN] .....	222
IDENTITY [Configuration Service] .....	96
Inbound [Firewall] .....	162
Inbound-User [Firewall] .....	162
Interface Groups [Firewall] .....	150
Interface/IPs [Control Centre] .....	30
Interfaces [Control Centre] .....	31,
[Configuration Service] .....	63
IP Tunneling [Configuration Service] .....	78
IPs [Control Centre] .....	31
IPSec [VPN] .....	215,
[phion management centre] .....	468
IPv4 Settings [Configuration Service] .....	100
IPv6-Host (AAAA) [DNS] .....	322
ISDN [DNS] .....	322

### K

Known Clients [DHCP] .....	275
----------------------------	-----



**L**

L2TP/IPSEC [VPN] ..... 210  
 LDAP [Configuration Service]..... 113  
 Licenses [Control Centre] ..... 37  
 Limit Handling [Proxy] ..... 347  
 Limits [Mail Gateway] ..... 255  
 Local Networks [VPN]..... 222  
 Local Storage [phion management centre] ..... 449  
 Logdata Streams [Configuration Service] ..... 117  
 Logging [Proxy] ..... 346  
 Logstream Destinations [Configuration Service] ..... 117

**M**

Mail Queue [Mail Gateway] ..... 263  
 Mail Rename (MR) [DNS] ..... 322  
 Mailbox (MB) [DNS]..... 322  
 Mailbox information (MINFO) [DNS]..... 321,  
 [DNS] ..... 322  
 Mail-Exchanger (MX) [DNS]..... 321,  
 [DNS] ..... 322  
 Mailgroup (MG) [DNS]..... 322  
 Main Rules [Firewall]..... 161  
 Mainboard [Control Centre] ..... 40  
 MC [phion management centre] ..... 395  
 Messages [VPN]..... 219  
 Monitoring [Configuration Service] ..... 95  
 Monitoring Setup [Configuration Service] ..... 117  
 MSAD [Configuration Service] ..... 111  
 MS-CHAP [Configuration Service] ..... 112  
 MSNT [Configuration Service] ..... 114

**N**

Nameserver (NS) [DNS] ..... 320,  
 [DNS] ..... 322  
 Neighbor Setup [OSPF and RIP] ..... 489  
 Network [Control Centre] ..... 30,  
 [Proxy] ..... 325  
 Network Interfaces [OSPF and RIP]..... 489  
 Network Routes [Configuration Service] ..... 68  
 Networks [Configuration Service] ..... 61,  
 [Firewall] ..... 140  
 Notification [Eventing]..... 308

**O**

Objects [phion management centre]..... 402  
 Obsolete Certificate [VPN] ..... 214  
 OCSP [Configuration Service]..... 115,  
 [VPN] ..... 209  
 Offline FW [VPN] ..... 219  
 Operational [Firewall]..... 128  
 Operational Setup [OSPF and RIP]..... 485  
 OSPF [Control Centre] ..... 32  
 OSPF Area Setup [OSPF and RIP] ..... 487  
 OSPF Preferences [OSPF and RIP]..... 485  
 OSPF Router Setup [OSPF and RIP]..... 486  
 Outbound [Firewall] ..... 162  
 Outbound-User [Firewall]..... 162

**P**

Page 1 [Eventing]..... 312  
 Page 2 [Eventing] ..... 312  
 Parameter [VPN]..... 222  
 Parameter Templates [VPN]..... 222  
 Parameters [DHCP] ..... 277  
 Partner [VPN] ..... 222  
 Partner Networks [VPN] ..... 222  
 Peer-to-Peer Detection [Firewall] ..... 126  
 Permission Profiles [SSH Gateway]..... 366  
 Personal Networks [VPN] ..... 206  
 Phibs [Firewall] ..... 131  
 Phion [VPN] ..... 216  
 Phion VPN CA [VPN]..... 212  
 Pictures [VPN]..... 219  
 Pointer (PTR) [DNS] ..... 322  
 Policy [VPN]..... 217  
 Pool Licenses [VPN]..... 212  
 POP3 Setup [Mail Gateway] ..... 249  
 PPTP [VPN] ..... 211  
 Processes [Control Centre]..... 36,  
 [Mail Gateway]..... 266  
 Protected IPs [Firewall] ..... 176  
 Proxy ARPs [Control Centre] ..... 32,  
 [Firewall]..... 150  
 Public Host Keys [Getting Started] ..... 24

**R**

RADIUS [Configuration Service]..... 114  
 Range [phion management centre]..... 431  
 RCS Setup [phion management centre]..... 413  
 Redirect Availability [Firewall]..... 177  
 Registry [VPN]..... 219  
 Relay Destinations [phion management centre]..... 451  
 Relay Filters [phion management centre] ..... 450  
 Relay Streams [phion management centre] ..... 452  
 Relaying Setup [phion management centre]..... 450  
 Reporting [Mail Gateway] ..... 256  
 Resources [Control Centre] ..... 36  
 Responsible Person (RP) [DNS] ..... 322  
 RIP Preferences [OSPF and RIP] ..... 488  
 RIP Router Setup [OSPF and RIP] ..... 487  
 Root Certificates [VPN]..... 208,  
 [phion management centre] ..... 466  
 Route (RT) [DNS]..... 322  
 Routing Cache [Configuration Service] ..... 100  
 RPC [Firewall] ..... 131  
 RSA-ACE [Configuration Service] ..... 114  
 Rule Tester [Firewall]..... 163  
 Rules [Firewall] ..... 135,  
 [VPN]..... 217

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

**S**

Scanner Versions [phion management centre] .....	405
Scanning Options [Anti-Virus] .....	369
SCEP [Configuration Service] .....	58
Scripts [Configuration Service] .....	96,
[VPN] .....	222
Server [Control Centre] .....	29,
[phion management centre] .....	431
Server Action [Eventing] .....	309
Server Certificates [VPN] .....	209
Server Key/Settings [VPN] .....	207
Server/Service Settings [phion management centre] .....	469
Service [phion management centre] .....	431
Service or Server (SRV) [DNS] .....	322
Services [Firewall] .....	143
Session Limits [Firewall] .....	127
Sessions [Control Centre] .....	40,
[phion management centre] .....	400
Settings [FTP Gateway] .....	353
Severity [Eventing] .....	307
SIP [Firewall] .....	131,
[Firewall] .....	177
Site to Site [VPN] .....	229
SMS Control [Configuration Service] .....	57
SMS Control Settings [Configuration Service] .....	58
Spam [Mail Gateway] .....	265
Special Needs [Configuration Service] .....	80
SSL [phion management centre] .....	448
Start of authority (SOA) [DNS] .....	319
STATISTICS [Proxy] .....	347
Statistics [Control Centre] .....	32
Statistics Collection [phion management centre] .....	401
Statistics Cooking [Statistics] .....	300
Status [Firewall] .....	169,
[VPN] .....	229
Status Filter [Firewall] .....	169,
[VPN] .....	229
Status Map [phion management centre] .....	397
Subject [phion management centre] .....	461
SUBNETS [DHCP] .....	273
System Access (Basic View) [Configuration Service] .....	54

**T**

Templates [VPN] .....	214
Test Report [Firewall] .....	164
Text (TXT) [DNS] .....	321,
[DNS] .....	322
Text Based Configuration [DHCP] .....	279,
[OSPF and RIP] .....	491
Thresholds [Eventing] .....	310
TI [VPN] .....	222
TI - Bandwidth Protection [phion management centre] .....	469
TI - VPN Envelope Policy [phion management centre] .....	469
Time Objects [Firewall] .....	139
TIME/NTP [Configuration Service] .....	56
TINA [phion management centre] .....	467
TINA Tunnels [VPN] .....	220
Traffic Selection [Firewall] .....	169
Type 1 Admin [phion management centre] .....	413
Type 3 Admin [phion management centre] .....	413
TYPE1 [Configuration Service] .....	105,
[phion management centre] .....	413
TYPE2 [Configuration Service] .....	105
TYPE3 [Configuration Service] .....	105

**U**

UMTS [Configuration Service] .....	76
User Authorization [SSH Gateway] .....	366
User Groups [Firewall] .....	150
User List [VPN] .....	211
Userspecific [FTP Gateway] .....	353

**V**

V3 Extensions [phion management centre] .....	461
Virtual LANs [Configuration Service] .....	65
VPN FW [VPN] .....	219
VPN GTI Settings [phion management centre] .....	469
VPN Selection [VPN] .....	229
VPN Service [phion management centre] .....	468
VPN Settings [VPN] .....	229

**W**

Well-Known Services (WKS) [DNS] .....	321,
[DNS] .....	322
WWW [Firewall] .....	131

**X**

X25 (X25) [DNS] .....	322
xDSL/ISDN/DHCP [Configuration Service] .....	70

# 5. Parameter List Directory

## 1 Getting Started

List 1-1	Configuring Installation Settings with phion.i	10
List 1-2	Configuring System Settings with phion.i	11
List 1-3	Configuring System Settings with phion.i - section DNS	11
List 1-4	Configuring System Settings with phion.i - section Network Time Protocol	11
List 1-5	Configuring Partition Settings with phion.i	12
List 1-6	NIC Adapter configuration parameters	13
List 1-7	Configuring Security Settings with phion.i	13
List 1-8	Configuring Security Settings with phion.i - section Root Login	13
List 1-9	Configuring Security Settings with phion.i - section phion Login	13
List 1-10	Configuring Software Packages with phion.i - section Software Packages	13
List 1-11	Configuring Software Packages with phion.i - section Advanced	13
List 1-12	Configuring Script Settings with phion.i - section Installation scripts	14
List 1-13	Configuring Script Settings with phion.i - section Installation-script files	14
List 1-14	Configuring Script Settings with phion.i - section Box public key	14
List 1-15	Configuring USB Stick Settings with phion.i - section Installation Mode Settings (1)	14
List 1-16	Configuring USB Stick Settings with phion.i - section Installation Mode Settings (2)	15
List 1-17	Configuring phion.a settings - Client tab - section Compression	22
List 1-18	Configuring phion.a settings - Client tab - section Cryptography	22
List 1-19	Configuring phion.a settings - Client tab - section Timeouts	22
List 1-20	Configuring phion.a settings - Client tab - section System	22
List 1-21	Configuring phion.a settings - Client tab - section Show Short/Long Date	22
List 1-22	Configuring phion.a settings - Client tab - section Configuration Settings	22
List 1-23	Configuring phion.a settings - Client tab - section Desktop Background	22
List 1-24	Configuring phion.a settings - Client tab - section SSH Colours	22
List 1-25	Configuring Advanced Cryptographic API Settings	23
List 1-26	Configuring Advanced Cryptographic API Settings - section Store Parameters	23

## 2 Control Centre

List 2-1	Types of network activation	38
----------	-----------------------------	----

## 3 Configuration Service

List 3-1	Box Config - section Identification Settings	52
List 3-2	Box Config - section Operational Settings	53
List 3-3	Box Config - section VPN World Settings	53
List 3-4	Administrative Settings - System Access - section Root Password	54
List 3-5	Administrative Settings - System Access - section Service Password	54
List 3-6	Administrative Settings - System Access - section Access Control List	54
List 3-7	Administrative Settings - System Access - section Serial Access	54
List 3-8	Administrative Settings - section Advanced Access Settings	54
List 3-9	Administrative Settings - DNS - section Basic DNS Settings	55
List 3-10	Administrative Settings - DNS - section Advanced DNS Settings	55
List 3-11	Administrative Settings - Caching DNS Service - section Advanced DNS Settings	55
List 3-12	Administrative Settings - TIME/NTPs - section Time Settings	56
List 3-13	Administrative Settings - TIME/NTPs - section NTP Settings	56
List 3-14	Administrative Settings - SMS Control - section SMS Control Settings	58
List 3-15	Administrative Settings - SMS Control - section Access Limitations	58
List 3-16	Administrative Settings - SMS Control - section Command Codes	58
List 3-17	Administrative Settings - SCEP - section BOX SCEP Settings	58
List 3-18	Administrative Settings - SCEP - SCEP Settings - section SCEP Server	59
List 3-19	Administrative Settings - SCEP - SCEP Settings - section SCEP Server - section SCEP HTTP Server Authentication	59
List 3-20	Administrative Settings - SCEP - SCEP Settings - section SCEP X509 Request	59
List 3-21	Administrative Settings - SCEP - SCEP Settings - section SCEP X509 Request Password	59
List 3-22	Administrative Settings - SCEP - SCEP Settings - section Connection Details	59
List 3-23	Administrative Settings - SCEP - SCEP Settings - section Connection Details - section SCEP HTTP Proxy Settings	59
List 3-24	Administrative Settings - SCEP - SCEP Settings - section Encoding Parameters	59
List 3-25	Identity - section Box Certificate	60
List 3-26	Identity - section SSH Private Key	60
List 3-27	Network - Management Network - section Device Name	62
List 3-28	Network - Management Network - section Management Network	62
List 3-29	Box Network - section Network Interface Configuration	63
List 3-30	Network - Virtual LANs Configuration - section Virtual LAN Configuration	65
List 3-33	Remote Management Access - Tunnel Details - section Management Tunnel Configuration (MC-managed box)	67
List 3-34	Remote Management Access - Tunnel Details - section Connection Monitoring	67
List 3-31	Management Access - section Remote Management Tunnel	67
List 3-32	Management Access - section Serial Console	67
List 3-35	Remote Management Access - Tunnel Details - section Management Tunnel Configuration - M-series (vpnc3)	67
List 3-36	Network - section Main Routing Table	69

List 3-37	Network Routes - Policy Routing - section Policy Source Matching .....	70
List 3-38	Network Routes - Policy Routing - section Policy Table Contents .....	70
List 3-39	Network - xDSL configuration - section Link Properties .....	71
List 3-40	Network - xDSL configuration - section PPTP Connection Details .....	71
List 3-41	Network - xDSL configuration - section PPPOE Connection Details .....	72
List 3-42	Network - xDSL configuration - section Authentication .....	72
List 3-43	Network - xDSL configuration - section Routing .....	72
List 3-44	Network - xDSL configuration - section Connection Monitoring .....	73
List 3-45	Networks - DHCP configuration .....	73
List 3-46	Networks - DHCP configuration - section Connection Details .....	73
List 3-47	Networks - DHCP configuration - section DNS .....	73
List 3-48	Networks - DHCP configuration - section Routing .....	74
List 3-50	Networks - ISDN configuration - section Connection Details .....	74
List 3-49	Networks - DHCP configuration - section Connection Monitoring .....	74
List 3-51	Networks - ISDN configuration - section Compression .....	75
List 3-52	Networks - ISDN configuration - section Authentication .....	75
List 3-53	Networks - ISDN configuration - section Routing .....	75
List 3-54	Networks - ISDN configuration - section Connection Monitoring .....	76
List 3-55	Networks - UMTS configuration - section UMTS (3G) Setup .....	76
List 3-56	Networks - UMTS configuration - section UMTS Connection Details .....	76
List 3-57	Networks - UMTS configuration - section Authentication .....	77
List 3-58	Networks - UMTS configuration - section Routing .....	77
List 3-60	Connection monitoring of dynamic links - section Connection Monitoring .....	78
List 3-59	Networks - UMTS configuration - section Connection Monitoring .....	78
List 3-61	Networks - IP Tunnels configuration - section Tunnel Configuration .....	79
List 3-62	Integrity Check configuration - section Integrity Check Settings .....	80
List 3-63	The monitoring executable openxdsl and its commands .....	80
List 3-64	Traffic Shaping configuration .....	85
List 3-65	Traffic Shaping configuration - section Outbound (traffic sent over the device) .....	85
List 3-66	Traffic Shaping configuration - section Inbound (traffic received by device) .....	85
List 3-67	Device/Tunnel Tree Mapping .....	86
List 3-68	Traffic Shaping configuration - Shaping connector .....	87
List 3-69	Shape Connector Rule .....	87
List 3-70	Shape Connector Rule - section Condition .....	87
List 3-71	Traffic Shaping configuration .....	88
List 3-72	Traffic Shaping configuration - section Policy Definition .....	88
List 3-73	Traffic Shaping configuration - section Devices .....	88
List 3-74	Administrators configuration - section Account Description .....	91
List 3-75	Administrators configuration - section Administrator Authorization .....	91
List 3-76	Administrators configuration - section Administrator Authentication .....	91
List 3-77	Administrators configuration - section Administrator Access Control .....	91
List 3-78	Advanced Configuration - section License Configuration .....	93
List 3-79	Server configuration - General settings on single boxes - section Virtual Server Definition .....	95
List 3-80	Server configuration - General settings on single boxes - section Virtual Server IP Addresses .....	95
List 3-81	Server configuration (single box) - Monitoring settings - section Operation Mode .....	95
List 3-82	Server configuration (single box) - Monitoring settings - section IP Monitoring .....	95
List 3-83	Server configuration (single box) - Monitoring settings - section Interface Monitoring .....	95
List 3-84	Server configuration (single box) - Scripts configuration - section Server Scripts .....	96
List 3-85	Server configuration (MC) - General configuration - section Virtual Server Definition .....	96
List 3-86	Server configuration - IDENTITY tab - section Virtual Server Identity .....	96
List 3-87	Server configuration - NETWORKS tab - section Virtual Server/GTI Networks .....	96
List 3-88	Service Configuration - General - section Service Definition .....	97
List 3-89	Service Configuration - General - section Bind IPs .....	97
List 3-90	Service Configuration - General - section Available Server IPs .....	97
List 3-91	Service Configuration - Statistics - section Statistics Settings .....	97
List 3-92	Service Configuration - Notification - section Access Notification .....	98
List 3-93	System Settings - section General IP Settings .....	100
List 3-94	System Settings- section ARP Settings .....	100
List 3-95	System Settings - Routing Cache - section Routing Cache Settings .....	100
List 3-96	System Settings - Routing Cache - section Garbage Collection .....	100
List 3-97	System Settings - I/O Settings .....	101
List 3-98	Box Tuning - Flash Memory - section RAM Partition .....	101
List 3-99	Box Tuning - Flash Memory - section Log Settings .....	101
List 3-100	Box Tuning - Flash Memory - section Flash Appliance Settings .....	101
List 3-101	Advanced Configuration - Bootloader - section Kernel Updates .....	102
List 3-102	Advanced Configuration - Bootloader - section Header Settings .....	102
List 3-103	Advanced Configuration - Log Cycling - section Common Settings .....	104
List 3-104	Log Cycling - File Specific Settings - section Log File Selection .....	104
List 3-105	Log Cycling - File Specific Settings - section Log Cycling Actions .....	104
List 3-106	Box Misc - Log Cycling - File Specific Settings - section Log Cycling Actions .....	104
List 3-107	Box Misc - Access Notification - section Console Access .....	106
List 3-108	Box Misc - SSH Basic Setup - section General Settings .....	106
List 3-109	Box Misc - SSH Advanced Setup - section Protocol Version 2 Options .....	107
List 3-110	Box Misc - SSH Advanced Setup - section Protocol Version 1 Options .....	107

List 3-111	Advanced Configuration - Software Update - section Common Settings	108
List 3-112	Advanced Configuration - Software Update - section Release Check	108
List 3-113	Advanced Configuration - Watchdog Basic Setup - section Monitoring Policy	110
List 3-114	Advanced Configuration - Watchdog Basic Setup - section Watchdog Repair Policy	110
List 3-115	Advanced Configuration - Watchdog Details - section Watchdog Operational Setup	110
List 3-116	Advanced Configuration - Watchdog Details - section Watchdog Monitored Entities	111
List 3-117	MSAD Authentication	112
List 3-118	MSAD Authentication - Basic - section Basic	112
List 3-121	Parameters for MS-CHAP Authentication	112
List 3-119	MSAD Authentication - Basic - section Mail Lookup	112
List 3-120	MSAD Authentication - Basic - section Extended	112
List 3-122	Parameters for LDAP Authentication - section LDAP	113
List 3-123	Parameters for Radius Authentication	114
List 3-124	Parameters for RSA-ACE Authentication	114
List 3-125	Parameters for MSNT Authentication	114
List 3-126	Parameters for OSCP Authentication	115
List 3-127	Parameters for Explicit Authentication	115
List 3-128	Parameters for Timeouts and Logging - section Log Settings	115
List 3-129	Parameters for Timeouts and Logging - section Timeout Settings	115
List 3-130	Infrastructure Services - Syslog Streaming - Basic Setup - section Operational Setup	115
List 3-132	Infrastructure Services - Syslog Streaming - Logdata Filters - section Affected Box Logdata	116
List 3-133	Infrastructure Services - Syslog Streaming - Logdata Filters - section Affected Service Logdata	116
List 3-131	Infrastructure Services - Syslog Streaming - Basic Setup - section System Identification & Authentication	116
List 3-134	Infrastructure Services - Syslog Streaming - Logstream Destinations - section Destination Address	117
List 3-135	Infrastructure Services - Syslog Streaming - Logstream Destinations - section Data Transfer Setup	117
List 3-136	Infrastructure Services - Syslog Streaming - Logstream Destinations - section Log Data Tagging	117
List 3-137	Infrastructure Services - Syslog Streaming - Logdata Streams - section Stream Configuration	117
List 3-138	Infrastructure Services - Control - Monitoring Setup - section Monitoring Parameters	117
List 3-141	Infrastructure Services - Control - Administrative Sessions - section Auto Logout Setup	118
List 3-142	Infrastructure Services - Control - Administrative Sessions - section Session Password Setup	118
List 3-139	Infrastructure Services - Control - Monitoring Setup - section HA Monitoring Parameters	118
List 3-140	Infrastructure Services - Control - Monitoring Setup - section ICMP Gateway Monitoring Exemptions	118
List 3-143	Infrastructure Services - Control - CPU-Load Monitoring - section Performance	118
List 3-144	Infrastructure Services - Control - CPU-Load Monitoring - section CPU-Load Warning Thresholds	118
List 3-145	Infrastructure Services - Control - CPU-Load Monitoring - section CPU Load Error Thresholds	118
List 3-146	Infrastructure Services - Log Configuration - section Log Configuration	119

## 4 Firewall

List 4-1	Box Services - General Firewall Configuration - Peer-to-Peer Detection	126
List 4-2	General Firewall Configuration - Global Limits - section Session Limits and Memory Settings	127
List 4-3	General Firewall Configuration - Global Limits - section Access Cache Settings	127
List 4-4	General Firewall Configuration - Session Limits	127
List 4-5	General Firewall Configuration - Operational	128
List 4-6	General Firewall Configuration - Audit and Reporting tab - section Limits and Operational Settings	129
List 4-7	General Firewall Configuration - Audit and Reporting tab - section Eventing Settings	129
List 4-8	General Firewall Configuration - Audit and Reporting tab - section Audit Information Generation	129
List 4-9	General Firewall Configuration - Audit and Reporting tab - section Connection Tracing	129
List 4-10	General Firewall Configuration - Eventing Settings	129
List 4-11	Audit Information Generation - Settings - section Audit Info Transport	130
List 4-12	Audit Information Generation - Settings - section Recorded Conditions	130
List 4-13	General Firewall Configuration - Connection Tracing	131
List 4-14	Firewall Forwarding Settings - Firewall - section Server Specific Firewall Settings	131
List 4-15	Items of the Navigations Bar's main element "Configuration"	134
List 4-16	Subordinate elements of the item Information in the navigation bar	135
List 4-17	Firewall configuration - Rule Creation/Editing	136
List 4-18	Firewall configuration - Action section	136
List 4-19	Firewall configuration - Destination section	137
List 4-20	Firewall configuration - Redirection section	138
List 4-21	Firewall configuration - Connection section	139
List 4-22	Firewall configuration - Time Object	140
List 4-23	Net Object configuration parameters	140
List 4-24	Net Object configuration parameters - section Excluded Entry	140
List 4-25	Net Object configuration parameters - section Bridging	141
List 4-26	Network Object - Type Hostname	142
List 4-27	Network Object - Type Hostname - section Entry / Excluded Entry	142
List 4-28	Firewall configuration - Service Objects parameters - section TCP & UDP	144
List 4-29	Firewall configuration - Service Objects parameters - section ICMP Echo	144
List 4-30	Firewall configuration - Service Objects parameters - section General	144
List 4-31	Firewall configuration - Service Objects - General settings	145
List 4-32	Firewall configuration - Service Objects - General settings - section Failover and Load Balancing	146
List 4-33	Firewall configuration - Service Objects - General settings - section VPN Traffic Intelligence (TI) Settings	146
List 4-34	Firewall configuration - Service Objects - General settings - section BOB Settings	146
List 4-35	Proxy ARP object configuration values	151

List 4-36	Firewall configuration - Content Filter creation	152
List 4-37	Firewall configuration - Advanced Rule Parameters - section Rule Mismatch Policy	154
List 4-38	Firewall configuration - Advanced Rule Parameters - section TCP Policy	154
List 4-39	Firewall configuration - Advanced Rule Parameters - section Resource Protection	155
List 4-40	Firewall configuration - Advanced Rule Parameters - section Counting / Eventing / Audit Trail	155
List 4-41	Firewall configuration - Advanced Rule Parameters - section Miscellaneous	155
List 4-43	Firewall configuration - Enhanced Advanced Rule Parameters - section Rule Settings	156
List 4-42	Firewall configuration - Advanced Rule Parameters - section Quarantine Policy	156
List 4-44	Firewall configuration - Time Restriction	157
List 4-45	Firewall configuration - Accept Policy section - section Firewall configuration - Advanced Rule Parameters - section Resource Protection	157
List 4-46	Firewall configuration - Accept Policy section - section Firewall configuration - Advanced Rule Parameters - section TCP Policy	157
List 4-47	Firewall Forwarding Settings - Bridging - section Layer2 Bridging	184
List 4-48	Firewall Forwarding Settings - Bridging - section Quarantine Bridging	184
List 4-49	Firewall Forwarding Settings - Bridging - section Quarantine Bridging- Quarantine Group	184
List 4-50	Firewall configuration - Authentication parameters - section FW Authentication Server	188
List 4-51	Firewall configuration - PHIBS settings - section Phibs Authentication Settings	189
List 4-52	Firewall configuration - Rules - User Groups - section Authentication Pattern	190
List 4-53	Firewall configuration - Rules - User Groups - section Policy Roles Patterns	190
List 4-54	Firewall configuration - Rules - User Groups - section X509 Certificate Pattern	190
List 4-55	Firewall configuration - Rules - User Groups - section VPN User Pattern	190
List 4-56	Firewall configuration - Rules - User Groups - section Authentication Method	190
List 4-57	Firewall configuration - Forwarding Firewall - RPC tab - section RPC Settings	194
List 4-58	Firewall configuration - Forwarding Firewall - RPC tab - section ONCRPC Servers / DCERPC Servers	194

## 5 VPN

List 5-1	VPN configuration - Personal Network - section Network	206
List 5-2	VPN configuration - Server Certificates - General - section Policy Service	207
List 5-3	VPN configuration - Server Certificates - General - section Server Configuration	207
List 5-4	VPN configuration - Server Certificates - General - section Default Server Certificate	207
List 5-5	VPN configuration - Server Certificates - Advanced - section Device Configuration	207
List 5-6	VPN configuration - Server Certificates - Advanced - section IKE Parameters	207
List 5-8	VPN configuration- Root Certificates - Certificate details tab - section Certificate	208
List 5-9	VPN configuration- Root Certificates - Certificate details tab - section Usage	208
List 5-10	VPN configuration- Root Certificates - Certificate details tab - section CRL error handling	208
List 5-7	VPN configuration - Server Certificates - Advanced - section Custom Ciphers	208
List 5-11	VPN configuration - Root Certificates - Certificate revocation tab - section URI	208
List 5-14	VPN configuration- Root Certificates - OCSP tab - section OCSP Server	209
List 5-15	VPN configuration- Root Certificates - OCSP tab - section OCSP Server Identification	209
List 5-12	VPN configuration - Root Certificates - Certificate revocation tab - section Login	209
List 5-13	VPN configuration - Root Certificates - Certificate revocation tab - section Proxy	209
List 5-16	VPN configuration- VPN GTI Settings	210
List 5-17	VPN configuration- VPN GTI Settings - section Proxy	210
List 5-18	VPN configuration- L2TP/PPTP Settings - General - section Common Settings	210
List 5-20	VPN configuration- L2TP/PPTP Settings - PPTP - section PPTP Settings	211
List 5-19	VPN configuration- L2TP/PPTP Settings - L2TP/IPSEC - section L2TP Settings	211
List 5-21	VPN configuration- L2TP/PPTP Settings - User List	211
List 5-22	VPN configuration - Client to Site - Phion VPN CA tab - Personal License creation	213
List 5-23	VPN configuration - Client to Site - Phion VPN CA tab - Personal License creation - section IP Address & Networking	213
List 5-24	VPN configuration - Client to Site - Phion VPN CA tab - Personal License creation - section Password and Peer Restriction	213
List 5-25	VPN configuration - Client to Site - Phion VPN CA tab - Personal License creation - section Active Certificate / Obsolete Certificate	214
List 5-26	VPN configuration - Client to Site - Phion VPN CA tab - phion Template creation	214
List 5-27	VPN configuration - Client to Site - External CA tab > IPsec tab - section Phase 1 (default) / Phase 2	215
List 5-28	VPN configuration - Client to Site - External CA tab > IPsec tab - section Lifetime	215
List 5-29	VPN configuration - Client to Site - External CA tab > Phion tab - section Phion	216
List 5-30	VPN configuration - Client to Site - External CA tab > Phion tab - section Accepted Ciphers	216
List 5-31	VPN configuration - Client to Site - External CA tab > Common tab - section Common	217
List 5-32	VPN configuration - Client to Site - External CA tab > Common tab - section Network Routes	217
List 5-33	VPN configuration - Client to Site - External CA tab > Common tab - section ACL	217
List 5-34	VPN configuration - Client to Site - External CA tab > Rules tab > ... Group Match Settings ... - section X.509 Client Security	217
List 5-35	VPN configuration - Client to Site - External CA tab > Rules tab > ... Group Match Settings ... - section Server	217
List 5-37	VPN configuration - Client to Site - External CA tab > Rules tab > ... Group VPN Settings > Preauthentication Details	218
List 5-36	VPN configuration - Client to Site - External CA tab > Rules tab > ... Group Match Settings ... - section Preauthentication	218
List 5-38	VPN configuration - Client to Site - External CA tab > Rules tab > Group Policy Condition	218
List 5-39	VPN configuration - Client to Site - External CA tab > Rules tab > Group Policy Condition - section X509 Certificate Conditions	219
List 5-40	VPN configuration - Client to Site - External CA tab > Rules tab > Group Policy Condition - section External Group Condition	219
List 5-41	VPN configuration - Client to Site - External CA tab > Rules tab > Group Policy Condition - section Peer Condition	219
List 5-42	VPN configuration - Client to Site - Registry tab > New Registry Rule Set ... - section Registry Entry	219
List 5-43	VPN configuration - Site to Site - TINA Tunnels tab > New TINA tunnel ... - section General tunnel settings	221
List 5-44	VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... - section TI Transport Classification	224
List 5-45	Firewall Connection Object - VPN Traffic Intelligence (TI) - section TI Transport Selection	224
List 5-46	Firewall Connection Object - VPN Traffic Intelligence (TI) - section TI Traffic Prioritisation	225
List 5-47	VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... > TI tab - section Bandwidth Protection	225
List 5-48	VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... > TI tab - section VPN Envelope Policy	226



List 5-49	VPN configuration - Site to Site - TINA Tunnels tab > New TINA Tunnel ... > TI tab - section Transport (complement) .....	226
List 5-50	VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Base configuration tab .....	227
List 5-51	VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Base configuration tab - section Phase 1 and Phase 2 .....	227
List 5-52	VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Base configuration tab - section Networks .....	227
List 5-53	VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Authentication tab .....	228
List 5-54	VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Authentication tab - section Partner Identification .....	228
List 5-55	VPN configuration - Site to Site - IPSEC Tunnels tab > New IPsec tunnel ... > Authentication tab - section Parameters .....	228
List 5-56	VPN configuration - SSL-VPN - Basic Setup - section General Service Settings .....	231
List 5-57	VPN configuration - SSL-VPN - Basic Setup - section Service Identification .....	231
List 5-58	VPN configuration - SSL-VPN - Authentication & Login - section User Authentication .....	231
List 5-59	VPN configuration - SSL-VPN - Authentication & Login - section Corporate ID .....	232
List 5-60	VPN configuration - SSL-VPN - entegra Access Control - section entegra Access Control Setup .....	232
List 5-61	VPN configuration - SSL-VPN - Web Resources - section Web Resource Configuration .....	232
List 5-62	Web Resources - section Web Resource Access Authorization .....	232
List 5-63	VPN configuration - SSL-VPN - Outlook Web Access - section Outlook Web Access Authorization .....	232
List 5-64	VPN configuration - SSL-VPN - WebDAV/Sharepoint - section WebDAV Resource Configuration .....	232
List 5-65	WebDAV Resources - section WebDAV Resource Access Authorization .....	232
List 5-66	VPN configuration - SSL-VPN - Application Tunneling - section Application Tunneling Configuration .....	233
List 5-67	Application Tunneling Configuration - Service Configuration - section Application Access Authorization .....	233
List 5-68	Application Tunneling Configuration - Generic Application Tunneling - section Generic Application Tunneling Authorization .....	233
List 5-69	Generic Application Tunneling Authorization - SSL Tunnels - section SSL Tunnel Configuration .....	233
List 5-70	VPN configuration - SSL-VPN - Dynamic Firewall Rules - section Dynamic Firewall Rules .....	233
List 5-71	Firewall Rule Activation - section Dynamic Firewall Rule Activation Authorization .....	233
List 5-72	VPN configuration - SSL-VPN - Access Rights Query - section Access Rights Query .....	233

## 6 Mail Gateway

List 6-1	MailGW Settings - Basic Setup - section Host Configuration .....	247
List 6-2	MailGW Settings - Basic Setup - section Local Domain Settings .....	247
List 6-3	MailGW Settings - Basic Setup - section Global Domain Parameters .....	247
List 6-4	MailGW Settings - section Extended Domain Setup .....	247
List 6-5	MailGW Settings - section Extended Domain Setup - Domains .....	248
List 6-6	MailGW Settings - Pop3 Setup - section POP3 Setup .....	249
List 6-7	MailGW Settings - Advanced Setup - section Operational Settings .....	250
List 6-8	MailGW Settings - Advanced Setup - section Allowed Relaying .....	250
List 6-9	MailGW Settings - Advanced Setup - section Cloning and Archiving .....	251
List 6-10	MailGW Settings - Content Filter - Attachment Stripping - section Advanced Attachment Options .....	253
List 6-11	MailGW Settings - Content Filter - Grey Listing - section Advanced Grey Listing Options .....	254
List 6-12	MailGW Settings - Content Filter - Blacklists .....	254
List 6-13	MailGW Settings - Content Filter - HTML-Tag Removal .....	255
List 6-14	MailGW Settings - Content Filter - Misc .....	255
List 6-15	MailGW Settings - Limits - section Mail Gateway Limits .....	255
List 6-16	MailGW Settings - Limits - section DoS Protection .....	255
List 6-17	MailGW Settings - section Entries in Access Cache .....	256
List 6-18	MailGW Settings - Event Settings .....	256
List 6-19	MailGW Settings - Spam Analysis .....	259
List 6-20	Spamfilter Config - section Spamfilter Settings .....	260
List 6-21	Spamfilter Config - section WHITE/BLACK LISTS .....	260
List 6-22	Spamfilter Config - section ONLINE TESTS .....	260
List 6-25	Spamfilter Config - Advanced Network Settings .....	261
List 6-23	Spamfilter Config - section RULES .....	261
List 6-24	Spamfilter Config - section TRAINING OPTIONS .....	261
List 6-26	Spamfilter Config - section TRAINING OPTIONS .....	261

## 7 DHCP

List 7-1	DHCP Enterprise Configuration - Operational Setup - section Service Availability .....	273
List 7-2	DHCP Enterprise Configuration - Operational Setup - section HA Synchronisation Setup .....	273
List 7-3	DHCP Enterprise - Address Pool Configuration - section Address Pool Configuration .....	273
List 7-4	DHCP Enterprise - Address Pool Configuration - section Subnets .....	273
List 7-5	DHCP Enterprise - Address Pool Configuration - section Multi Subnet Configuration .....	274
List 7-6	DHCP Enterprise Configuration - SUBNETS tab - section Address Pools .....	274
List 7-7	DHCP Enterprise - Address Pool Configuration - section Further Subnets .....	274
List 7-8	DHCP Enterprise Configuration - Known Clients - section Group Based Assignment .....	275
List 7-9	DHCP Enterprise - Known Clients - Client Group Member - section Client Description .....	275
List 7-10	DHCP Enterprise - Known Clients - Client Group Member - section Client Match & Address Assignment .....	275
List 7-11	DHCP Enterprise - Known Clients - Client Group Member - section Advanced Client Assignments .....	275
List 7-12	DHCP Enterprise - DHCP Option Templates - section Template Description .....	276
List 7-13	DHCP Enterprise - DHCP Option Templates - section Basic Options .....	276
List 7-14	DHCP Enterprise - DHCP Option Templates - section entegra Policy Service Options .....	276
List 7-15	DHCP Enterprise - DHCP Option Templates - section Extended Options .....	276
List 7-16	DHCP Enterprise - Parameter Templates - section Template Description .....	277
List 7-17	DHCP Enterprise - Parameter Templates - section Lease Constraints .....	277
List 7-18	DHCP Enterprise - Parameter Templates - section Dynamic DNS Parameters .....	277

List 7-19	DHCP Enterprise - Parameter Templates - section Miscellaneous Parameters	277
List 7-20	DHCP Enterprise - Classes - section Class Configuration	278
List 7-21	DHCP Enterprise - Dynamic DNS - section DNS Update Configuration	278
List 7-22	DHCP Enterprise - Dynamic DNS - section DNS Authentication	278
List 7-23	DHCP Enterprise - GUI as Text	279
List 7-24	DHCP Enterprise - Text Based Configuration	279
List 7-25	DHCP Server Settings - section GLOBAL SETTINGS	283
List 7-26	DHCP Server Settings - section Option Section and IP RANGES	283
List 7-27	DHCP Server Settings - section SPECIAL CLIENTS	283
List 7-28	DHCP Server Settings - section BASIC OPTIONS	283
List 7-29	DHCP Server Settings - section EXTENDED OPTIONS	283
List 7-30	DHCP Relay Settings	286

## 8 Log Viewer

## 9 Statistics

List 9-1	Control field for type Curve with time axis - section Options	297
List 9-2	Control field for type Curve with time axis - section Time Interval - Curves	298
List 9-3	Control field for type Curve with time axis - section Time Interval - Bars	298
List 9-4	Infrastructure Services - Statistics General - section Global Settings	300
List 9-5	Box Services - Statistics Cooking - section Statistic Cooking - section Cook Settings	300
List 9-6	Statistic Cooking - section Type: Time	300
List 9-8	Statistic Transfer - Transfer Settings	301
List 9-7	Statistic Cooking - section Type: Top	301

## 10 Eventing

List 10-1	Events tab - Event details	307
List 10-3	Severity tab - Severity details	308
List 10-2	Severity tab - Column view	308
List 10-4	Notification tab - Column view	308
List 10-5	Server Action tab - Type SNMP	309
List 10-6	SNMP Notifications	311
List 10-7	SNMP Notifications - section Default SNMP	311
List 10-8	SNMP Notifications - section Default Mail	311
List 10-9	Event Properties - Page 1 tab	312
List 10-10	Event Properties - Page 2 tab - section Confirmed	312
List 10-11	Event Properties - Page 2 tab - section Time	312

## 11 DNS

List 11-1	DNS Server - Properties configuration - section Interface	317
List 11-2	DNS Server - Properties configuration - section Security	318
List 11-3	DNS Server - Zone configuration - section General	318
List 11-4	DNS Server - Zone configuration - Advanced Settings - section Interface	319
List 11-5	DNS Server - Zone configuration - Advanced Settings - section Security	319
List 11-6	DNS Server - SOA configuration	319
List 11-7	DNS Server - Name Server configuration	320
List 11-8	DNS Server - Adding a New Host - Host (A) tab	320
List 11-12	DNS Server - Adding a New Mail-Exchanger - Mail-Exchanger (MX) tab	321
List 11-13	DNS Server - Adding a New Mail-Exchanger - Mailbox information (MINFO) tab	321
List 11-14	DNS Server - Adding a New Mail-Exchanger - Well-Known Services (WKS) tab	321
List 11-9	DNS Server - Adding a New Host - Host Information (HINFO) tab	321
List 11-10	DNS Server - Adding a New Host - Text (TXT) tab	321
List 11-11	DNS Server - Adding a New Host - Well-Known Services (WKS) tab	321

## 12 Proxy

List 12-1	HTTP Proxy Service Parameters - General - section Basic Settings	325
List 12-2	HTTP Proxy Service Parameters - General - section Log Settings	325
List 12-3	HTTP Proxy Service Parameters - General - section Misc. Settings	325
List 12-4	HTTP Proxy Service Parameters - Network - section Network Settings	325
List 12-5	HTTP Proxy Service Parameters - General - Neighbour Settings	326
List 12-6	HTTP Proxy Service Parameters - General - Neighbour Settings - section Option Settings	326
List 12-7	HTTP Proxy Service Parameters - General - Neighbour Settings - section Cache Behaviour	326
List 12-8	HTTP Proxy Service Parameters - General - section SNMP	327
List 12-9	HTTP Proxy Service Parameters - Authentication Settings	327
List 12-10	HTTP Proxy Service Parameters - Authentication Settings - section PHIBS Specific Authentication Scheme	328
List 12-11	HTTP Proxy Service Parameters - Authentication Settings - ACL Entries	329
List 12-12	HTTP Proxy Service Parameters - Authentication Settings - Actions	331
List 12-13	HTTP Proxy Service Parameters - Authentication Settings - ACL FileList	331
List 12-14	ACL Filelist Usage Example	331
List 12-15	HTTP Proxy Service Parameters - Authentication Settings - Legacy	332

List 12-16	HTTP Proxy Service Parameters - Authentication Settings - Time Restriction configuration	332
List 12-17	ACL ENTRIES configuration	333
List 12-18	Proxy Service Parameters - section Data Leak Prevention	335
List 12-19	Proxy Service Parameters - Advanced view - section Optimizations	335
List 12-20	Proxy Service Parameters - Advanced view - section Advanced	335
List 12-21	Secure Web Proxy - section SSL Settings	338
List 12-22	Secure Web Proxy - SSL Certificates - section Certificate Verification	338
List 12-23	Secure Web Proxy - SSL Certificates - section Certificate Revocation	338
List 12-24	Secure Web Proxy - SSL Certificates - section Client Certificates	339
List 12-25	Proxy Service Parameters - section Redirector Settings	344
List 12-26	IIS Proventia Web Filter Configuration - General - section ISS Proventia General Settings	344
List 12-27	IIS Proventia Web Filter Configuration - General - section ISS Proventia Database Settings	344
List 12-28	IIS Proventia Web Filter Configuration - General - section ISS Proventia Support Options	344
List 12-29	IIS Proventia Web Filter Configuration - section ISS Proventia Proxy	344
List 12-30	IIS Proventia Web Filter Configuration - Filter Settings - section ISS Proventia Settings	345
List 12-31	IIS Proventia Web Filter Configuration - Filter Settings - section Configurations	345
List 12-32	IIS Proventia Web Filter Configuration - Filter Settings - section TIME SETTINGS	345
List 12-33	IIS Proventia Web Filter Configuration - section ISS Proventia Deny Message	346
List 12-34	IIS Proventia Web Filter Configuration - section ISS Proventia Exceptions	346
List 12-35	IIS Proventia Web Filter Configuration - section ISS Proventia Cascaded Redirector	346
List 12-36	IIS Proventia Web Filter Configuration - section ISS Proventia Logging Settings	346
List 12-37	IIS Proventia Web Filter Configuration - section ISS Proventia Limit Handling	347

### 13 FTP Gateway

List 13-1	FTP-GW Settings configuration - section BEHAVIOR	353
List 13-2	FTP-GW Settings configuration - section Virus Scanning	353
List 13-3	FTP-GW Settings configuration - section Logging	353
List 13-4	FTP-GW Settings Configuration - User specific - section Configuration Assignment	353
List 13-5	FTP-GW Settings Configuration - User specific - section Special Destinations	353
List 13-6	FTP-GW Settings Configuration - User specific - section Default User Specific	354
List 13-7	FTP-GW Settings Configuration - User specific - section Time Restrictions	354
List 13-8	FTP-GW Settings Configuration - User specific - Default User Specific - section SPECIAL DESTINATIONS	354
List 13-9	FTP-GW Settings Configuration - User specific - Default User Specific - section OTHER DESTINATIONS	354
List 13-10	FTP-GW Settings Configuration - User specific - Default User Specific - section Time Restrictions	354
List 13-11	FTP-GW Settings Configuration - section Local Authentication	354

### 14 Voice over IP

List 14-1	Firewall Forwarding Settings - H.323 Gatekeeper tab	359
List 14-2	Box Firewall Settings - SIP Parameters - section Access Cache Settings	360
List 14-3	Forwarding Firewall Settings - SIP Parameters	360

### 15 SSH Gateway

List 15-1	SSH Proxy configuration - General - section General Service Settings	365
List 15-2	SSH Proxy configuration - General - section Service Identification	365
List 15-3	SSH Proxy configuration - Authentication & Login - section User Authentication	365
List 15-4	SSH Proxy configuration - Authentication & Login - section User Session Handling	365
List 15-5	SSH Proxy configuration - Default Permissions - section Security Options	366
List 15-6	SSH Proxy configuration - Default Permissions - section Access Options	366
List 15-7	SSH Proxy configuration - Access Lists- section Access List Configuration	366
List 15-8	SSH Proxy configuration - Access Lists - Access List Configuration - section Access List Configuration	366
List 15-9	SSH Proxy configuration - Access Lists - Access List Configuration - section Allowed Host Configuration	366
List 15-10	SSH Proxy configuration - User Authorization	366

### 16 Anti-Virus

List 16-1	Virus Scanner Settings - Basic Setup - section Basic Setup	368
List 16-2	Virus Scanner Settings - Basic Setup - section Updates	368
List 16-5	Virus Scanner Settings - Archive Scanning - section Archive Scanning	369
List 16-6	Virus Scanner Settings - Scanning Options - section Non-Virus Detection	369
List 16-7	Virus Scanner Settings - Scanning Options - section HTTP Streaming	369
List 16-3	Virus Scanner Settings - Basic Setup - section Reporting	369
List 16-4	Virus Scanner Settings - Basic Setup - section Advanced	369
List 16-8	HTTP Proxy Settings - Content Inspection - section Virus Scanner	370
List 16-9	Content Inspection - section Virus Scanner - Progress Popup	370
List 16-10	MailGWSettings - Virus Scanning - section Virus Protection	371
List 16-11	MailGWSettings - Advanced Virus Protection Option - section Scanner Location	371
List 16-12	MailGWSettings - Advanced Virus Protection Option - section Notification	372
List 16-13	MailGWSettings - Advanced Virus Protection Option - section Adaptions	372
List 16-14	MailGWSettings - Advanced Virus Protection Option - section No Scan Exceptions	372
List 16-15	MailGWSettings - External Scan Engine	372

## 17 High Availability

## 18 phion management centre

List 18-1	Server configuration - Virtual Server Definition on MC boxes - section Virtual Server Definition	393
List 18-2	Schedule Task configuration	403
List 18-3	MC Identity - Identification - section MC Identification	412
List 18-4	MC Identity - Identification - section MC IP Addresses	412
List 18-5	MC Identity - Trust Chain Configuration - section Trust Chain Configuration	412
List 18-6	MC Identity - Trust Chain Configuration - section MC SSH Access Keys	413
List 18-7	MC Parameters - Operational Setup - section Status Map Setup	413
List 18-8	MC Parameters - Operational Setup - section Configuration Update Setup	413
List 18-9	MC Parameters - Operational Setup - section Remote Execution Setup	413
List 18-10	MC Parameters - Operational Setup - section VPN World Setup	413
List 18-11	Administrative Roles - Role Setup - Roles - section Role Name	414
List 18-12	Administrative Roles - Role Setup - Roles - section ... Module	414
List 18-13	Box VIP Network Ranges - VPN Settings	416
List 18-14	Creating a new range - section Identification	416
List 18-15	Creating a new range - section Contact Info	416
List 18-16	Creating a new range - section Specific Settings	416
List 18-17	Creating a new cluster - section Identification	418
List 18-18	Creating a new cluster - section Contact Information	418
List 18-19	Creating a new cluster - section Specific Settings	418
List 18-20	Creating a Cluster Service - section Service Definition	419
List 18-21	Creating a Cluster Service - section Admin Restrictions	419
List 18-22	Creating a Cluster Service - section Access Notification	419
List 18-23	management centre Node Properties	420
List 18-24	management centre Node Properties - section Administrative Level	420
List 18-25	Creating a new administrator - Administrator tab - section General	433
List 18-26	Creating a new administrator - Details tab - section Password Parameters	434
List 18-27	Creating a new administrator - Administrator tab - section Administrative Scope	434
List 18-28	Creating a new administrator - Administrator tab - section Operative Settings	435
List 18-29	Master Statistic Collection Configuration	436
List 18-30	Statistics Cook Settings - section Global Settings	438
List 18-31	Statistics Cook Settings - Statistics Cooking - section Cook Settings	438
List 18-32	Statistics Cook Settings - Statistics Cooking - section Type: Time	439
List 18-33	Statistics Cook Settings - Statistics Cooking - section Type: Top	439
List 18-34	Statistics Cook Settings - Transfer Settings	440
List 18-35	MC Syslog Server configuration - section Operational Setup	447
List 18-36	MC Syslog Server configuration - section Plain Data Reception	448
List 18-38	MC Syslog Server configuration - Trusted Data Reception	448
List 18-37	MC Syslog Server configuration - section Tuning Parameters	448
List 18-40	MC Syslog Server configuration - Local Storage Setup - section Local Log Directory	449
List 18-39	MC Syslog Server configuration - Trusted Data Reception - section <b>SSL</b> Client Authentication	449
List 18-41	MC Syslog Server configuration - HA Synchronization - section HA Synchronization Setup	449
List 18-42	MC Syslog Server configuration - Relaying Setup - section Relaying Setup	450
List 18-43	MC Syslog Server configuration - Relaying Setup - section SSL Delivery Setup	450
List 18-44	MC Syslog Server configuration - Relay Filters - section Data Origin	450
List 18-45	MC Syslog Server configuration - Relay Filters - section Data Selection	450
List 18-46	MC Syslog Server configuration - Relay Destinations - section Connection Type Setup	451
List 18-47	MC Syslog Server configuration - Relay Destinations - section Connect by Destination SSL Setup	451
List 18-48	MC Syslog Server configuration - Relay Destinations - section Stream to Destination Setup	451
List 18-49	MC Syslog Server configuration - Relay Destinations - section Data Tag Policy	451
List 18-50	MC Syslog Server configuration - Relay Streams - section Relay Streams	452
List 18-51	Public Key Infrastructure (PKI) Configuration Settings - section General Settings	459
List 18-52	Public Key Infrastructure (PKI) Configuration Settings - section LDAP Server	459
List 18-53	Public Key Infrastructure (PKI) - Certificate Creation	460
List 18-54	Public Key Infrastructure (PKI) - Certificate Creation - General Settings tab	460
List 18-55	Public Key Infrastructure (PKI) - Certificate Creation - Subject tab	461
List 18-56	Public Key Infrastructure (PKI) - Certificate Creation - V3 Extensions tab	461
List 18-57	VPN GTI Editor - Group Edit - TINA tab - section General Settings	467
List 18-58	VPN GTI Editor - Group Edit - TINA tab - section Accepted Ciphers	467
List 18-59	VPN GTI Editor - Group Edit - TINA tab - section Bandwidth Protection	467
List 18-60	VPN GTI Editor - Group Edit - TINA tab - section VPN Envelope Policy	467
List 18-61	VPN GTI Editor - Group Edit - IPsec tab - section Phase 1 / Phase2	468
List 18-62	VPN GTI Editor - Group Edit - IPsec tab - section General Settings	468
List 18-63	VPN GTI Editor - Adding a VPN Service to a VPN Group - section Server/Service	468
List 18-64	VPN GTI Editor - Adding a VPN Service to a VPN Group - section Attributes	468
List 18-65	VPN GTI Editor - Adding a VPN Service to a VPN Group - section Tunnels	468
List 18-66	VPN GTI Editor - Adding a VPN Service to a VPN Group - section In Groups	468
List 18-67	VPN world - section Graphics	471
List 18-68	VPN world - section Connection to MC	472
List 18-69	MC Parameters - RCS Setup	473

List 18-70 RCS Change Filter settings ..... 476

**19 SNMP**

List 19-1 SNMP Configuration - section Access Groups ..... 481

**20 OSPF and RIP**

List 20-1 OSPF/RIP Settings - section Operational Setup ..... 485

List 20-2 OSPF/RIP Settings - OSPF Preferences - section OSPF Preferences Configuration ..... 485

List 20-3 OSPF/RIP Settings - OSPF Preferences - section RIP SETTINGS ..... 486

List 20-4 OSPF/RIP Settings - OSPF Router Setup - section OSPF Router Configuration ..... 486

List 20-6 OSPF/RIP Settings - section OSPF Area Configuration ..... 487

List 20-5 OSPF/RIP Settings - OSPF Router Setup - section Router Distribution Configuration ..... 487

List 20-7 OSPF/RIP Settings - RIP Router Setup - section RIP Router Configuration ..... 487

List 20-8 OSPF/RIP Settings - RIP Router Setup - section Router Distribution Configuration ..... 488

List 20-9 OSPF/RIP Settings - RIP Preferences - section RIP Preferences Configuration ..... 488

List 20-10 OSPF/RIP Setting - section Network Interface Configuration ..... 489

List 20-11 OSPF/RIP Settings - Network Interfaces Configuration - Interfaces - section Shared Interface Configuration ..... 489

List 20-12 OSPF/RIP Settings - Network Interfaces Configuration - Interfaces - section OSPF Specific Parameters ..... 489

List 20-13 OSPF/RIP Settings - Network Interfaces Configuration - Interfaces - section RIP Specific Parameters ..... 489

List 20-14 OSPF/RIP Settings - Network Interfaces Configuration - Available Interfaces - section Available Interfaces ..... 489

List 20-15 OSPF/RIP Settings - Network Interfaces Configuration - Parameter Template Configuration - section OSPF Parameters ..... 489

List 20-16 OSPF/RIP Settings - Network Interfaces Configuration - Parameter Template Configuration - section RIP Parameters ..... 489

List 20-17 OSPF/RIP Settings - Neighbor Setup - section Neighbors ..... 489

List 20-19 OSPF/RIP Settings - Filter Setup - section Access List Filters ..... 490

List 20-20 OSPF/RIP Settings - Filter Setup - Route Map Filters - section Route Map Filters ..... 490

List 20-21 OSPF/RIP Settings - Filter Setup - Route Map Filters - section Route Map Configuration ..... 490

List 20-22 OSPF/RIP Settings - Filter Setup - Route Map Filters - section OSPF Specific Conditions ..... 490

List 20-23 OSPF/RIP Settings - Filter Setup - Route Map Filters - section RIP Specific Conditions ..... 490

List 20-24 OSPF/RIP Settings - Filter Setup - IP Prefix List Filters - section IP Prefix List Filters ..... 490

List 20-25 OSPF/RIP Settings - Filter Setup - IP Prefix List Filters - section IP Prefix List Configuration ..... 490

List 20-18 OSPF/RIP Settings - Neighbor Setup - section OSPF Parameters ..... 490

List 20-26 OSPF/RIP Settings - GUI as Text - section Text Equivalent of GUI ..... 491

List 20-27 OSPF/RIP Settings - Text Based Configuration - section Free Format OSPF Configuration / Free Format RIP Configuration ..... 491

**21 Licensing**

**22 System Information**

**23 Appendix**

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

## 6. Index of Configuration Parameters

### Numerics

2-Way [Firewall] .....	136,
[Firewall] .....	137,
[Firewall] .....	150

### A

ABR Type [OSPF and RIP] .....	486
Accept Identification Type [VPN] .....	210,
[phion management centre] .....	467
Accept Limit Exceeded [Firewall] .....	129
Accept Loose Domain Name [Mail Gateway] .....	255
Accept Policy [Firewall] .....	128
Accept Timeout (s) [Firewall] .....	154
Accepted Ciphers [VPN] .....	215,
[phion management centre] .....	467
Accepted Identification Type [phion management centre] .....	468
Access Cache Entry [Firewall] .....	155
Access Cache Management [phion management centre] .....	415
Access Concentrator [Configuration Service] .....	72
Access Configuration [Proxy] .....	328
Access Control Entries [Proxy] .....	332
Access Control Policy [SSH Gateway] .....	366
Access Lists [SSH Gateway] .....	366
Access Password [Configuration Service] .....	72,
[Configuration Service] .....	73,
[Configuration Service] .....	75,
[Configuration Service] .....	77
Access to MC PKI [phion management centre] .....	414
Access Type [Configuration Service] .....	54
Account [Mail Gateway] .....	261
Account Info Length [FTP Gateway] .....	353
ACK Timeout [Voice over IP] .....	360
ACL [Getting Started] .....	13,
[Configuration Service] .....	54,
[VPN] .....	217,
[Mail Gateway] .....	248
ACL Description [Proxy] .....	331
ACL Entries [Proxy] .....	331
ACL Entries for this Action [Proxy] .....	331
ACL Filelist [Proxy] .....	331
ACL list [VPN] .....	214
ACL Name [OSPF and RIP] .....	490
ACL Priority [Proxy] .....	331
ACL Type [Proxy] .....	329
ACLs [OSPF and RIP] .....	488
ACPF Allowed Msg Buffer [Firewall] .....	130
ACPF Blocked Msg Buffer [Firewall] .....	130
ACPF Dropped Msg Buffer [Firewall] .....	130
ACPF Memory (MB) [Firewall] .....	127
Action [Configuration Service] .....	104,
[Firewall] .....	152,
[VPN] .....	208,
[VPN] .....	219,
[Proxy] .....	331
Activate Config for [OSPF and RIP] .....	489
Activate Driver [Configuration Service] .....	63
Activate Kernel Update [phion management centre] .....	414
Activate New Configuration [phion management centre] .....	414
Activate Scheme [Configuration Service] .....	112,
[Configuration Service] .....	113,
[Configuration Service] .....	114,
[Configuration Service] .....	115
Activation Lag [Configuration Service] .....	65
Active [Configuration Service] .....	117,
[Firewall] .....	178,
[VPN] .....	232,
[VPN] .....	233,
[phion management centre] .....	452,
[OSPF and RIP] .....	489
Active 2nd Channel [Configuration Service] .....	76
Active Box [Configuration Service] .....	95
Active Content Rewrite [VPN] .....	232
Active directory searching user [Configuration Service] .....	112
Active Sync (DOWN) [Firewall] .....	172
Active Sync (UP) [Firewall] .....	172
Active Zone [Configuration Service] .....	56
AD searching user password [Configuration Service] .....	112
Add Agent ID (AID) [DHCP] .....	286
Add Body to Notice [Anti-Virus] .....	372

Add Group [phion management centre] .....	465
Add Status in Body [Anti-Virus] .....	372
Add UTC Offset [Configuration Service] .....	117
Add VPN Service to GTI Editor [phion management centre] .....	465
Add VPN Services to GTI Group [phion management centre] .....	466
Add X-Status in Header [Anti-Virus] .....	372
Additional Addresses (NAT) [Firewall] .....	194
Additional gateway route [Getting Started] .....	13
Additional Interfaces [Firewall] .....	151
Additional IP [Configuration Service] .....	95
Additional IP Addresses [Configuration Service] .....	62
Additional Mail Fields [Configuration Service] .....	112
Additional MC IP Addresses [phion management centre] .....	412
Additional Pattern [Mail Gateway] .....	248
Address Control [Configuration Service] .....	75
Address Pools [DHCP] .....	274
Address Selection [Firewall] .....	146
Admin [phion management centre] .....	476
Admin Connections [Mail Gateway] .....	250
Admin Discard Mail Cmd [Mail Gateway] .....	256
Admin Distance [OSPF and RIP] .....	486
Admin Reception Commands [Mail Gateway] .....	256
Administered by [phion management centre] .....	419
Administrative Distance [OSPF and RIP] .....	488
Advanced Attachments Options [Mail Gateway] .....	253
Advanced Cryptographic Settings [Getting Started] .....	22
Advanced Grey Listing Options [Mail Gateway] .....	254
Advanced IDE Options [Configuration Service] .....	101
Advanced Mode Configuration [Getting Started] .....	22
Advanced RAW ISAKMP settings [VPN] .....	228
Advanced Settings [OSPF and RIP] .....	486,
[OSPF and RIP] .....	488
Advanced Spam Options [Mail Gateway] .....	259
Advanced Virus Protection Option [Anti-Virus] .....	371
Advertise Route [Configuration Service] .....	62,
[Configuration Service] .....	69,
[Configuration Service] .....	73,
[Configuration Service] .....	74,
[Configuration Service] .....	76,
[Configuration Service] .....	78,
[Configuration Service] .....	79,
[VPN] .....	222
Advertise via OSPF [VPN] .....	206
Advertised Range [OSPF and RIP] .....	487
Affected Box Logfiles [phion management centre] .....	450
Affected Groups [Proxy] .....	345,
[FTP Gateway] .....	353
Affected IPs for Anonymous [FTP Gateway] .....	353
Affected Networks [Proxy] .....	345
Affected Service Logfiles [phion management centre] .....	451
Affected Users [Proxy] .....	345,
[FTP Gateway] .....	353
AID Relay Policy [DHCP] .....	286
Alarm [Eventing] .....	312
Alarm Period [Configuration Service] .....	67
Aliases [Configuration Service] .....	55
ALL [SNMP] .....	481
All Clients Policy [DHCP] .....	274
all-OR-all-present [Configuration Service] .....	95
Allow Active-Active Mode [Firewall] .....	128
Allow Block Virus Pattern Update [phion management centre] .....	415
Allow Bulk Transports [VPN] .....	225
Allow CommonName Wildcards [Proxy] .....	338
Allow Compression [Configuration Service] .....	77,
[Configuration Service] .....	107
Allow Config View on Box [phion management centre] .....	414
Allow Emergency Override [phion management centre] .....	414
Allow Fallback Transports [VPN] .....	225
Allow Inbound Compression [SSH Gateway] .....	365,
[SSH Gateway] .....	366
Allow Local Access [SSH Gateway] .....	366
Allow Manual Virus Pattern Update [phion management centre] .....	415
allow notify [DNS] .....	318,
[DNS] .....	319
Allow Public Keys [SSH Gateway] .....	366
Allow Quality Transports [VPN] .....	225
allow query [DNS] .....	318,
[DNS] .....	319
allow recursion [DNS] .....	318



Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Allow Relaying from [Mail Gateway] ..... 247,  
 [Mail Gateway] ..... 248  
 Allow SSLv2 [VPN] ..... 231  
 Allow TCP Forwarding [Configuration Service] ..... 107  
 allow transfer [DNS] ..... 318,  
 [DNS] ..... 319  
 allow update [DNS] ..... 319  
 Allow Visit After Confirm [Proxy] ..... 338  
 Allowed Broadcast Reply [DHCP] ..... 275  
 Allowed Classes [DHCP] ..... 274  
 Allowed Hosts [SSH Gateway] ..... 366  
 Allowed Hosts List [SSH Gateway] ..... 366  
 Allowed Local Sessions [Firewall] ..... 130  
 Allowed MIME-Types [Anti-Virus] ..... 369  
 Allowed Networks [Firewall] ..... 184  
 Allowed Phone Numbers [Configuration Service] ..... 58  
 Allowed Sessions [Firewall] ..... 130  
 Allowed URLs per IP [Proxy] ..... 347  
 Allowed URLs per User [Proxy] ..... 347  
 Allowed User Groups [VPN] ..... 231,  
 [VPN] ..... 232,  
 [VPN] ..... 233,  
 [SSH Gateway] ..... 365  
 also notify [DNS] ..... 319  
 Alternative [Firewall] ..... 146  
 Alternative HA IP [Configuration Service] ..... 118  
 Alternative Name [Configuration Service] ..... 59  
 AltName [Firewall] ..... 190  
 Always Keep (File instances) [Configuration Service] ..... 104  
 Always use session password [Getting Started] ..... 22  
 Analyse Internal Mails [Mail Gateway] ..... 259  
 APN Name [Configuration Service] ..... 76  
 Appliance Model [Configuration Service] ..... 52,  
 [Configuration Service] ..... 63  
 Application Protocol [VPN] ..... 233  
 Application Server IP [VPN] ..... 233  
 Application TCP Port [VPN] ..... 233  
 Apply to Device [OSPF and RIP] ..... 489  
 Architecture [Getting Started] ..... 13  
 Archiving Settings [Mail Gateway] ..... 251  
 Area Default Cost [OSPF and RIP] ..... 487  
 Area Export Filters [OSPF and RIP] ..... 487  
 Area ID Format [OSPF and RIP] ..... 487  
 Area Import Filters [OSPF and RIP] ..... 487  
 Area in Filters [OSPF and RIP] ..... 487  
 Area out Filters [OSPF and RIP] ..... 487  
 ARP Cache Size [Configuration Service] ..... 100  
 ARP Reverse Route Check [Firewall] ..... 128  
 ARP Src IP Announcement [Configuration Service] ..... 100  
 Assigned Network [VPN] ..... 217  
 Assigned Range [phion management centre] ..... 434  
 Assigned Source IP [Configuration Service] ..... 69  
 Assigned Virtual Tree [Configuration Service] ..... 86  
 Assigned VPN Group Policy [VPN] ..... 218  
 Associated Netmask [Configuration Service] ..... 62  
 Assumed Rate [Configuration Service] ..... 85,  
 [Configuration Service] ..... 86  
 at [SNMP] ..... 481  
 Attachment Stripping [Mail Gateway] ..... 253  
 Audit Delivery [Firewall] ..... 130  
 Authenticated User [Firewall] ..... 156  
 Authentication [Firewall] ..... 155,  
 [VPN] ..... 222,  
 [Proxy] ..... 326,  
 [phion management centre] ..... 467  
 Authentication error page [Firewall] ..... 188  
 Authentication index page [Firewall] ..... 189  
 Authentication Level [Configuration Service] ..... 91,  
 [phion management centre] ..... 434  
 Authentication logout page [Firewall] ..... 189  
 Authentication Method [Configuration Service] ..... 72,  
 [Configuration Service] ..... 75,  
 [Configuration Service] ..... 77  
 Authentication Mode [Getting Started] ..... 13,  
 [Configuration Service] ..... 54  
 Authentication Scheme [VPN] ..... 217,  
 [VPN] ..... 231,  
 [SSH Gateway] ..... 365  
 Authentication Scheme General [Proxy] ..... 327  
 Authentication success page [Firewall] ..... 188  
 Authentication Sync Zone [Configuration Service] ..... 53  
 Authentication Text [Proxy] ..... 328  
 Authentication Text MS-CHAP [Proxy] ..... 327

Authentication Type [Configuration Service] ..... 59,  
 [OSPF and RIP] ..... 487,  
 [OSPF and RIP] ..... 489  
 Authentication Worker [Proxy] ..... 328  
 Authentication Worker MS-CHAP [Proxy] ..... 327  
 authorityInfoAccess [phion management centre] ..... 461  
 authorityKeyIdentifier [phion management centre] ..... 461  
 Authorized Root Keys [Configuration Service] ..... 55  
 Auto white list (senders) [Mail Gateway] ..... 254  
 Auto-Cost Ref Bwidth [OSPF and RIP] ..... 486  
 Automatic Hostname Assignment [DHCP] ..... 275  
 Automatically Detect MIME-Type [Mail Gateway] ..... 253  
 Availability [Configuration Service] ..... 64  
 Average 1/5/15 Mins [Configuration Service] ..... 118  
 AVIRA license [Anti-Virus] ..... 368

**B**

Backup Box [Configuration Service] ..... 95  
 Backup MX [Configuration Service] ..... 72,  
 [Configuration Service] ..... 74,  
 [Configuration Service] ..... 75,  
 [Configuration Service] ..... 77  
 Bad Rulefile Loaded [Mail Gateway] ..... 256  
 Balance Preferred and Second [VPN] ..... 224  
 Balanced Timeout [Firewall] ..... 144  
 Band [Firewall] ..... 156  
 Band A-G [Configuration Service] ..... 88  
 Band Policy [VPN] ..... 226,  
 [VPN] ..... 228  
 Bandwidth [Configuration Service] ..... 88,  
 [OSPF and RIP] ..... 489  
 Bandwidth Policy [VPN] ..... 225  
 Base DN [Configuration Service] ..... 112,  
 [phion management centre] ..... 459  
 Basic [Configuration Service] ..... 112  
 basicConstraints [phion management centre] ..... 461  
 Bind IP [Anti-Virus] ..... 372  
 Bind IPs [VPN] ..... 231  
 Bind NTPd [Configuration Service] ..... 62  
 Bind policy [FTP Gateway] ..... 353  
 Bind To Authenticate [Configuration Service] ..... 113  
 Bind Type [Configuration Service] ..... 97  
 Bitmap [VPN] ..... 214,  
 [VPN] ..... 216  
 BK Colour... [Getting Started] ..... 22  
 Black List [Proxy] ..... 345  
 blackhole [DNS] ..... 318  
 Blacklist From [Mail Gateway] ..... 260  
 Blacklists [Mail Gateway] ..... 254  
 Block [Firewall] ..... 136,  
 [Firewall] ..... 137,  
 [Firewall] ..... 138,  
 [Firewall] ..... 139,  
 [Firewall] ..... 159,  
 [Firewall] ..... 162  
 Block & Terminate [Firewall] ..... 159  
 Block Box Sync [phion management centre] ..... 415  
 Block encrypted archives [Anti-Virus] ..... 369  
 Block if mismatch [Firewall] ..... 140,  
 [Firewall] ..... 157,  
 [Proxy] ..... 332  
 Block If User Limit Exceeded [Proxy] ..... 347  
 Block on error [Anti-Virus] ..... 369  
 Block on Mismatch [Firewall] ..... 154  
 Block Server [phion management centre] ..... 414  
 Block Service [phion management centre] ..... 414  
 Block Unknown State [Proxy] ..... 338  
 Block unsupported archives [Anti-Virus] ..... 369  
 Block Update [phion management centre] ..... 399  
 Blocked Local Sessions [Firewall] ..... 130  
 Blocked Sessions [Firewall] ..... 130  
 Blocked User Groups [VPN] ..... 231,  
 [SSH Gateway] ..... 365  
 Blocked Users [SSH Gateway] ..... 366  
 BOB Settings [Firewall] ..... 146  
 Boot File [DHCP] ..... 277  
 Boot File Name [DHCP] ..... 277,  
 [DHCP] ..... 284  
 Boot File Server [DHCP] ..... 277  
 Boot Loader Location [Configuration Service] ..... 102  
 Boot Unknown Clients [DHCP] ..... 277  
 BOOTP Clients Policy [DHCP] ..... 274  
 Boottime Release Check [Configuration Service] ..... 108

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Box [Firewall] .....	190,
[Eventing] .....	312
Box Authentication [phion management centre] .....	403
Box Certificate [Configuration Service] .....	60
Box DNS Domain [Configuration Service] .....	55
Box Inventory [Configuration Service] .....	103
Box Log Patterns [phion management centre] .....	451
Box Name [Configuration Service] .....	52
Box Private Key [Configuration Service] .....	60
Box Reachable Statistics [phion management centre] .....	413
Box Unique Name [Configuration Service] .....	52
Box->MC Access [Configuration Service] .....	53
Bridging Device [Firewall] .....	184
Bridging Group [Firewall] .....	184
Bridging TTL Policy [Firewall] .....	184
Broadcast Address [DHCP] .....	276,
[DHCP] .....	283
Broadcast RAS [Voice over IP] .....	359
Broad-Multicast [Firewall] .....	137,
[Firewall] .....	138,
[Firewall] .....	139
Browse... [Getting Started] .....	22
Browser Cleanup [VPN] .....	232
Browser Config [Proxy] .....	330
Browsers [Anti-Virus] .....	370
BSD [Configuration Service] .....	75
Buffer-overflow protection [FTP Gateway] .....	353
Bump Mapping [phion management centre] .....	471
Transfer Rate Limit [Configuration Service] .....	75

## C

CA Root [VPN] .....	209
CA Sign Password [phion management centre] .....	460
Cache Direct Objects [Proxy] .....	326
Cache Domain Objects [Proxy] .....	326
Cache IP Objects [Proxy] .....	326
Cache MSAD-groups [Configuration Service] .....	112
Cache Peer Access [Proxy] .....	326
Cache Priority [Proxy] .....	326
Call Redirect [Voice over IP] .....	359
Cascade [Firewall] .....	137,
[Firewall] .....	138,
[Firewall] .....	139
Cascade Back [Firewall] .....	137,
[Firewall] .....	138,
[Firewall] .....	139
Cascaded is Primary [Proxy] .....	346
Cascaded Redirector [Proxy] .....	346
Cascading Included [phion management centre] .....	440
Categories [Proxy] .....	345
CCP Control Protocol [Configuration Service] .....	75
Cert. Authorities Management [phion management centre] .....	415
Certificate Login Matching [VPN] .....	217
Certificate Mgmt... [VPN] .....	214
Certificate Policy [VPN] .....	219
Challenge Timeout (sec) [Configuration Service] .....	115
Change Events [phion management centre] .....	414
Change HW clock to UTC [Getting Started] .....	12
Change Permissions [phion management centre] .....	414
Change Personal Network [VPN] .....	206
Change Server Password... [VPN] .....	214
Change Settings [phion management centre] .....	415
Channel Bonding Settings [Configuration Service] .....	75
Check Interval [Configuration Service] .....	78,
[Configuration Service] .....	110
Check Reachability [Configuration Service] .....	79
Check Spam [Mail Gateway] .....	250
Check System Load [Configuration Service] .....	111
Check User Home [Configuration Service] .....	107
Class [Eventing] .....	312
Clear [Getting Started] .....	22
Clear DF Bit [Firewall] .....	155
Clear Filter - deletes the set filter [phion management centre] .....	466
Clear Log [phion management centre] .....	403
Clear Log ... [phion management centre] .....	403
Clear on Failure [Configuration Service] .....	108
Clear on Success [Configuration Service] .....	108
Client [Firewall] .....	146,
[Firewall] .....	162
Client Alive Interval [SSH Gateway] .....	365
Client Alive Max Count [SSH Gateway] .....	365

Client Authentication [phion management centre] .....	449
Client Certificate Action [Proxy] .....	339
Client Description [DHCP] .....	275
Client DHCP Options [DHCP] .....	275
Client Hostname [DHCP] .....	276
Client Log Level [SSH Gateway] .....	366
Client Loopback TCP Port [VPN] .....	233
Client Parameters [DHCP] .....	275
Client Port Used [Firewall] .....	144
Client Updates [DHCP] .....	278
Clone Routes [Configuration Service] .....	73,
[Configuration Service] .....	74,
[Configuration Service] .....	76,
[Configuration Service] .....	76
Closing [Firewall] .....	169
Cluster [phion management centre] .....	435
Cluster Name [phion management centre] .....	418
Collect Statistics [Configuration Service] .....	53,
[phion management centre] .....	416,
[phion management centre] .....	418
Color [Firewall] .....	155,
[phion management centre] .....	468
Comment [VPN] .....	208,
[Eventing] .....	307
Common Name [Configuration Service] .....	59,
[phion management centre] .....	461
Community [Eventing] .....	309,
[Proxy] .....	327,
[SNMP] .....	481
Complete Update [phion management centre] .....	399
Completed [phion management centre] .....	399
Compression [Configuration Service] .....	104,
[VPN] .....	224
Condense after (days) [phion management centre] .....	439
Condense Data after (Days) [Statistics] .....	301
Configuration Level [phion management centre] .....	435
Configuration Read [Getting Started] .....	22
Configurations [Proxy] .....	345
Confirm Events [phion management centre] .....	414
Confirmed [Eventing] .....	312
Connect Timeout [Configuration Service] .....	76
Connection Color [Firewall] .....	145
Connection Timeout [Firewall] .....	146
Connection Type [Configuration Service] .....	71,
[phion management centre] .....	451
Connections [Firewall] .....	134
Consistency Verification [Configuration Service] .....	80
Console Max. Idle [Configuration Service] .....	118
Console(COM)AndManagement [Configuration Service] .....	54
ConsoleOnly(COM1) [Configuration Service] .....	54
Contact Info [SNMP] .....	481
Contact Mail [Proxy] .....	325,
[Anti-Virus] .....	368
Contact Person [phion management centre] .....	416,
[phion management centre] .....	418
Content [VPN] .....	219
Content Filter [Firewall] .....	134
Context Identifier [Configuration Service] .....	77
Continue if mismatch [Firewall] .....	140,
[Firewall] .....	157
Continue on Mismatch [Firewall] .....	150,
[Firewall] .....	154
Control Permissions [phion management centre] .....	414
Cookie Server [DHCP] .....	276,
[DHCP] .....	284
Cookie Timeout (Min.) [VPN] .....	231
Copy to Obsolete [VPN] .....	214
Corrupted Data Action [Statistics] .....	300,
[phion management centre] .....	438
Count Destination IP [Firewall] .....	155
Count Source IP [Firewall] .....	155
Country [Configuration Service] .....	59,
[phion management centre] .....	461
Create Boxes [phion management centre] .....	414
Create Cluster [phion management centre] .....	414
Create Copy ... [phion management centre] .....	403
Create Default Route [Configuration Service] .....	72,
[Configuration Service] .....	74,
[Configuration Service] .....	76,
[Configuration Service] .....	77
Create New Key [VPN] .....	214
Create PAR File [phion management centre] .....	414

Create Proxy ARP [Firewall] ..... 137,  
 [Firewall] ..... 138,  
 [Firewall] ..... 146  
 Create Range [phion management centre] ..... 414  
 Create Repository [phion management centre] ..... 414  
 Create Server [phion management centre] ..... 414  
 Create Service [phion management centre] ..... 414  
 Create Task [phion management centre] ..... 403  
 Create Time Interval for Rule [Firewall] ..... 140  
 Created [phion management centre] ..... 420  
 CRL Poll Time [VPN] ..... 207  
 criDistributionPoints [phion management centre] ..... 461  
 Cryptographic Service Provider [Getting Started] ..... 23  
 Cumulative Interval [Firewall] ..... 129  
 Cumulative Maximum [Firewall] ..... 129  
 Custom Template Logo [Anti-Virus] ..... 371  
 Cut Whitelists [Mail Gateway] ..... 253  
 Cycle [Firewall] ..... 136

**D**

Daily Report Mail to [Mail Gateway] ..... 254  
 Daily Schedule [Configuration Service] ..... 103  
 Data Limit (kB) [Firewall] ..... 131  
 Data Selection [Configuration Service] ..... 116  
 Data Selector [Configuration Service] ..... 116  
 Data Types for Service [phion management centre] ..... 440  
 Data Types for Subservice [phion management centre] .. 440  
 Dataport range [FTP Gateway] ..... 353  
 DDNS Domainname [DHCP] ..... 277  
 DDNS Hostname [DHCP] ..... 276  
 Deactivation Lag [Configuration Service] ..... 65  
 Dead Neighbor Poll Interval [OSPF and RIP] ..... 490  
 Dead Peer Detection Interval (s) [VPN] ..... 208  
 Debug Level [Proxy] ..... 325  
 Debug Log Level [Anti-Virus] ..... 369  
 Def Lease Time [DHCP] ..... 277  
 Default [Proxy] ..... 328,  
 [Proxy] ..... 331  
 Default HTTPS Certificate [Firewall] ..... 189  
 Default HTTPS Private Key [Firewall] ..... 189  
 Default Image Name [Configuration Service] ..... 102  
 Default Internal Mail Server [Mail Gateway] ..... 248  
 Default Internal MX [Mail Gateway] ..... 247  
 Default Key [VPN] ..... 207  
 Default Master DNS [Configuration Service] ..... 56  
 Default Metric [OSPF and RIP] ..... 486,  
 [OSPF and RIP] ..... 488  
 Default NIC [Getting Started] ..... 13  
 Default Policy [Firewall] ..... 155,  
 [Proxy] ..... 345  
 Default Poll Time (secs) [Firewall] ..... 194  
 Default Recipient DB [Mail Gateway] ..... 247  
 Default Recipients [Mail Gateway] ..... 247  
 Default Recipients Lookup [Mail Gateway] ..... 247,  
 [Mail Gateway] ..... 249  
 Default Route Distribution [OSPF and RIP] ..... 487  
 Default Route Redistribution [OSPF and RIP] ..... 488  
 Default Store [Getting Started] ..... 23  
 Default User specific [FTP Gateway] ..... 354  
 Define Browser Access [Proxy] ..... 330  
 Define Maximum Connections [Proxy] ..... 330  
 Define Request Method [Proxy] ..... 330  
 Define Transfer Protocol [Proxy] ..... 330  
 Delay [VPN] ..... 226  
 Delete [phion management centre] ..... 399  
 Delete Box Logfiles [phion management centre] ..... 414  
 Delete Box Statistics [phion management centre] ..... 414  
 Delete Data after (Days) [Statistics] ..... 301  
 Delete Data after (days) [phion management centre] .... 439  
 Delete Events [phion management centre] ..... 414  
 Delete Group [phion management centre] ..... 465  
 Delete Infected Mails [Mail Gateway] ..... 250  
 Delete Service Logfiles [phion management centre] ..... 414  
 Delete Stripped Attachments [phion management centre] 415  
 Delete Task [phion management centre] ..... 402  
 Delete Tunnel [phion management centre] ..... 466,  
 [phion management centre] ..... 468  
 Delete VPN Service from Group [phion management centre] 466  
 Delete VPN Service from GTI Editor [phion management centre] 465  
 Delete Wild Route [phion management centre] ..... 414  
 Delivered Entries [Mail Gateway] ..... 256

Delivery IPs [Mail Gateway] ..... 248  
 Delivery Policy [Mail Gateway] ..... 248  
 Demo Mode [phion management centre] ..... 472  
 Demo or Export Mode [Getting Started] ..... 11  
 Denied Classes [DHCP] ..... 274  
 Denied source-networks [FTP Gateway] ..... 354  
 Denied URLs per IP [Proxy] ..... 347  
 Denied URLs per User [Proxy] ..... 347  
 Deny [Firewall] ..... 136,  
 [Firewall] ..... 137,  
 [Firewall] ..... 138,  
 [Firewall] ..... 139,  
 [Firewall] ..... 162  
 Deny active ftp-data transfer [FTP Gateway] ..... 353  
 Deny additional ftp- commands [FTP Gateway] ..... 353  
 Deny delete dir [FTP Gateway] ..... 354  
 Deny Expired Certificates [Proxy] ..... 338  
 Deny file-delete [FTP Gateway] ..... 354  
 Deny file-download [FTP Gateway] ..... 353,  
 [FTP Gateway] ..... 354  
 Deny file-extensions [FTP Gateway] ..... 354  
 Deny file-rename [FTP Gateway] ..... 354  
 Deny file-upload [FTP Gateway] ..... 353,  
 [FTP Gateway] ..... 354  
 Deny make dir [FTP Gateway] ..... 354  
 Deny on Mismatch [Firewall] ..... 154  
 Deny Page [Proxy] ..... 346  
 Deny passive ftp data-transfer [FTP Gateway] ..... 353  
 Deny structure mount [FTP Gateway] ..... 354  
 Deny Threshold [Mail Gateway] ..... 259  
 Deny URL [Proxy] ..... 346  
 Description [Configuration Service] ..... 97,  
 [Configuration Service] ..... 118  
 Dest. [Firewall] ..... 173  
 Destination [Firewall] ..... 154,  
 [Eventing] ..... 309,  
 [FTP Gateway] ..... 353,  
 [FTP Gateway] ..... 354  
 Destination Address [Firewall] ..... 178  
 Destination IP [phion management centre] ..... 451  
 Destination IP Config [Proxy] ..... 330  
 Destination Port [Firewall] ..... 178,  
 [phion management centre] ..... 451  
 Destination SSL Certificate [phion management centre] . 451  
 Destination SSL IP [phion management centre] ..... 451  
 Destination SSL Port [phion management centre] ..... 451  
 Destination-specific SSL-Settings [Firewall] ..... 189  
 Detect All Available Protocols [Firewall] ..... 126  
 Detect Dialers [Anti-Virus] ..... 369  
 Detect Games [Anti-Virus] ..... 369  
 Detect Jokes [Anti-Virus] ..... 369  
 Detect PMS [Anti-Virus] ..... 369  
 Detection Regex [Anti-Virus] ..... 370  
 Device [Getting Started] ..... 10,  
 [Configuration Service] ..... 88,  
 [Firewall] ..... 184  
 Device Addresses Reside [Firewall] ..... 141  
 Device Autodetection [DHCP] ..... 273  
 Device Index [VPN] ..... 207,  
 [VPN] ..... 227  
 Device IP Address [Firewall] ..... 184  
 Device Name [Configuration Service] ..... 85  
 Device Realm [Configuration Service] ..... 79  
 Devices [Configuration Service] ..... 88,  
 [OSPF and RIP] ..... 488  
 devmtu [Configuration Service] ..... 73  
 DHCP Client Identifier [DHCP] ..... 275  
 DHCP Connect Timeout [Configuration Service] ..... 73  
 DHCP Enabled [Configuration Service] ..... 73  
 DHCP Interface [Configuration Service] ..... 73  
 DHCP Packet Size [DHCP] ..... 286  
 DHCP Server Identifier [DHCP] ..... 273  
 DHCP Server IPs [DHCP] ..... 286  
 DHCP Server Permissions [phion management centre] .. 414  
 DH-Group [VPN] ..... 215,  
 [VPN] ..... 227,  
 [phion management centre] ..... 468  
 Dial Allowed From [Configuration Service] ..... 75  
 Dial Allowed Until [Configuration Service] ..... 75  
 Dial Mode [Configuration Service] ..... 75  
 Dial Out Prefix [Configuration Service] ..... 74  
 Digest Authentication Key [OSPF and RIP] ..... 487,  
 [OSPF and RIP] ..... 489



Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Direction [Firewall].....	152,	Drop Mails over Attachment Limit [Mail Gateway] .....	255
[VPN] .....	221,	Dropped Packets [Firewall] .....	130
[VPN] .....	227	DSA Host Key [SSH Gateway] .....	365
Directory Pattern [Statistics].....	300,	DSN for Max Data Size Excess [Mail Gateway].....	255
[phion management centre] .....	439,	DSN for Max Recipients Excess [Mail Gateway].....	255
[phion management centre] .....	440	DSN Mails in MIME-Format [Mail Gateway].....	250
Disable [Firewall] .....	159	Dst Statistics [Configuration Service] .....	97
Disable & Terminate [Firewall].....	159	Dst Time-Statistics [Configuration Service].....	97
Disable Assembler Ciphers [Firewall].....	128	Duplicates Policy [DHCP] .....	276
Disable Box [Configuration Service].....	53	Duration of Validity [phion management centre] .....	460
Disable Device Check [Firewall].....	150	Dyn. Service [Firewall] .....	144
Disable Events System Tray [Getting Started].....	22	Dyn. Service Name Entries [Firewall].....	127
Disable FTP [Proxy] .....	325	Dynamic Address Assignment [Configuration Service] ...	75
Disable Interface Check [Firewall].....	150	Dynamic BOOTP Lease Time [DHCP].....	277
Disable Nagle Algorithm (No Delayed ACK) [Firewall] ...	154	Dynamic DNS Params [Configuration Service] .....	72,
Disable Quarantine Group [Firewall].....	184	[Configuration Service] .....	73,
Disable Service [Configuration Service] .....	97	[Configuration Service] .....	75,
Disable Session Passwords [Configuration Service] .....	118	[Configuration Service] .....	77
Disable Smartcard / Token [Getting Started].....	23	Dynamic Rule Control [phion management centre] .....	415
Disable Summary [OSPF and RIP].....	487	Dynamic Rule Selector [VPN] .....	233
Disable Update [Anti-Virus] .....	368,	Dyndns Name [Configuration Service].....	72,
[phion management centre] .....	416	[Configuration Service] .....	73,
Disable Updates [phion management centre].....	418	[Configuration Service] .....	75,
Disable/Enable VPN Tunnels [phion management centre]	415	[Configuration Service] .....	77
Disabled [Configuration Service].....	91,	<b>E</b>	
[VPN] .....	221,	Echo Limit Exceeded [Firewall].....	129
[phion management centre] .....	399	Echo/Src Limit Exceeded [Firewall] .....	129
Disc Write [Statistics] .....	300	Edit ... [phion management centre] .....	402,
Disk [Getting Started] .....	12	[phion management centre] .....	403
DLP [Proxy].....	335	Edit Certificate... [VPN].....	214
DLP Exception URLs [Proxy] .....	335	Edit Group [phion management centre] .....	465
DNS [VPN].....	214,	Edit Tunnel [phion management centre].....	466,
[VPN] .....	217	[phion management centre] .....	468
DNS Config [DNS].....	317	EMail Address [Configuration Service] .....	59
DNS Lifetime (Sec) [Firewall].....	142	Email Address [phion management centre].....	416,
DNS Master IP [Configuration Service] .....	56	[phion management centre] .....	418,
DNS Query [Mail Gateway].....	250	[phion management centre] .....	461
DNS Query ACL [Configuration Service].....	56	ENA [VPN].....	213,
DNS Query Rotation [Configuration Service] .....	55	[VPN] .....	216
DNS Query Timeout [Configuration Service] .....	55	Enable [Firewall].....	159
DNS Resolved IP [Configuration Service] .....	114	Enable Attachment Stripping [Mail Gateway].....	253
DNS Reverse Lookup [SSH Gateway].....	365	Enable Autonegotiation [Configuration Service].....	64
DNS Search Domains [Configuration Service] .....	55	Enable Blacklist [Mail Gateway].....	254
DNS Server [DHCP] .....	283	Enable Certificate Verification [Proxy] .....	338
DNS Server IP [Configuration Service].....	55,	Enable Cloning and Archiving [Mail Gateway] .....	251
[DHCP] .....	278	Enable Commands [phion management centre] .....	414,
DNS Servers [DHCP] .....	276	[phion management centre] .....	415
DNS Slave Zones [Configuration Service].....	56	Enable Compression [Getting Started] .....	22
DNS Update Scheme [DHCP] .....	278	Enable Configuration [OSPF and RIP] .....	487
DNS Zone [DHCP].....	274	Enable Domain Check [Mail Gateway] .....	259
DNS Zones [DHCP].....	278	Enable FW Compression [Firewall].....	128
Do Fwd Updates [DHCP] .....	277	Enable Grey Listing [Mail Gateway] .....	254
Do not eject CD-ROM after installation [Getting Started].	14	Enable H.323 Gatekeeper [Voice over IP].....	359
Domain [Configuration Service] .....	59,	Enable HA Sync [Mail Gateway] .....	260,
[VPN] .....	214,	[DHCP] .....	283
[VPN] .....	216,	Enable Inbound Shaping [Configuration Service] .....	88
[Anti-Virus] .....	369	Enable L2TP [VPN] .....	210
Domain Action [Mail Gateway].....	259	Enable Monitoring on Secondary [Configuration Service].	95
Domain Config [Proxy] .....	330	Enable Peer-To-Peer Detection [Firewall].....	126
Domain Controller [Configuration Service].....	113,	Enable Poisoned Reverse [OSPF and RIP].....	489
[Proxy] .....	328	Enable Post Settings [Mail Gateway] .....	251
Domain Controller IP [Configuration Service] .....	112,	Enable PPP Multilink [Configuration Service].....	71
[Configuration Service].....	114	Enable Pre Settings [Mail Gateway] .....	251
Domain Controller Name [Configuration Service].....	112,	Enable Progress Popup [Anti-Virus].....	370
[Configuration Service].....	114	Enable Proxy [Proxy].....	344
Domain Manipulation [Mail Gateway].....	251	Enable Redirector [Proxy] .....	344
Domain Name [Configuration Service].....	114,	Enable Revocation Check [Proxy].....	338
[DHCP] .....	276,	Enable SCEP [Configuration Service].....	58
[DHCP] .....	283	Enable serial console [Getting Started].....	14
Domain Realm [Configuration Service] .....	112	Enable SNMP [Proxy] .....	327
Domain Restrictions [Proxy] .....	326	Enable Spam Analysis [Mail Gateway] .....	259
Domain Suffix [Getting Started] .....	11	Enable Split Horizon [OSPF and RIP].....	489
Domain Whitelist [Mail Gateway].....	259	Enable SSL Description [Proxy].....	338
DomainController [phion management centre].....	461	Enable SSL-VPN [VPN].....	231
Domains [Mail Gateway] .....	248,	Enable Traffic Shaping [Configuration Service].....	88
[Proxy].....	330,	Enable Training [Mail Gateway].....	261
[Anti-Virus] .....	370	Enable Trickle Feature [Anti-Virus] .....	370
Download CRLs at Hour (0.23) [Proxy] .....	338	Enable Tunnel [Configuration Service] .....	67
Driver Module Name [Configuration Service].....	63	Enable Virus Detection [Anti-Virus] .....	371
Driver Options [Configuration Service] .....	63	Enable Virus Scanner [Anti-Virus] .....	370
Driver Type [Configuration Service].....	63	Encapsulation Mode [Configuration Service].....	74,
Drop Event [Eventing].....	307	[Configuration Service] .....	79
Drop event [Eventing].....	308		
Drop Fragmented Mails [Mail Gateway].....	255		



Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Encryption [VPN] ..... 215,  
 [VPN] ..... 221,  
 [VPN] ..... 227,  
 [phion management centre] ..... 467,  
 [phion management centre] ..... 468  
 Encryption Level [Configuration Service] ..... 52,  
 [Configuration Service] ..... 95  
 End Date [phion management centre] ..... 476  
 Ending Offset [Firewall] ..... 152  
 Endpoint Descriptor [Configuration Service] ..... 71  
 Enforced Metric [OSPF and RIP] ..... 488  
 Enter in Registry [Getting Started] ..... 14  
 Enterprise [Eventing] ..... 309  
 Enterprise ID [SNMP] ..... 481  
 Envelope Band Value [VPN] ..... 226,  
 [VPN] ..... 228  
 Envelope TOS Value [VPN] ..... 226,  
 [VPN] ..... 228  
 Error mailbox (MB) [DNS] ..... 321  
 Established [Firewall] ..... 169  
 Estimated Bandwidth [VPN] ..... 225  
 Ethernet MTU [Configuration Service] ..... 63  
 Ethernet Trunks [Configuration Service] ..... 65  
 Event ID [Eventing] ..... 307  
 Event must be confirmed [Eventing] ..... 308  
 Event on NTPd [Configuration Service] ..... 57  
 Event on SSH [Configuration Service] ..... 106  
 Event Permissions [phion management centre] ..... 414  
 Event Settings [Mail Gateway] ..... 256  
 Eventing [Firewall] ..... 155  
 Exception Regex [Anti-Virus] ..... 370  
 Exchange Timeout (s) [VPN] ..... 208  
 Exclude Networks [Firewall] ..... 151  
 Excluded Domains [Anti-Virus] ..... 370  
 Excluded Sources [Anti-Virus] ..... 370  
 Exclusive Parent [Proxy] ..... 326  
 Executable [Firewall] ..... 130  
 Execute [Firewall] ..... 137,  
 [Firewall] ..... 138,  
 [Firewall] ..... 139  
 Expire (TTL) [DNS] ..... 320,  
 [DNS] ..... 321  
 Expire after [DNS] ..... 319  
 Expiry Grace Period [Configuration Service] ..... 91  
 Explicit [Firewall] ..... 137,  
 [Firewall] ..... 146,  
 [Firewall] ..... 162  
 Explicit Bind IP [FTP Gateway] ..... 353  
 Explicit Bind IPs [Configuration Service] ..... 97  
 Explicit Box IP [Configuration Service] ..... 53  
 Explicit Groups [Configuration Service] ..... 115  
 Explicit IP [Firewall] ..... 146  
 Explicit MC IP [Configuration Service] ..... 53  
 Explicit Node Name [Configuration Service] ..... 117  
 Explicit X509 [VPN] ..... 209  
 Export ... [phion management centre] ..... 403  
 Export Issuer Cert... [VPN] ..... 214  
 Export RuleList... [Firewall] ..... 135  
 Export to Clipboard... [VPN] ..... 214  
 Export to File... [VPN] ..... 214  
 Expose Postmaster Alerts [Anti-Virus] ..... 372  
 Expose Sender Alerts [Anti-Virus] ..... 372  
 extendedKeyUsage [phion management centre] ..... 461  
 Extent Type [OSPF and RIP] ..... 491  
 External Authentication [Configuration Service] ..... 91,  
 [VPN] ..... 217,  
 [phion management centre] ..... 434  
 External Boxes [phion management centre] ..... 413  
 External DB Files [Configuration Service] ..... 115  
 External LDAP Server [phion management centre] ..... 459  
 External Listen Address [Mail Gateway] ..... 247  
 External Login Name [Configuration Service] ..... 91  
 External login name [phion management centre] ..... 434  
 External Relaying [phion management centre] ..... 448  
 External Root CA Certificate [Proxy] ..... 338  
 External Root CA Private Key [Proxy] ..... 338  
 External Scan Engine [Anti-Virus] ..... 371  
 External-Signed Certificate [VPN] ..... 231  
 External-Signed Private Key [VPN] ..... 231

**F**

Failed [phion management centre] ..... 399  
 Failed Local Sessions [Firewall] ..... 130

Failed Sessions Termination [Firewall] ..... 130  
 Failing [Firewall] ..... 169  
 Failure Retry Intervals (Minutes) [Configuration Service] ..... 59  
 Failure Standoff [Configuration Service] ..... 67,  
 [Configuration Service] ..... 78  
 Fallback [Firewall] ..... 136  
 Fallback Driver Options [Configuration Service] ..... 63  
 Fallback Enabled [Configuration Service] ..... 63  
 Fallback Module Name [Configuration Service] ..... 63  
 File [Getting Started] ..... 22  
 File Extension Filter [Mail Gateway] ..... 253  
 File Limit [Firewall] ..... 131  
 File Sync Frequency (lines) [phion management centre] ..... 449  
 File system [Getting Started] ..... 12  
 Filename [Proxy] ..... 331  
 Filename Length [FTP Gateway] ..... 353  
 Filled [phion management centre] ..... 468  
 Filter [Firewall] ..... 153,  
 [Statistics] ..... 297  
 Filter Box Affiliation [phion management centre] ..... 450  
 Find String [Proxy] ..... 345  
 Firewall Always ON [VPN] ..... 216  
 Firewall login [Proxy] ..... 344  
 Firewall Permissions [phion management centre] ..... 415  
 Firewall Rule Activation [VPN] ..... 233  
 First DNS [VPN] ..... 210  
 First WINS [VPN] ..... 210  
 First-IP (SI) [Configuration Service] ..... 95  
 Fit to Screen [phion management centre] ..... 466  
 Fixed IP Address [DHCP] ..... 275  
 Fixed Radius Password [Voice over IP] ..... 359  
 Fixed Radius User [Voice over IP] ..... 359  
 Flags [Getting Started] ..... 23  
 Flood Ping [Firewall] ..... 130  
 Follow Referrals [Configuration Service] ..... 112  
 Force Delete [phion management centre] ..... 399  
 Force Flash [Configuration Service] ..... 101  
 Force Full Update [phion management centre] ..... 466  
 Force Key Authentication [Configuration Service] ..... 107  
 Force MSS (Maximum Segment Size) [Firewall] ..... 154  
 Force Non Flash [Configuration Service] ..... 101  
 Force password change every [phion management centre] ..... 434  
 Force re-authentication [Firewall] ..... 188  
 foreign [Mail Gateway] ..... 248  
 Foreign IP Sufficient [Configuration Service] ..... 69  
 Format USB-Stick [Getting Started] ..... 14  
 Forward [Firewall] ..... 169,  
 [DNS] ..... 318  
 forward [DNS] ..... 317  
 Forward Band [Firewall] ..... 136  
 Forward Log Policy [Firewall] ..... 129  
 forward source-ip [DNS] ..... 318  
 Forward X11 Connection [SSH Gateway] ..... 365  
 Forward X11 connections [SSH Gateway] ..... 366  
 Forward Zone Name [DHCP] ..... 278  
 forwarders [DNS] ..... 317  
 Forwards [DNS] ..... 318  
 Free Format Text [DHCP] ..... 279,  
 [OSPF and RIP] ..... 491  
 FTP-command/protocol check [FTP Gateway] ..... 353  
 Full Address Manipulation [Mail Gateway] ..... 251  
 Full Name [Configuration Service] ..... 55,  
 [Configuration Service] ..... 91,  
 [phion management centre] ..... 416,  
 [phion management centre] ..... 418,  
 [phion management centre] ..... 433  
 Fully Meshed [phion management centre] ..... 468  
 Further Subnets [DHCP] ..... 274  
 Further Tries Transport Selection Policy [VPN] ..... 224

**G**

Garbage Collect Timer [OSPF and RIP] ..... 488  
 Gatekeeper Bind IP [Voice over IP] ..... 359  
 Gatekeeper Name [Voice over IP] ..... 359  
 Gatekeeper Password [Voice over IP] ..... 359  
 Gateway [Getting Started] ..... 10,  
 [Configuration Service] ..... 69,  
 [VPN] ..... 206  
 Gateway Hostname [Voice over IP] ..... 359  
 Gateway IP [Voice over IP] ..... 359,  
 [OSPF and RIP] ..... 490  
 Gateway to Modem IP [Configuration Service] ..... 72



Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

GC Busy Threshold [Configuration Service] .....	116,
[phion management centre] .....	448
GC Elasticity [Configuration Service] .....	100
GC Idle Threshold [Configuration Service] .....	116,
[phion management centre] .....	448
GC Interval [Configuration Service] .....	101
GC Min Interval [Configuration Service] .....	101
GC Threshold [Configuration Service] .....	101
GC Timeout [Configuration Service] .....	101
Generate Audit Info [Firewall] .....	130
Generate Events [Firewall] .....	129
Generate Statistics [Configuration Service] .....	97
Generic Application Tunneling [VPN] .....	233
Generic Forwarded Networks [Firewall] .....	129
Generic OID [VPN] .....	219
Generic Schedule [Configuration Service] .....	103
Generic squid.conf Entries [Proxy] .....	335
Geometry Quality [phion management centre] .....	471
Global Append Option [Configuration Service] .....	102
Global Position [Configuration Service] .....	53
Global Replay Window Size [VPN] .....	207
Global Reverse Device Policy [Firewall] .....	128
Global TCP Delay Policy [Firewall] .....	128
Global TOS Copy [VPN] .....	207
Go to Box [phion management centre] .....	466
Go to Config Tree [phion management centre] .....	466
Grace period after expiration [phion management centre] .....	434
Graphical API [phion management centre] .....	471
GRE with Assigned IP [Configuration Service] .....	73,
[Configuration Service] .....	74,
[Configuration Service] .....	76,
[Configuration Service] .....	78
Greeting Name [Mail Gateway] .....	247
Grey Listing Settings [Mail Gateway] .....	253
Grey Listing Time [Mail Gateway] .....	254
Group Attribute [Configuration Service] .....	113,
[Configuration Service] .....	114
Group Attribute Delimiter [Configuration Service] .....	114
Group Attribute Usage [Configuration Service] .....	114
Group Description [DHCP] .....	275
Group DHCP Options [DHCP] .....	275
Group Name [Configuration Service] .....	115
Group Parameters [DHCP] .....	275
Group Pattern [VPN] .....	219
Group Patterns [Firewall] .....	190
grow [Getting Started] .....	12
GTI Editor Defaults [phion management centre] .....	465
GUI Corresponding Text [DHCP] .....	279

**H**

H.323 Alias [Voice over IP] .....	359
H.323 Endpoints [Voice over IP] .....	359
H.323 Neighbors [Voice over IP] .....	359
HA Sync [SSH Gateway] .....	365
HA Sync Key [SSH Gateway] .....	365
HA Sync Mode [phion management centre] .....	436,
[phion management centre] .....	459
HA Sync Period [DHCP] .....	283
HA Sync Timeout [phion management centre] .....	413
HA Synchronisation [DHCP] .....	273
Halfside Close Timeout (s) [Firewall] .....	154
hard Network Device [DHCP] .....	273
Hash Meth. [VPN] .....	215,
[VPN] .....	227,
[phion management centre] .....	468
Header Reordering [Configuration Service] .....	66
Help Text (html) [VPN] .....	232
Heuristic Macro Detection [Anti-Virus] .....	369
Heuristic Others Detection [Anti-Virus] .....	369
Hide in netfence VPN World [phion management centre] .....	467
Hint [DNS] .....	318
Hint Zone [DNS] .....	317
History [phion management centre] .....	421
HMAC-MD5 Key [DHCP] .....	278
Host [VPN] .....	208,
[VPN] .....	209,
[DNS] .....	320,
[DNS] .....	321,
[Anti-Virus] .....	368
Host IP [Configuration Service] .....	55
Host Name [Configuration Service] .....	55,
[DHCP] .....	283
Hosting Interface [Configuration Service] .....	65

Hostname [Getting Started] .....	11,
[Configuration Service] .....	62,
[OSPF and RIP] .....	485
Hostname via Rev-DNS [DHCP] .....	277
HTML Templates [Anti-Virus] .....	369
HTTP Authentication [Configuration Service] .....	59
HTTP/1.1-Keep-Alive [Firewall] .....	188
HTTP/1.1-Keep-Alive timeout [Firewall] .....	188
Hub [phion management centre] .....	468
HW Accel. [VPN] .....	227
HW Acceleration [VPN] .....	221

**I**

I/O Tuning [Configuration Service] .....	101
ICP Port [Proxy] .....	325,
[Proxy] .....	326
ID [Configuration Service] .....	87
IDE-DMA Support [Configuration Service] .....	101
Identification Type [VPN] .....	228
Idle Hangup Time [Configuration Service] .....	75
Idle Mode [Configuration Service] .....	115,
[SSH Gateway] .....	365,
[phion management centre] .....	447,
[OSPF and RIP] .....	485
Idle Timeout [VPN] .....	211
IEN Name Server [DHCP] .....	276,
[DHCP] .....	284
Image [Getting Started] .....	15
Import ... [phion management centre] .....	403,
[phion management centre] .....	408
Import Key... [VPN] .....	214
Import License [phion management centre] .....	414
Import RuleList... [Firewall] .....	135
Impress Server [DHCP] .....	276,
[DHCP] .....	284
Inactive [Configuration Service] .....	54,
[Firewall] .....	156
inactive [Firewall] .....	136
Inactivity Grace Time [SSH Gateway] .....	366
Inbound [Firewall] .....	128,
[Firewall] .....	154,
[Firewall] .....	162
Inbound Bandwidth [Configuration Service] .....	88
Inbound Rate [Configuration Service] .....	86
Inbound SMS Handling [Configuration Service] .....	76
Inbound Threshold (%) [Firewall] .....	128
Inbound-User [Firewall] .....	162
Include Node Creation [phion management centre] .....	476
Include Server IPs [Configuration Service] .....	80
Include Subdomains [Mail Gateway] .....	247
Included subservice directories [phion management centre] .....	440
Info [phion management centre] .....	468
Initial directory [FTP Gateway] .....	353
Initiation Timeout [VPN] .....	211
Insert [Eventing] .....	312
Insert new Personal Network [VPN] .....	206
Install Utilities [Getting Started] .....	13
Instances [Statistics] .....	299
Area ID [OSPF and RIP] .....	487
Interface Realm [Configuration Service] .....	62
Interface [Firewall] .....	146,
[Firewall] .....	173
Interface Addresses [OSPF and RIP] .....	489
Interface Computation [Configuration Service] .....	64
Interface Default [OSPF and RIP] .....	488
Interface Description [OSPF and RIP] .....	489
Interface Groups [Firewall] .....	134
Interface Monitoring Policy [Configuration Service] .....	95
Interface Name [Configuration Service] .....	62,
[Configuration Service] .....	65,
[Configuration Service] .....	69,
[Configuration Service] .....	70,
[Firewall] .....	146,
[OSPF and RIP] .....	490
Interface Realm [Configuration Service] .....	69,
[Configuration Service] .....	73,
[Configuration Service] .....	74,
[Configuration Service] .....	76,
[Configuration Service] .....	78
Interface Usage [Configuration Service] .....	64
Interface/Tunnel Name [Configuration Service] .....	86
Interfaces [OSPF and RIP] .....	489
interfaces [SNMP] .....	481
internal [Mail Gateway] .....	248



Internal Interface Name [Configuration Service] ..... 63  
 Internal IP-Addresses [Mail Gateway] ..... 250  
 Internal Listen Address [Mail Gateway] ..... 247  
 Introduce Route on Device [Firewall] ..... 151  
 Introduce Routes [Firewall] ..... 141  
 Invalid ARPs [Firewall] ..... 130  
 Inventory [Configuration Service] ..... 103  
 INVITE Timeout [Voice over IP] ..... 360  
 Area ID [OSPF and RIP] ..... 487  
 IP [Getting Started] ..... 12  
 ip [SNMP] ..... 481  
 IP Address [Getting Started] ..... 10,  
     [Configuration Service] ..... 62,  
     [Firewall] ..... 184,  
     [Firewall] ..... 194,  
     [VPN] ..... 211,  
     [DHCP] ..... 283,  
     [DNS] ..... 320  
 IP address [DNS] ..... 321  
 IP Address or Device used for Tunnel Address [VPN] ..... 222  
 IP Address/Mask [SNMP] ..... 481  
 IP Addresses [VPN] ..... 207  
 IP Begin [DHCP] ..... 274  
 IP Blacklist [Mail Gateway] ..... 255  
 IP Configuration [Proxy] ..... 329,  
     [Proxy] ..... 330  
 IP Dyn Address [Configuration Service] ..... 100  
 IP End [DHCP] ..... 274  
 IP Monitoring Policy [Configuration Service] ..... 95  
 IP Netmask [Firewall] ..... 184  
 IP Prefix List [OSPF and RIP] ..... 488,  
     [OSPF and RIP] ..... 490  
 IP Ranges [Proxy] ..... 329,  
     [Proxy] ..... 330  
 IP Spoofing [Firewall] ..... 130  
 IP/Hostname [Proxy] ..... 326  
 IP/Mask [Proxy] ..... 327  
 IP-Begin [DHCP] ..... 283  
 IP-End [DHCP] ..... 283  
 IPs Allowed To Connect (ACL) [Mail Gateway] ..... 261  
 IPSec Client [VPN] ..... 219  
 IPSec Log Level [VPN] ..... 208  
 IPSec Personal [VPN] ..... 208  
 IPSec PSK [VPN] ..... 211  
 IPSec Site-to-Site [VPN] ..... 208  
 ISDN Card [Configuration Service] ..... 74  
 ISDN Enabled [Configuration Service] ..... 74  
 ISDN MSN [Configuration Service] ..... 74  
 ISDN on Standby [Configuration Service] ..... 74  
 ISDN Settings [Configuration Service] ..... 74  
 Issuer [Firewall] ..... 190,  
     [VPN] ..... 207,  
     [VPN] ..... 208  
 issuerAltName [phion management centre] ..... 461

**K**

Keep Log Structure [Configuration Service] ..... 104  
 Keep Mails In Mailbox [Mail Gateway] ..... 261  
 Keep Structural Info [phion management centre] ..... 451  
 Kernel Parameter [Getting Started] ..... 13  
 Key Algorithm [phion management centre] ..... 460  
 Key Encryption [phion management centre] ..... 460  
 Key Length [Getting Started] ..... 23  
 Key Regeneration Period [Configuration Service] ..... 107  
 Key Time Limit [VPN] ..... 214,  
     [VPN] ..... 216,  
     [VPN] ..... 221,  
     [phion management centre] ..... 467  
 Key Traffic Limit [VPN] ..... 214,  
     [VPN] ..... 216,  
     [VPN] ..... 222,  
     [phion management centre] ..... 467  
 Key/Key String [OSPF and RIP] ..... 487  
 Keyboard Layout [Getting Started] ..... 11  
 Keysize in Bits [phion management centre] ..... 460  
 keyUsage [phion management centre] ..... 461  
 Kill Handler Processes [phion management centre] ..... 415  
 Kill Sessions [phion management centre] ..... 414  
 Kill Worker Process [Mail Gateway] ..... 256  
 Kind of Application [VPN] ..... 232  
 Known Clients [DHCP] ..... 274,  
     [DHCP] ..... 275  
 Known Hosts [Configuration Service] ..... 55

**L**

LACPDU Packet Rate [Configuration Service] ..... 65  
 LAN Interfaces [Firewall] ..... 184  
 Language on Error Pages [Proxy] ..... 325  
 Large ICMP Packet [Firewall] ..... 130  
 Last ACK Timeout (s) [Firewall] ..... 154  
 Last Modified [phion management centre] ..... 420  
 Last Password Change [phion management centre] ..... 434  
 Layer [Eventing] ..... 312  
 LCP Check Interval [Configuration Service] ..... 78  
 LCP Echo Failure [VPN] ..... 211  
 LCP Echo Interval [VPN] ..... 211  
 LDAP Admin DN [Configuration Service] ..... 113  
 LDAP Admin Password [Configuration Service] ..... 113  
 LDAP Alternative Login Name Field [VPN] ..... 218  
 LDAP Authentication Selector Field [VPN] ..... 218  
 LDAP Base DN [Configuration Service] ..... 113  
 LDAP Group Information [VPN] ..... 218  
 LDAP IP Attribute [VPN] ..... 218  
 LDAP Password Field [Configuration Service] ..... 113  
 LDAP Server [Configuration Service] ..... 113  
 LDAP Server Port [Configuration Service] ..... 113  
 LDAP User Field [Configuration Service] ..... 113  
 LDAP VPN Group Attribute [VPN] ..... 218  
 Lease Limit [DHCP] ..... 278  
 Lease Time [DHCP] ..... 283  
 Leases Critical [DHCP] ..... 283  
 Leases Low [DHCP] ..... 283  
 Level1 Directories [Proxy] ..... 325  
 Level2 Directories [Proxy] ..... 325  
 License [VPN] ..... 213  
 License is disabled [VPN] ..... 213  
 License Type [VPN] ..... 214  
 Licenses [Getting Started] ..... 13,  
     [Configuration Service] ..... 93  
 Lifetime [VPN] ..... 227,  
     [phion management centre] ..... 468  
 LIFO linear [Getting Started] ..... 14  
 Limit Mail Data Size [Mail Gateway] ..... 255  
 Link Active [Configuration Service] ..... 71,  
     [Configuration Service] ..... 73  
 Link Check [Configuration Service] ..... 65  
 Link Check Mode [Configuration Service] ..... 65  
 Link Description [VPN] ..... 232,  
     [VPN] ..... 233  
 Link Properties [Configuration Service] ..... 71  
 List of Critical Ports [Firewall] ..... 138  
 Listen on [Mail Gateway] ..... 249  
 Listen on Devices [DHCP] ..... 273  
 Listen timeout [FTP Gateway] ..... 353  
 Listen to Port 443 [phion management centre] ..... 416  
 Listening Port [Mail Gateway] ..... 261,  
     [FTP Gateway] ..... 353  
 Load Interface Info [OSPF and RIP] ..... 489  
 Load Network Info [DHCP] ..... 273  
 Loader Delay [Configuration Service] ..... 102  
 Loader Password [Configuration Service] ..... 102  
 Local Address [Firewall] ..... 138,  
     [VPN] ..... 227  
 Local Clock Stratum [Configuration Service] ..... 57  
 Local Deliver IP [Mail Gateway] ..... 248  
 Local End IP [Configuration Service] ..... 79  
 Local In [Firewall] ..... 169  
 Local IP [Configuration Service] ..... 72  
 Local IP Selection [Configuration Service] ..... 71  
 Local Log Directory [phion management centre] ..... 449  
 Local Networks [VPN] ..... 227  
 Local Out [Firewall] ..... 169  
 Local Part Manipulation [Mail Gateway] ..... 251  
 Local Redirect [Firewall] ..... 137,  
     [Firewall] ..... 138,  
     [Firewall] ..... 139  
 Local Redirect Object [Firewall] ..... 137,  
     [Firewall] ..... 138,  
     [Firewall] ..... 139  
 Local Redirection / Local Routing Loop [Firewall] ..... 130  
 Local SSL Port [phion management centre] ..... 451  
 Local Subnets [DHCP] ..... 276,  
     [DHCP] ..... 284  
 Local Tunnel IP [VPN] ..... 211  
 Locality [phion management centre] ..... 461  
 Localnet [phion management centre] ..... 425

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Location [Configuration Service] .....	59,	MAC Address [DHCP] .....	275
[SNMP] .....	481	MAC Change Allowed [Firewall] .....	184
Log Add. Meta-directory Fields [Configuration Service]..	115	MAC Type [DHCP] .....	275
Log Allowed URLs [Proxy] .....	346	MAC-Address [DHCP] .....	283
Log append file [FTP Gateway] .....	353	Mail Data Size (MB) [Mail Gateway] .....	255
Log Categories per URL [Proxy] .....	344	Mail Data Size Limit [Mail Gateway] .....	256
Log Change Differences [phion management centre] ...	473	Mail Denied [Mail Gateway] .....	256
Log change to upper dir denies [FTP Gateway] .....	353	Mail Queue [Mail Gateway] .....	263
Log Connections [phion management centre] .....	459	Mail Router Permissions [phion management centre] ...	415
Log create dir denies [FTP Gateway] .....	353	Mail Server [Eventing] .....	311
Log create directory [FTP Gateway] .....	353	Mail Transfer Agents (MTAs) [Mail Gateway] .....	250
Log Creation Differences [phion management centre] ...	473	Mailbox (MB) [DNS] .....	321
Log Decisions [Anti-Virus] .....	370	Mailbox FORGET [Mail Gateway] .....	261
Log delete dir denies [FTP Gateway] .....	353	Mailbox HAM [Mail Gateway] .....	261
Log delete directory [FTP Gateway] .....	353	Mailbox SPAM [Mail Gateway] .....	261
Log delete file [FTP Gateway] .....	353	Mailserver (A) [DNS] .....	321
Log delete file-denies [FTP Gateway] .....	353	Mailserver (IMAP) [Mail Gateway] .....	261
Log denied ftp-commands [FTP Gateway] .....	353	Mailserver priority [DNS] .....	321
Log denied local logins [FTP Gateway] .....	353	Manage Admins [phion management centre] .....	414
Log Denied URLs [Proxy] .....	346	Manage Box File Update [phion management centre] ...	414
Log destination denies [FTP Gateway] .....	353	Manage Box REXEC [phion management centre] .....	414
Log Destinations [Configuration Service] .....	117,	Manage Box Software Updates [phion management centre] 414	
[phion management centre] .....	452	Manage Config. Updates [phion management centre] ...	414
Log DNS Queries [Configuration Service] .....	56	Manage HA Sync [phion management centre] .....	414
Log download file [FTP Gateway] .....	353	Management IP [Configuration Service] .....	62
Log extension denies [FTP Gateway] .....	353	Management IP (MIP) [Configuration Service] .....	62
Log File Entry [Firewall] .....	155	Management IP address / Subnet mask [Getting Started].	13
Log file-download denies [FTP Gateway] .....	353	Management Traffic [Configuration Service] .....	88
Log file-upload denies [FTP Gateway] .....	353	ManagementOnly [Configuration Service] .....	54
Log Filters [Configuration Service] .....	117,	Mandatory Client Credentials [VPN] .....	217
[phion management centre] .....	452	Manipulate Access Cache Entries [phion management centre] 415	
Log Groups [Configuration Service] .....	115,	Map [Firewall] .....	137,
[Configuration Service] .....	116	[Firewall] .....	138,
Log Keep Duration [phion management centre] .....	449	[Firewall] .....	139,
Log Level [Configuration Service] .....	78,	[Firewall] .....	146
[Firewall] .....	129,	Map to Network [Firewall] .....	146
[phion management centre] .....	459,	Mark as Read [phion management centre] .....	414
[OSPF and RIP] .....	485,	Master [DNS] .....	318
[OSPF and RIP] .....	486,	Master Device [Configuration Service] .....	65
[OSPF and RIP] .....	488	Masters [DNS] .....	318
Log Local Session Termination [Firewall] .....	130	Match Condition [OSPF and RIP] .....	490
Log logins [FTP Gateway] .....	353	Match Parameter [DHCP] .....	278
Log Message Filter [Configuration Service] .....	116	Max Acceptors [Firewall] .....	127
Log other file-actions [FTP Gateway] .....	353	Max Age of crashed Mails (d) [Mail Gateway] .....	255
Log other ftp-commands [FTP Gateway] .....	353	Max Echo (%) [Firewall] .....	127
Log Permissions [phion management centre] .....	414	Max Event Records [Eventing] .....	311
Log protocol denies [FTP Gateway] .....	353	Max files to cache [Firewall] .....	189
Log Removal Differences [phion management centre] ...	473	Max Illegal Inputs [SSH Gateway] .....	366
Log rename file [FTP Gateway] .....	353	Max Int TCP Conns [Configuration Service] .....	115
Log rename-file denies [FTP Gateway] .....	353	Max ISS Proventia Processes [Proxy] .....	344
Log Server [DHCP] .....	276,	Max Lease Time [DHCP] .....	277
[DHCP] .....	284	Max Load (1-15 mins) [Configuration Service] .....	111
Log Session State Change [Firewall] .....	155	Max Local-In Echo/Src [Firewall] .....	127
Log structure-mount denies [FTP Gateway] .....	353	Max Local-In Other/Src [Firewall] .....	128
Log succeeded local logins [FTP Gateway] .....	353	Max Local-In Session/Src [Firewall] .....	127
Log Synced Sessions [Firewall] .....	128	Max Local-In UDP/Src [Firewall] .....	127
Log to Disk [Configuration Service] .....	119	Max Memory Used [Configuration Service] .....	111
Log upload file [FTP Gateway] .....	353	Max MTU/MRU Size [Configuration Service] .....	72
Log via Syslog [Proxy] .....	325	Max Other (%) [Firewall] .....	127
Logfile Name Patterns [Configuration Service] .....	104	Max Pending Local Accepts/Src [Firewall] .....	128
Loghost IP Address [Configuration Service] .....	117	Max Ping Size [Firewall] .....	144
Loghost Port [Configuration Service] .....	117	Max Queued Message [Configuration Service] .....	115
Login Event [Configuration Service] .....	91,	Max Routing Cache Entries [Configuration Service] .....	100
[phion management centre] .....	435	Max size of a file to cache (kb) [Firewall] .....	189
Login Grace Time [SSH Gateway] .....	365	Max Storage Time [Configuration Service] .....	104
Login Greeting Text [VPN] .....	232,	Max TCP Connections [phion management centre] .....	448
[SSH Gateway] .....	365	Max UDP (%) [Firewall] .....	127
Login Name [Configuration Service] .....	115,	Max. Access Entries [Firewall] .....	127
[Firewall] .....	190,	Max. Archive Ratio [Anti-Virus] .....	369
[phion management centre] .....	433	Max. Archive Size (MB) [Anti-Virus] .....	369
Login Timeout [Configuration Service] .....	107	Max. ARP Entries [Firewall] .....	127
Login+Password Authentication [Firewall] .....	190	Max. Attachments [Mail Gateway] .....	255
Logo [VPN] .....	232	Max. Bandwidth [Configuration Service] .....	88
Logtick [Configuration Service] .....	111	Max. Block Entries [Firewall] .....	127
Loopback [Firewall] .....	169	Max. DNS Entries [Firewall] .....	127
Loopback SSL Port [phion management centre] .....	451	Max. Drop Entries [Firewall] .....	127
Low Priority Lower Limit [VPN] .....	225	Max. Dynamic Rules [Firewall] .....	127
Low Priority Upper Limit [VPN] .....	225	Max. Exec Processes [phion management centre] .....	413
LPR Server [DHCP] .....	276,	Max. Fail Entries [Firewall] .....	127
[DHCP] .....	284	Max. file RAM usage (MB) [Anti-Virus] .....	368
<b>M</b>		Max. Forwarding Echo/Src [Firewall] .....	131
Mac [Firewall] .....	154	Max. Forwarding Other/Src [Firewall] .....	131

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Max. Forwarding Session/Src [Firewall] ..... 131  
 Max. Forwarding UDP/Src [Firewall] ..... 131  
 Max. Hops for Referrals [Configuration Service]..... 112  
 Max. Lifetime [VPN]..... 227,  
     [phion management centre] ..... 468  
 Max. Multiple Redirect IPs [Firewall] ..... 127  
 Max. nesting [Anti-Virus] ..... 369  
 Max. Num. Workers [Anti-Virus] ..... 368  
 Max. Number of Sessions [Firewall] ..... 155  
 Max. Number of Sessions per Source [Firewall]. .... 155  
 Max. Pending Forward Accepts/Src [Firewall] ..... 131  
 Max. Pending Inbounds [Firewall]..... 127  
 Max. phase 1 Lifetime (s) [VPN]..... 211  
 Max. Plugins [Firewall] ..... 127  
 Max. Segment Size [Configuration Service] ..... 72  
 Max. Session Slots [Firewall] ..... 127  
 Max. SIP Calls [Firewall] ..... 127,  
     [Voice over IP] ..... 360  
 Max. SIP Media [Firewall] ..... 127,  
     [Voice over IP] ..... 360  
 Max. SIP Transaction [Voice over IP]..... 360  
 Max. SIP Transactions [Firewall]..... 127  
 Max. Size (MB) [Mail Gateway] ..... 259  
 Max. SMTP Line Length [Mail Gateway]..... 255  
 Max. Status Age [Configuration Service] ..... 115  
 Max. Tunnels [VPN]..... 231  
 Max. Update Processes [phion management centre] ..... 413  
 Max. Validity Discrepancy [Configuration Service] ..... 115  
 Maximal allowed workers [FTP Gateway] ..... 353  
 Maximum [VPN]..... 215  
 Maximum Bytes [Firewall] ..... 178  
 Maximum Children [Mail Gateway] ..... 249,  
     [Mail Gateway] ..... 260  
 Maximum Connections Config [Proxy]..... 330  
 Maximum Counts [Firewall] ..... 178  
 Maximum Number of Recipients [Mail Gateway] ..... 255  
 Maximum Number shown [Statistics]..... 299  
 Maximum Receive Unit [VPN] ..... 210  
 Maximum Transmission Unit [VPN] ..... 210  
 MC Activates Network Changes [Configuration Service].. 53  
 MC Certificate [phion management centre] ..... 412  
 MC Config Permissions [phion management centre] ..... 414  
 MC Control Permissions [phion management centre] ..... 414  
 MC Identifier [phion management centre] ..... 412  
 MC IP Address [phion management centre]..... 412  
 MC License [phion management centre]..... 412  
 MC Policy Service Permissions [phion management centre] 415  
 MC Private Key [phion management centre] ..... 413  
 MC SSH Key [phion management centre]..... 413  
 MC SSL Certificate [phion management centre] ..... 412  
 MC->Box Access [Configuration Service]..... 53  
 Meshed [phion management centre] ..... 467  
 Message [VPN]..... 214,  
     [VPN] ..... 216  
 Message Digest Algorithm [phion management centre] .. 460  
 Message Digest Key ID [OSPF and RIP]..... 489  
 Message for Deny [Proxy] ..... 346  
 Message Queue Size [phion management centre] ..... 448  
 Message to Recipient [Mail Gateway] ..... 253  
 Method [Configuration Service] ..... 112,  
     [Configuration Service] ..... 113,  
     [Configuration Service] ..... 114,  
     [Configuration Service] ..... 115,  
     [Firewall] ..... 154  
 Metric Offsets [OSPF and RIP] ..... 488  
 Mgmt Baud Rate [Configuration Service] ..... 54  
 Mgmt COM Port [Configuration Service]..... 54  
 Migrate Cluster [phion management centre] ..... 422  
 Migrate Clusters [phion management centre] ..... 422  
 Migrate Complete Tree [phion management centre] ..... 422  
 Migrate Node [phion management centre]..... 423  
 Migrate Range [phion management centre]..... 422  
 Migrate Ranges [phion management centre] ..... 422  
 MIME-Type [Mail Gateway]..... 253  
 MIME-Type Exceptions [Mail Gateway] ..... 253  
 Mime-Types [Anti-Virus]..... 370  
 Min Delay [Firewall]..... 144  
 Min Lease Time [DHCP] ..... 277  
 Min. Lifetime [VPN]..... 227,  
     [phion management centre] ..... 468  
 Min. phase 1 Lifetime (s) [VPN] ..... 211  
 Minimum [VPN] ..... 215  
 Minimum TTL [DNS] ..... 319

Misc Settings [Mail Gateway] ..... 255  
 Modem Device [Configuration Service]..... 72,  
     [Configuration Service] ..... 76  
 Modem IP [Configuration Service] ..... 71  
 Modify Connections [phion management centre]..... 415  
 Modify Event [phion management centre]..... 420  
 Module parameters [Getting Started] ..... 13  
 Monitor Devs I / II [Configuration Service]..... 96  
 Monitor IPs I [Configuration Service] ..... 95  
 Monitor IPs I/ II [Configuration Service] ..... 95  
 Monitoring Method [Configuration Service]..... 78  
 Monthly Schedule [Configuration Service]..... 103  
 MPPE Encryption Strength [VPN] ..... 211  
 MTA Retry Sequence [Mail Gateway] ..... 250  
 MTAs for Urgent Mail [Mail Gateway] ..... 250  
 MTU [Configuration Service]..... 62,  
     [Configuration Service] ..... 64,  
     [Configuration Service] ..... 66,  
     [Configuration Service] ..... 69,  
     [VPN] ..... 207  
 Multicast Addresses [VPN] ..... 207  
 Multipath Gateway [Configuration Service] ..... 69  
 Multipath Handling [OSPF and RIP] ..... 486,  
     [OSPF and RIP] ..... 488  
 Must Be Healthy [VPN]..... 232,  
     [VPN] ..... 233  
 MX Record [Configuration Service] ..... 72,  
     [Configuration Service] ..... 74,  
     [Configuration Service] ..... 75,  
     [Configuration Service] ..... 77  
 My Domains List [Mail Gateway]..... 247  
 My IP Explicit [VPN] ..... 210  
 My IP Type [VPN]..... 210  
 My Peer IP Explicit [VPN]..... 210  
 My Peer Type [VPN] ..... 210

**N**

Name [Configuration Service]..... 65,  
     [Configuration Service] ..... 71,  
     [Configuration Service] ..... 73,  
     [Configuration Service] ..... 87,  
     [Firewall] ..... 145,  
     [Firewall] ..... 194,  
     [VPN] ..... 206,  
     [VPN] ..... 208,  
     [VPN] ..... 214,  
     [VPN] ..... 216,  
     [VPN] ..... 217,  
     [VPN] ..... 221,  
     [VPN] ..... 227,  
     [VPN] ..... 232,  
     [Proxy]..... 326,  
     [phion management centre] ..... 414,  
     [phion management centre] ..... 420,  
     [phion management centre] ..... 450,  
     [phion management centre] ..... 451,  
     [phion management centre] ..... 452,  
     [phion management centre] ..... 467  
 Name of NIC [Configuration Service]..... 64  
 Nameserver [Getting Started] ..... 10  
 NAS IP Address [Configuration Service]..... 114  
 NAS IP Port [Configuration Service] ..... 114  
 NAS-ID [Configuration Service] ..... 114  
 NBDD Server [DHCP] ..... 276,  
     [DHCP]..... 283  
 Neighbor IP [OSPF and RIP] ..... 489  
 Neighbor Priority [OSPF and RIP] ..... 490  
 Neighbor Timeout [Voice over IP] ..... 359  
 Neighbour Settings [Proxy]..... 325  
 Neighbour Type [Proxy]..... 326  
 Net Join Status [Configuration Service]..... 113  
 Netbios Domain Name [Configuration Service]..... 112  
 Netbios Node Type [DHCP] ..... 276,  
     [DHCP]..... 284  
 Netbios Scope Id [DHCP] ..... 276,  
     [DHCP]..... 284  
 netfence base system [Getting Started]..... 13  
 Netmask [Firewall] ..... 146,  
     [DHCP]..... 274,  
     [DHCP]..... 275  
 Network [VPN]..... 213  
 Network ACL [SSH Gateway] ..... 366  
 Network Address [Firewall] ..... 151,  
     [VPN] ..... 206,  
     [DHCP]..... 274

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Network Device [OSPF and RIP] .....	487
Network Interface Cards [Configuration Service] .....	63
Network Mask [VPN] .....	206
Network Prefix [OSPF and RIP] .....	486,
[OSPF and RIP] .....	487,
[OSPF and RIP] .....	490
Network Routes [VPN] .....	215,
[VPN] .....	217
Network Type [OSPF and RIP] .....	489
Networks [Firewall] .....	134,
[OSPF and RIP] .....	487
New ... [phion management centre] .....	402,
[phion management centre] .....	403
New Domain Name [DNS] .....	321
New Others [DNS] .....	322
New Prefix [Voice over IP] .....	359
New Root Passwd [Configuration Service] .....	54
New Service Password [Configuration Service] .....	54
Next Forced Change [Configuration Service] .....	91
NIC Type [Configuration Service] .....	63,
[Configuration Service] .....	64
NIS Domain Name [DHCP] .....	276,
[DHCP] .....	283
NIS Server [DHCP] .....	276,
[DHCP] .....	283
No ACPI [Getting Started] .....	14,
[Configuration Service] .....	102
No Difference Details [phion management centre] .....	476
No graphic adapter available [Getting Started] .....	14
NO ICMP AT ALL [Firewall] .....	159
No Inline Authentication [Firewall] .....	190
No local authorization needed [FTP Gateway] .....	354
No Popups If Less Than (sec) [Anti-Virus] .....	370
No Probing for Interfaces [Configuration Service] .....	118
No Rule Update Time Range [Firewall] .....	129
No Scan For (Recipients) [Anti-Virus] .....	372
No Scan For (Sender) [Anti-Virus] .....	372
No. of ICMP Probes [Configuration Service] .....	67,
[Configuration Service] .....	78
No. of LCP Checks [Configuration Service] .....	78
no-monitoring [Configuration Service] .....	95
None [Firewall] .....	159
Notification ID [Eventing] .....	307,
[Eventing] .....	308
notify [DNS] .....	317,
[DNS] .....	319
Notify Again After (min) [Proxy] .....	338
Notify User [Proxy] .....	338
Nr. [VPN] .....	213
nsComment [phion management centre] .....	461
NSSA-ABR Translate Election [OSPF and RIP] .....	487
NTP Server [DHCP] .....	276,
[DHCP] .....	283
NTP sync on Startup [Configuration Service] .....	56
Number of HA retries [phion management centre] .....	436
Number of Interfaces [Configuration Service] .....	63
Number of Processes [Configuration Service] .....	112,
[Configuration Service] .....	113,
[Configuration Service] .....	114,
[Configuration Service] .....	115
Number of Queued Mails [Mail Gateway] .....	256
Number of Redirectors [Proxy] .....	344

**O**

Object Name [phion management centre] .....	402
Object Type [OSPF and RIP] .....	488
Offline Rules [VPN] .....	214,
[VPN] .....	216
Offline sync (every n min./hour) [Configuration Service] .....	112
On Demand Transport Delay [VPN] .....	226
On Demand Transport Timeout [VPN] .....	226
one-AND-one-present [Configuration Service] .....	95
Open Files [Configuration Service] .....	101
Operation Mode [Configuration Service] .....	65,
[Configuration Service] .....	85,
[Configuration Service] .....	86,
[OSPF and RIP] .....	485
Optimised Updates [DHCP] .....	277
Option Section [DHCP] .....	283
Option150 [DHCP] .....	277
Optional Bind IP [Firewall] .....	194
Options [Proxy] .....	326

Organisation [phion management centre] .....	412,
[phion management centre] .....	461
Organisation Unit [phion management centre] .....	461
Organization [Configuration Service] .....	59
Origin [Firewall] .....	190
Origin Domain Name [DNS] .....	318
Original Prefix [Voice over IP] .....	359
Originate Always [OSPF and RIP] .....	487
Originator Systems [phion management centre] .....	450
OS Platform [Configuration Service] .....	52
OSPF Dead Interval [OSPF and RIP] .....	489
OSPF External Metric [OSPF and RIP] .....	487
OSPF Hello Interval [OSPF and RIP] .....	489
OSPF Metric [OSPF and RIP] .....	487
OSPF Priority [OSPF and RIP] .....	489
OSPF Retransmit Interval [OSPF and RIP] .....	489
OSPF Text [OSPF and RIP] .....	491
OSPF Transmit Delay [OSPF and RIP] .....	489
Other Limit Exceeded [Firewall] .....	130
Other root [VPN] .....	209
Other/Src Limit Exceeded [Firewall] .....	130
Out Interface Name [OSPF and RIP] .....	490
Outbound [Firewall] .....	128,
[Firewall] .....	154,
[Firewall] .....	162
Outbound Bandwidth [Configuration Service] .....	88
Outbound Rate [Configuration Service] .....	86
Outbound-User [Firewall] .....	162
Override Node Name [Configuration Service] .....	117
Override SyncIP-Primary [phion management centre] .....	449
Override SyncIP-Secondary [phion management centre] .....	449
Oversized SYN Packet [Firewall] .....	130
OWA URL [VPN] .....	232
Own Cook Settings [phion management centre] .....	417
Own Event Settings [phion management centre] .....	417,
[phion management centre] .....	418
Own Firewall Objects [phion management centre] .....	417,
[phion management centre] .....	418
Own IP [Control Centre] .....	39
Own Log File [Firewall] .....	155
Own Policy Server Objects [phion management centre] ..	417,
[phion management centre] .....	418
Own Routing Table [Configuration Service] .....	72,
[Configuration Service] .....	74,
[Configuration Service] .....	76,
[Configuration Service] .....	77
Own Shaping Trees [phion management centre] .....	417,
[phion management centre] .....	418
Own VPN GTI Editor [phion management centre] .....	417,
[phion management centre] .....	418

**P**

Packet Forwarding [Firewall] .....	154
Packet Hop Count [DHCP] .....	286
Packet Load Balancing [Configuration Service] .....	69
Parallel Connection Limit [Mail Gateway] .....	256
Parallel connections for collection [phion management centre]	
436	
Parallel Inbound Conn. per Peer [Mail Gateway] .....	255
Parallel Inbound Connections [Mail Gateway] .....	255
Parallel Outbound Conn. per Peer [Mail Gateway] .....	255
Parallel Outbound Connections [Mail Gateway] .....	255
Parameter Length [FTP Gateway] .....	353
Parameter Resolution [phion management centre] .....	440
Parameter Template [OSPF and RIP] .....	489
Parameter Template for Address [OSPF and RIP] .....	489
Parameters... [VPN] .....	213
Parent Network [Firewall] .....	141
Partner Networks [VPN] .....	222
Pass [Firewall] .....	136,
[Firewall] .....	137,
[Firewall] .....	138,
[Firewall] .....	139,
[Firewall] .....	162
Passive Interface [OSPF and RIP] .....	489
Passive Sync (DOWN) [Firewall] .....	172
Passive Sync (UP) [Firewall] .....	172
Password [Getting Started] .....	13,
[Configuration Service] .....	54,
[Configuration Service] .....	59,
[Configuration Service] .....	91,
[VPN] .....	209,
[VPN] .....	210,
[VPN] .....	211,



Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

[Mail Gateway] .....	261,	Port Labelling [Configuration Service] .....	63
[Proxy] .....	326,	Port Range [Firewall] .....	144
[Anti-Virus] .....	368,	Port Scan [Firewall] .....	130
[phion management centre] .....	434,	Port Scan Detection Interval [Firewall] .....	129
[phion management centre] .....	460,	Port Scan Threshold [Firewall] .....	129
[phion management centre] .....	472	Portmapper Port [Firewall] .....	194
Password Length [FTP Gateway] .....	353	Position [Getting Started] .....	22
Password must differ on change [phion management centre] .....	434	Post Settings [Mail Gateway] .....	251
Password Protection [Configuration Service] .....	102	Postinstall-script [Getting Started] .....	14
Path [VPN] .....	219	Postmaster Mail-Address [Mail Gateway] .....	247
Pattern [Firewall] .....	152,	PPP Local IP [Configuration Service] .....	67
[Mail Gateway] .....	251	PPP Remote IP [Configuration Service] .....	67
PDP Context [Configuration Service] .....	77	PPTP Bind IP [VPN] .....	211
PDP Type [Configuration Service] .....	77	PPTP Enable [VPN] .....	211
Peer [phion management centre] .....	476	Pre Settings [Mail Gateway] .....	251
Peer Address/Network [VPN] .....	219	Preauthentication Scheme [VPN] .....	218
Peer IP Restriction [Configuration Service] .....	91,	Prebuild Cookies on Startup [VPN] .....	207,
[phion management centre] .....	434	[phion management centre] .....	416
Peer SSL Certificate [Configuration Service] .....	117	Preceding Private Key #1, #2, #3 [phion management centre] .....	413
Peers [SNMP] .....	481	Preceding SSH Key [phion management centre] .....	413
Peer-To-Peer Bandwidth [Firewall] .....	126	Prefer Routing over Bridging [Firewall] .....	155
Peer-To-Peer Policy [Firewall] .....	126	Preferred Transport Class [VPN] .....	224
Pending [Firewall] .....	169,	Preferred Transport ID [VPN] .....	224
[phion management centre] .....	399	Prefix [Voice over IP] .....	359
Pending Accepts Critical [Firewall] .....	130	Prefix Length [OSPF and RIP] .....	491
Pending Session Limit [SSH Gateway] .....	365	Preinstall-script [Getting Started] .....	14
Pending Session Limitation [VPN] .....	207,	Prepend Hierarchy Info [Configuration Service] .....	117
[phion management centre] .....	416	Prepend Received Time [phion management centre] .....	449
Perform DDNS Updates [DHCP] .....	274,	Primary / Secondary [Getting Started] .....	11
[DHCP] .....	275	Primary Box [Configuration Service] .....	96
Perform Mask Discovery [DHCP] .....	276,	Primary Link [Configuration Service] .....	71
[DHCP] .....	284	Primary Network Interface [Firewall] .....	151
Perform Router Discovery [DHCP] .....	276,	Primary Sever [DNS] .....	319
[DHCP] .....	284	Print Header [Getting Started] .....	22
Performance Statistics [Configuration Service] .....	118	Priority [Configuration Service] .....	87,
Permission Profile [SSH Gateway] .....	366	[phion management centre] .....	403
Permit Root Login [Configuration Service] .....	107	Priority Adjustment [Configuration Service] .....	85,
Persistence [Firewall] .....	154	[Configuration Service] .....	86
Persistent [Eventing] .....	307	Priority Switch after (minutes) [Mail Gateway] .....	250
Phase 1 Lifetime (s) [VPN] .....	211	Priority Weights [Configuration Service] .....	85,
PHIBS Authentication Scheme [Firewall] .....	189,	[Configuration Service] .....	86
[Proxy] .....	328,	Privileged Admins [phion management centre] .....	419
[FTP Gateway] .....	354	Privileged RIP Terminal Password [OSPF and RIP] .....	487
PHIBS Listen IP [Firewall] .....	189,	Privileged Terminal Password [OSPF and RIP] .....	486
[Proxy] .....	328,	Product Type [Configuration Service] .....	52,
[FTP Gateway] .....	354	[Configuration Service] .....	95,
Phibs Scheme [VPN] .....	209	[phion management centre] .....	393
Phibs settings [FTP Gateway] .....	354	Progress Popup [Anti-Virus] .....	370
PHIBS Timeout [Firewall] .....	189,	Progress Template [Anti-Virus] .....	371
[Proxy] .....	328,	Propagate to MC [Eventing] .....	307,
[FTP Gateway] .....	354	[Eventing] .....	308
Phion Archive Files [Getting Started] .....	15	Propagation List [Firewall] .....	187
Phion Client [VPN] .....	219	Protection Profile [Mail Gateway] .....	248
Phion Personal [VPN] .....	208	Proto. [Firewall] .....	173
Phion Site-to-Site [VPN] .....	208	Protocol [VPN] .....	208
phiona Max. Idle [Configuration Service] .....	118	Protocol Config [Proxy] .....	330
Phone Number [Configuration Service] .....	77	Protocol Field [Configuration Service] .....	75
Physical Interfaces [Configuration Service] .....	64	Protocol Selection [Firewall] .....	126
Ping Check [DHCP] .....	278	Protocol Type [VPN] .....	232
Ping Timeout [DHCP] .....	278	Provider Name [Configuration Service] .....	72,
PKCS7 Cipher [Configuration Service] .....	59	[Configuration Service] .....	75
PKCS7 Hash [Configuration Service] .....	59	Provider Phone Number [Configuration Service] .....	74
PKCS7 Replay Protection [Configuration Service] .....	59	Proxy [VPN] .....	209
Plugin [Firewall] .....	144	Proxy Address [VPN] .....	210
Policy [Configuration Service] .....	88,	Proxy ARPs [Firewall] .....	134
[Firewall] .....	146,	Proxy Assigned [Firewall] .....	146
[Firewall] .....	155,	Proxy Authentication Type [Configuration Service] .....	59
[Firewall] .....	190,	Proxy Domain [Configuration Service] .....	59
[FTP Gateway] .....	353,	Proxy Dynamic [Firewall] .....	146
[FTP Gateway] .....	354	Proxy First [Firewall] .....	146
Policy Server IP [VPN] .....	232	Proxy Host [Proxy] .....	344
Policy Service IPs/Names [DHCP] .....	276	Proxy IP Address [Configuration Service] .....	59
Policy Service Permissions [phion management centre] .....	414	Proxy Password [Configuration Service] .....	59,
Poll Box VPN Status [phion management centre] .....	413	[Configuration Service] .....	67,
Poll VPN Tunnel Status [Configuration Service] .....	53	[Proxy] .....	344
Polling Time (secs) [Firewall] .....	194	Proxy Port [Proxy] .....	326,
Pool description [DHCP] .....	274	[Proxy] .....	344
Pool IP-Begin [VPN] .....	211	Proxy Port Number [Configuration Service] .....	59
Pool Size [VPN] .....	211	Proxy Second [Firewall] .....	146
Popup After (sec) [Anti-Virus] .....	370	Proxy Server IP [Configuration Service] .....	67
Port [Firewall] .....	173,	Proxy Server Port [Configuration Service] .....	67
[VPN] .....	209,	Proxy Settings [Configuration Service] .....	59
[Anti-Virus] .....	368		
Port Config [Proxy] .....	330		



Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Proxy Type [VPN].....	210,	Redirected [Firewall].....	137
[VPN].....	222	Redirection [FTP Gateway] .....	353
Proxy User [Configuration Service] .....	67,	Referenced Map [Firewall].....	138
[VPN].....	210,	References [Configuration Service].....	64
[Proxy].....	344	Refresh (% Lifetime) [Configuration Service] .....	59
Proxy User Name [Configuration Service].....	59	Refresh after [DNS].....	319
Proxydyn [Firewall] .....	162	Refresh auth every ... min [Firewall].....	189
Public Key [phion management centre].....	434	Refresh auth tolerance ... min [Firewall].....	189
Public RSA Key [Configuration Service] .....	54,	Refresh Timer [OSPF and RIP] .....	486
[Configuration Service].....	91	Refuse Empty Mail from [Mail Gateway] .....	255
<b>Q</b>		Register in Standby [Configuration Service] .....	76
Quarantine [VPN].....	206	Register Timeout [Configuration Service] .....	76
Quarantine Class 1 Interface [Firewall].....	184	Registry [VPN] .....	216
Quarantine Class 2 Interface [Firewall] .....	184	Regular Poll Interval [Configuration Service].....	118
Quarantine Class 3 Interface [Firewall] .....	184	Relay Interfaces [DHCP].....	286
Quarantine Directory [Anti-Virus].....	368	Release [phion management centre].....	420
Quarantine Group [Firewall].....	184	Reload Externals [Firewall] .....	135
Query Process Priority [Statistics] .....	300	Reload GTI Objects [Firewall].....	135
Query Source Address [Configuration Service].....	55	Reload Object [phion management centre] .....	403
Queue Size (Bytes) [Configuration Service] .....	85,	Remote Address [VPN].....	227
[Configuration Service].....	86	Remote Control via SMS [Configuration Service] .....	58
<b>R</b>		Remote End IP [Configuration Service].....	79
Radio Preference [Configuration Service].....	76	Remote Loghost [Configuration Service] .....	117
Radius IDCache Timeout [Voice over IP].....	359	Remote Networks [Configuration Service].....	67,
Radius Password [Voice over IP].....	359	[VPN] .....	227
Radius Server [Voice over IP] .....	359	Remote Peer IP [Configuration Service].....	78
Radius Server Address [Configuration Service].....	114	Remove [phion management centre].....	402,
Radius Server Key [Configuration Service].....	114	[phion management centre] .....	403,
Radius Server Port [Configuration Service] .....	114	[phion management centre] .....	408
Radius Server Timeout [Voice over IP] .....	359	Remove Box [phion management centre].....	403
Radius Server Transmission [Voice over IP].....	359	Remove Boxes [phion management centre].....	414
Radius with Terminal Alias [Voice over IP] .....	359	Remove Cluster [phion management centre].....	414
Range [phion management centre] .....	434	Remove from Grey List after (h) [Mail Gateway] .....	254
Range Action [OSPF and RIP] .....	487	Remove from White List after (d) [Mail Gateway] .....	254
Range Cost [OSPF and RIP] .....	487	Remove HTML Img Src Tag [Mail Gateway] .....	255
Range DHCP Options [DHCP].....	274	Remove HTML Link Tag [Mail Gateway] .....	255
Range IDs [Configuration Service] .....	104	Remove HTML Tags [Mail Gateway].....	255
Range Name [phion management centre].....	416	Remove License [phion management centre] .....	414
RAS Authentication [Voice over IP] .....	359	Remove Phion ID [Mail Gateway] .....	255
Raw [Anti-Virus].....	370	Remove Range [phion management centre] .....	414
RDP Application Path [VPN].....	233	Remove Repository [phion management centre] .....	414
Reachable IPs [Configuration Service].....	67,	Remove Server [phion management centre] .....	414
[Configuration Service].....	69,	Remove Service [phion management centre] .....	414
[Configuration Service].....	78	Renew Time [DHCP] .....	283
Read [phion management centre].....	420	Repair Attempts [Configuration Service] .....	110
Read Box Logfiles [phion management centre].....	414	Repair Mode [Configuration Service].....	110
Read Box Statistics [phion management centre].....	414	Replay Window Size [VPN].....	226,
Read Only Colour... [Getting Started].....	22	[VPN] .....	228
Read Service Logfiles [phion management centre].....	414	Reply AID Mismatch Policy [DHCP].....	286
Read Timeout (sec.) [Proxy].....	335	Reply Delay [DHCP].....	277
Read Timeout in seconds for data [phion management centre]	436	Reply Timeout [Voice over IP].....	360
Real IP/Mask [Firewall] .....	138	Reply to Ping [Configuration Service] .....	95
Realtime Mode [Configuration Service].....	110	Report Language [Mail Gateway].....	260
Rebind Time [DHCP] .....	283	Report Processing Script [phion management centre] ...	474
Reboot [Configuration Service].....	58	Request Timeout (sec) [Configuration Service].....	115
Reboot System [phion management centre] .....	414	Requestmethod Config [Proxy].....	330
Rebuild Mgmt Tunnel [Configuration Service] .....	58	Require PAP [Configuration Service].....	67
Receive Protocol [OSPF and RIP] .....	489	Required DHCP Link [Configuration Service] .....	71
Recipient Blacklist [Mail Gateway] .....	254	Required for All Users [Proxy].....	330
Recipient DB [Mail Gateway] .....	249	Requires Authentication [Anti-Virus].....	368
Recipient Dropped [Mail Gateway] .....	256	Re-Reachable Command [Configuration Service] .....	69
Recipient Lookup [Mail Gateway] .....	248	Reschedule [phion management centre].....	402
Recipient Whitelist [Mail Gateway] .....	253	Resolution [Statistics].....	301,
Recipients [Mail Gateway] .....	249	[phion management centre] .....	439
Recipients Lookup req. Groups [Mail Gateway] .....	247,	Resolution 1d after (Days) [Statistics] .....	301
[Mail Gateway] .....	249	Resolution 1d after (days) [phion management centre] ...	439
Reconnect Network [Configuration Service].....	58	Resolution 1h after (Days) [Statistics] .....	301
Record Terminal Session [SSH Gateway] .....	366	Resolution 1h after (days) [phion management centre] ...	439
Recorded Users [SSH Gateway] .....	366	Resolve [Firewall].....	142
recursion [DNS] .....	317	Resolve Access Cache IPs [Firewall] .....	129
Redirect [Firewall] .....	136,	Resource Location Server [DHCP] .....	276,
[Firewall] .....	137,	[DHCP].....	284
[Firewall] .....	138,	Responds to Ping [Configuration Service] .....	62
[Firewall] .....	139,	Responsible person [DNS] .....	319
[Firewall] .....	162	Restart Network Subsystem [phion management centre].....	414
Redirect Object [Firewall].....	136,	Restart phion Services [Configuration Service].....	58
[Firewall] .....	137,	Restart Phion Subsystem [phion management centre] ...	414
[Firewall] .....	138,	Restart Processes [phion management centre].....	399
[Firewall] .....	139	Restrict PARP to Parent Network [Firewall].....	141
		Resume Delivery [Mail Gateway] .....	264
		Retransmission Timeout (s) [Firewall].....	154
		Retrieve Stripped Attachments [phion management centre].....	415



Retry after [DNS] ..... 319  
 Retry Time [Configuration Service] ..... 74,  
   [Configuration Service] ..... 75,  
   [Configuration Service] ..... 77  
 Rev DDNS Domainname [DHCP] ..... 277  
 Reverse [DNS] ..... 318  
 Reverse Band [Firewall] ..... 136  
 Reverse Interface [Firewall] ..... 150  
 Reverse Lookup Net [Configuration Service] ..... 56,  
   [DHCP] ..... 278  
 Reverse Lookup Netmask [Configuration Service] ..... 56  
 Rewrite [Mail Gateway] ..... 251  
 RFC1048 Conformance [DHCP] ..... 277  
 RFC1583 Compatibility [OSPF and RIP] ..... 486  
 RIP Key Chain [OSPF and RIP] ..... 489  
 RIP Keychains [OSPF and RIP] ..... 487  
 RIP Metric [OSPF and RIP] ..... 488  
 RIP Terminal Password [OSPF and RIP] ..... 487  
 RIP Text [OSPF and RIP] ..... 491  
 RIP Text Secret [OSPF and RIP] ..... 489  
 RIP Version [OSPF and RIP] ..... 487  
 Roles [Configuration Service] ..... 91,  
   [phion management centre] ..... 435  
 Root Aliases [Configuration Service] ..... 54  
 Root CA Certificate [Proxy] ..... 338  
 Root CA Private Key [Proxy] ..... 338  
 Root Certificate [phion management centre] ..... 467,  
   [phion management centre] ..... 468  
 Root certificates [Firewall] ..... 189  
 Root DN [phion management centre] ..... 459  
 Root Password [phion management centre] ..... 459  
 Root Public RSA Key [Configuration Service] ..... 54  
 Root RSA Key [Getting Started] ..... 13  
 Route In/Out Filters [OSPF and RIP] ..... 488  
 Route Maps [OSPF and RIP] ..... 487,  
   [OSPF and RIP] ..... 488  
 Route Preference Number [Configuration Service] ..... 69,  
   [Configuration Service] ..... 73,  
   [Configuration Service] ..... 74,  
   [Configuration Service] ..... 76,  
   [Configuration Service] ..... 78,  
   [Configuration Service] ..... 79  
 Route Redistribution [OSPF and RIP] ..... 487,  
   [OSPF and RIP] ..... 488  
 Route Type [Configuration Service] ..... 69  
 Route Types [OSPF and RIP] ..... 487,  
   [OSPF and RIP] ..... 488  
 Route Update Filtering [OSPF and RIP] ..... 488  
 Router [DHCP] ..... 276,  
   [DHCP] ..... 283  
 Router ID [OSPF and RIP] ..... 485  
 Router ID Mask [OSPF and RIP] ..... 485  
 Routes [Configuration Service] ..... 70  
 Routing Next-Hop [VPN] ..... 221,  
   [phion management centre] ..... 467  
 Routing Protocols [OSPF and RIP] ..... 489  
 RSA Configuration File [Configuration Service] ..... 114  
 RSA Host Key [SSH Gateway] ..... 365  
 RSA Server IP [Configuration Service] ..... 114  
 RSA Slave-Server IP [Configuration Service] ..... 114  
 RSA Unique Name [Configuration Service] ..... 114  
 Rule [Firewall] ..... 178  
 Rule Change Behaviour [Firewall] ..... 128  
 Rule Limit Exceeded [Firewall] ..... 129  
 Rule Tester [Firewall] ..... 134  
 Rules [Firewall] ..... 134,  
   [Mail Gateway] ..... 261  
 Run as User [SSH Gateway] ..... 365,  
   [phion management centre] ..... 448  
 Run Forwarding/Caching DNS [Configuration Service] ..... 55  
 Run OSPF Router [OSPF and RIP] ..... 485  
 Run Probes Every [Configuration Service] ..... 67  
 Run RIP Router [OSPF and RIP] ..... 485  
 Run S.M.A.R.T [Configuration Service] ..... 110  
 Run Slave DNS [Configuration Service] ..... 55  
 Run Watchdog [Configuration Service] ..... 110

**S**

Minimum Slave Uptime [Configuration Service] ..... 75  
 Same Port [Firewall] ..... 146  
 Save Object [phion management centre] ..... 402  
 Save to [Getting Started] ..... 14  
 Save to Disk [Getting Started] ..... 14

Scan Archives [Anti-Virus] ..... 369  
 Scan Engine IPs [Anti-Virus] ..... 372  
 Scan Engine Port [Anti-Virus] ..... 372  
 Scanner IP [Anti-Virus] ..... 371  
 Scanner Location [Anti-Virus] ..... 370,  
   [Anti-Virus] ..... 371  
 Scanning Exceptions [Anti-Virus] ..... 369  
 SCEP HTTPS Client Cert. [Configuration Service] ..... 59  
 SCEP HTTPS Client Key [Configuration Service] ..... 59  
 SCEP Password [Configuration Service] ..... 59  
 SCEP Password Policy [Configuration Service] ..... 59  
 SCEP Password Search Pattern [Configuration Service] ..... 59  
 SCEP Password URL Path [Configuration Service] ..... 59  
 SCEP Server IP or Hostname [Configuration Service] ..... 59  
 SCEP server port number [Configuration Service] ..... 59  
 SCEP server protocol [Configuration Service] ..... 59  
 SCEP Settings [Configuration Service] ..... 58  
 SCEP URL path [Configuration Service] ..... 59  
 Scheduled Time [phion management centre] ..... 403  
 Scheduler Priority [Configuration Service] ..... 110  
 Scheduling Mode [phion management centre] ..... 403  
 Scheme [VPN] ..... 213  
 Second DNS [VPN] ..... 210  
 Second Try Transport Class [VPN] ..... 224  
 Second Try Transport ID [VPN] ..... 224  
 Second WINS [VPN] ..... 210  
 Secondary Box [Configuration Service] ..... 96  
 Second-IP (S2) [Configuration Service] ..... 95  
 Secure Client [VPN] ..... 216  
 Secure FTP Support [Configuration Service] ..... 107  
 Secure Update [Configuration Service] ..... 72,  
   [Configuration Service] ..... 73,  
   [Configuration Service] ..... 75,  
   [Configuration Service] ..... 77  
 Secure-Web-Proxy Permissions [phion management centre] ..... 415  
 Select Encryption Certificate [Configuration Service] ..... 59  
 Select Smartcard Reader [Getting Started] ..... 23  
 Selected Message Types [Configuration Service] ..... 116  
 Selection [phion management centre] ..... 399  
 Self-Signed Certificate [VPN] ..... 231  
 Self-Signed Private Key [VPN] ..... 231  
 Send Event to MC [Eventing] ..... 311  
 Send Keepalives [Configuration Service] ..... 107  
 Send Protocol [OSPF and RIP] ..... 489  
 Send Statistics to Reporter [phion management centre] ..... 417,  
   [phion management centre] ..... 418  
 Send TCP RST for OOS Pkts. [Firewall] ..... 129  
 Send to IP Address [Firewall] ..... 130  
 Send to Port [Firewall] ..... 130  
 Send Unsolicited ARP [Firewall] ..... 151  
 Sender Blacklist [Mail Gateway] ..... 254  
 Sender IP [Configuration Service] ..... 117,  
   [phion management centre] ..... 451  
 Sender Whitelist [Mail Gateway] ..... 253  
 Sequence Number [OSPF and RIP] ..... 490  
 Serial [DNS] ..... 319  
 Serial Access / Serial Settings [Configuration Service] ..... 54  
 Serial Console [Getting Started] ..... 11,  
   [Configuration Service] ..... 102  
 Serial Number [Configuration Service] ..... 52  
 Serial Settings [Configuration Service] ..... 54  
 Server [Firewall] ..... 190,  
   [phion management centre] ..... 468  
 Server Address Labels [Configuration Service] ..... 97  
 Server Alive Interval [SSH Gateway] ..... 366  
 Server Certificate [Configuration Service] ..... 96,  
   [VPN] ..... 218  
 Server Default [Firewall] ..... 154  
 Server IP [VPN] ..... 233,  
   [DHCP] ..... 274,  
   [DHCP] ..... 275,  
   [phion management centre] ..... 472  
 Server Is Authoritative [DHCP] ..... 273,  
   [DHCP] ..... 274,  
   [DHCP] ..... 275  
 Server Key [VPN] ..... 214  
 Server Key Length (Bits) [Configuration Service] ..... 107  
 Server Log Level [SSH Gateway] ..... 365  
 Server Name [Configuration Service] ..... 95  
 Server Port [phion management centre] ..... 472  
 Server Private Key [Configuration Service] ..... 96  
 Server Protocol Key [VPN] ..... 218  
 Server/GTI Networks [Configuration Service] ..... 96

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Servername [DNS].....	320	Skip Null Stats [Statistics].....	300
Service [Firewall].....	154,	Skip RBL-Tests [Mail Gateway].....	260
[Firewall].....	174,	Slave [DNS].....	318
[Firewall].....	190,	Slave Channel Policy [Configuration Service].....	75
[phion management centre].....	468	Slave Devices [Configuration Service].....	65
Service Certificate [phion management centre].....	448,	SMB Path [VPN].....	233
[phion management centre].....	449	SMP Kernel [Configuration Service].....	102
Service Configuration [VPN].....	233	SNMP Access Groups [SNMP].....	481
Service Default (Failure) [Configuration Service].....	98	SNMP Address [Proxy].....	327
Service Default (Success) [Configuration Service].....	98	SNMP Community [Eventing].....	311
Service Key [phion management centre].....	448	SNMP Destination [Eventing].....	311
Service Label [Firewall].....	144	SNMP Port [Proxy].....	327
Service Log Patterns [Configuration Service].....	116,	SNMP Settings [Proxy].....	325
[phion management centre].....	451	Socket Connect [Getting Started].....	22
Service Name [Configuration Service].....	72,	Socks Port on 1st IP [Firewall].....	131
[Configuration Service].....	97	Socks Port on 2nd IP [Firewall].....	131
Service Statistics [Firewall].....	155	Software Module [Configuration Service].....	97,
Service Type [Configuration Service].....	77	[phion management centre].....	419
Services [Firewall].....	134	Software Release [phion management centre].....	418
Session Duration Limit (s) [Firewall].....	155	Source [Firewall].....	154,
Session Termination [Firewall].....	130	[Firewall].....	173
Session Timeout [Firewall].....	144	Source Address [Configuration Service].....	69,
Session/Src Limit Exceeded [Firewall].....	129	[Firewall].....	178
Set Action [OSPF and RIP].....	490	Source Address Restriction [Firewall].....	151
Set allow [Firewall].....	140,	Source Interface [Firewall].....	150
[Firewall].....	157,	Source IP [Configuration Service].....	79
[Proxy].....	332,	Source IP Config [Proxy].....	329,
[Proxy].....	346	[Proxy].....	346
Set HW Clock to UTC [Configuration Service].....	56	Source IP Type [Configuration Service].....	79
Set Multicast Flag [Configuration Service].....	79	Source Mask [Configuration Service].....	79
Set or Sync Box Time [phion management centre].....	414	Source Networks [Configuration Service].....	70,
Set OSPF External Metric [OSPF and RIP].....	490	[Configuration Service].....	72,
Set OSPF Metric [OSPF and RIP].....	490	[Configuration Service].....	74,
Set RIP Metric [OSPF and RIP].....	490	[Configuration Service].....	76,
Set RIP Next-Hop IP [OSPF and RIP].....	490	[Configuration Service].....	77,
Set Timeout [Control Centre].....	38	[Configuration Service].....	79
Set TOS Value [Firewall].....	155	Source Port [Firewall].....	178
Settings [Firewall].....	129,	Source/Rule Limit Exceeded [Firewall].....	129
[Firewall].....	188	Spam Analyser IP [Mail Gateway].....	259
Settings for [Statistics].....	300,	Spam Analyser Port [Mail Gateway].....	259
[phion management centre].....	439	Spam Detection [Mail Gateway].....	253
settings for [phion management centre].....	440	SPAM Mail Modification [Mail Gateway].....	260
Setup [Firewall].....	135	Spawn Parameter [DHCP].....	278
Severity ID [Eventing].....	307,	Spawn Subclasses [DHCP].....	278
[Eventing].....	308	Spec Type [Eventing].....	309
severity_tab_R.gif [Eventing].....	307	Special File Patterns [phion management centre].....	450
Shared DHCP Options [DHCP].....	273,	Special Networks [phion management centre].....	426
[DHCP].....	274	Special Type [OSPF and RIP].....	487
Shared Network Device [DHCP].....	274	Specialnet [phion management centre].....	426
Shared Parameters [DHCP].....	273,	Specific Cook Settings [phion management centre].....	418
[DHCP].....	274	Specifies the provider type [Getting Started].....	23
Shell Level [Configuration Service].....	91,	Specify Destination Port Address [Proxy].....	330
[phion management centre].....	435	Speed (baud) [Configuration Service].....	76
Show ... [phion management centre].....	408	SPF Delay Timer [OSPF and RIP].....	486
Show Admins [phion management centre].....	414	SPF Hold Timer [OSPF and RIP].....	486
Show as Text [OSPF and RIP].....	491	Spool ID [Mail Gateway].....	266
Show Box REXEC [phion management centre].....	414	Spool Queue Sync [Mail Gateway].....	250
Show Box Software Updates [phion management centre].....	414	Spooling Limit [Mail Gateway].....	256
Show Config. Updates [phion management centre].....	414	Src Filter [Statistics].....	299
Show Detail for Linked Nodes [phion management centre].....	476	Src Statistics [Configuration Service].....	97
Show Full Screen (F11) [phion management centre].....	466	Src Time-Statistics [Configuration Service].....	97
Show GUI as Text [DHCP].....	279	Src-Dst Statistics [Configuration Service].....	97
Show Last Update Time [phion management centre].....	472	SSH Authentication Key [phion management centre].....	449
Show Log ... [phion management centre].....	403	SSH Escape Character [SSH Gateway].....	366
Show Map [phion management centre].....	414	SSH Host Key [phion management centre].....	449
Show Name [phion management centre].....	468	SSH login [Configuration Service].....	106
Show Save Button [Anti-Virus].....	370	SSH Private Key [Configuration Service].....	60
Show Selected Object... [Firewall].....	160	SSHD Port [phion management centre].....	449
Show Tunnel Names [phion management centre].....	466	SSHD rexec [Configuration Service].....	106
Signing CA [phion management centre].....	460	SSL Busy Timeout [phion management centre].....	448,
Silence Events [phion management centre].....	414	[phion management centre].....	450
Silent Box [Eventing].....	311	SSL Certificate [Configuration Service].....	116
Silently Drop Phishing Mail [Anti-Virus].....	372	SSL Close Timeout [phion management centre].....	448,
SIM PIN [Configuration Service].....	76	[phion management centre].....	450
Simple Authentication Key [OSPF and RIP].....	487,	SSL Idle Timeout [phion management centre].....	448,
[OSPF and RIP].....	489	[phion management centre].....	450
Single IPs [Proxy].....	329,	SSL Listen Port [phion management centre].....	448
[Proxy].....	330	SSL Peer Authentication [Configuration Service].....	117,
Size [Getting Started].....	12	[phion management centre].....	450
Size (%) [Configuration Service].....	101	SSL Private Key [Configuration Service].....	116
Size (MB) [Configuration Service].....	101	SSL Tunnels [VPN].....	233
Size in MB [Proxy].....	325	Standalone [Firewall].....	151
Size Settings [Configuration Service].....	101		

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Standby Mode [Configuration Service] ..... 71,  
 [Configuration Service] ..... 73,  
 [Configuration Service] ..... 76

Start Data Collection (hour) [phion management centre]. 436

Start Date [phion management centre]. 476

Start LDAP Server [phion management centre] ..... 459

Start NTPd [Configuration Service] ..... 57

Start Script [Configuration Service]. 96

Start Server [phion management centre]. 414

Start Service [phion management centre] ..... 414

Startup Poll Interval [Configuration Service] ..... 117

Stat. Name [VPN]. 213

State [Configuration Service] ..... 59

State or Province [phion management centre] ..... 461

Static Bridge MAC [Firewall] ..... 184

Static Gateway IP [Configuration Service] ..... 75

Static IP/Mask [Configuration Service] ..... 75

Static Route [DHCP] ..... 284

Static Route Net [DHCP]. 276

Static Source IP [SSH Gateway] ..... 366

Statistic [Getting Started] ..... 22

Statistic Name [VPN] ..... 217

Statistics Entry [Firewall]. 155

Statistics for Local Firewall [Firewall] ..... 129

Statistics Permissions [phion management centre] ..... 414

Statistics Settings [Mail Gateway] ..... 256

Statistics Type [Statistics]. 297

Statistics type [Statistics] ..... 299

Stop Alarm [phion management centre]. 414

Stop Script [Configuration Service] ..... 96

Stop Server [phion management centre] ..... 414

Stop Service [phion management centre] ..... 414

Storage Architecture [Configuration Service]. 52

Storage Dir [Configuration Service]. 104

Storage Time [Configuration Service] ..... 104

Store on Disk [phion management centre]. 448

Stream Forwarding [Firewall] ..... 154

strictly internal [Mail Gateway]. 248

strictly\_foreign [Mail Gateway]. 248

String Length [FTP Gateway] ..... 353

Strip Received Lines [Mail Gateway] ..... 255

Strip Received Lines Text [Mail Gateway]. 255

Subject [Firewall]. 190,  
 [VPN] ..... 207,  
 [VPN] ..... 208,  
 [VPN] ..... 219,  
 [Mail Gateway] ..... 250

Subject Blacklist [Mail Gateway]. 254

subjectAltName [phion management centre]. 461

subjectKeyIdentifier [phion management centre]. 461

Subnet Description [DHCP] ..... 274

Subnet DHCP Options [DHCP]. 274,  
 [DHCP] ..... 275

Subnet mask [Getting Started] ..... 10

Subnet Parameters [DHCP]. 274,  
 [DHCP] ..... 275

Subnet Type [DHCP] ..... 274

Subnetmask [DHCP] ..... 276,  
 [DHCP] ..... 283

Successive Command Maximum [Configuration Service] . 58

Summary Range IP/Mask [OSPF and RIP]. 487

Superordinate domain [DNS]. 320,  
 [DNS] ..... 321

Support Agent Forwarding [SSH Gateway]. 366

Support Opaque LSA [OSPF and RIP] ..... 486

Support Trusted Data Reception [phion management centre]. 448

Support X11 Forwarding [SSH Gateway] ..... 365

Supported Protocols [Configuration Service] ..... 107,  
 [phion management centre] ..... 448

Supported SSH Protocol [SSH Gateway]. 366

Swap List View [phion management centre] ..... 465

Swap Server [DHCP] ..... 276,  
 [DHCP] ..... 284

SYN Cookie High Watermark (%) [Firewall]. 128

SYN Cookie Low Watermark (%) [Firewall] ..... 128

Syn Flood Protection (Forward) [Firewall] ..... 154

Syn Flood Protection (Reverse) [Firewall] ..... 154

Sync Authentication to Trustzone [VPN] ..... 207

Sync Timeout (s) [phion management centre]. 436

Sync to HA Partner [phion management centre] ..... 448

Synchronous PPP [Configuration Service]. 71

Sys-CMD (login) [Configuration Service]. 106

Sys-CMD (su) [Configuration Service] ..... 106

system [SNMP]. 481

**T**

t.disabled [Eventing] ..... 312

Table Names [OSPF and RIP] ..... 486,  
 [OSPF and RIP] ..... 488

Table Placement [Configuration Service]. 70,  
 [Configuration Service] ..... 79

Target Alive Interval [SSH Gateway]. 366

Target Alive Max Count [SSH Gateway] ..... 366

Target FQDN [SSH Gateway]. 366

Target IP Address [SSH Gateway] ..... 366

Target List [Firewall]. 138

Target Network Address [Configuration Service]. 69

Target Networks [Configuration Service]. 67,  
 [Configuration Service] ..... 72,  
 [Configuration Service] ..... 74,  
 [Configuration Service] ..... 76,  
 [Configuration Service] ..... 78,  
 [Configuration Service] ..... 79

TCP ECN Active [Configuration Service]. 100

TCP Listen Port [SSH Gateway] ..... 365

TCP Listening Port [Proxy] ..... 325

TCP Outgoing Address [Proxy]. 325

TCP Port [phion management centre]. 448

TCP Retry Interval [Configuration Service] ..... 115,  
 [phion management centre] ..... 450

TCP Sync Frequency (lines) [phion management centre]. 449

Telephone Nr. [phion management centre]. 416,  
 [phion management centre] ..... 418

Template [Mail Gateway]. 250,  
 [phion management centre] ..... 460

Template Zone [DNS]. 317

Terminal Password [OSPF and RIP]. 486

Terminate Connections [phion management centre]. 415

Terminate existing [Firewall]. 140,  
 [Firewall]. 157

Terminate VPN Tunnels [phion management centre] .... 415

Test Report [Firewall]. 134

Text [DNS]. 321

Text To Insert Into Subject [Mail Gateway] ..... 260

Texture Quality [phion management centre]. 471

TFTP Server Name [DHCP] ..... 277,  
 [DHCP]. 284

Thickness [phion management centre]. 468

Threshold [Mail Gateway] ..... 260

TI Classification [VPN] ..... 224

TI Learning Policy [VPN] ..... 225

Ticket Management [phion management centre]. 415

TI-ID [VPN] ..... 224

Time [VPN] ..... 215

Time (h) [Mail Gateway]. 261

Time (min) [Mail Gateway]. 261

Time Interval [DHCP] ..... 273

Time Object [Firewall]. 156

Time Object Name [Firewall]. 140

Time Offset [DHCP]. 276,  
 [DHCP]. 284

Time Period [Configuration Service]. 87

Time Restriction [Firewall]. 155

Time Restrictions [Proxy] ..... 329

Time Server [DHCP] ..... 276,  
 [DHCP]. 284

Time Server IP [Configuration Service]. 57

Time Settings [Proxy]. 329,  
 [Proxy]. 346,  
 [FTP Gateway] ..... 354

Time Zone [Getting Started] ..... 11,  
 [Proxy]. 329,  
 [Proxy]. 345,  
 [FTP Gateway] ..... 354

Timed [Firewall]. 156,  
 [Firewall]. 159

timed [Firewall] ..... 136

Timeout [Mail Gateway] ..... 250,  
 [Mail Gateway]. 259,  
 [Proxy]. 345,  
 [FTP Gateway] ..... 354

Timeout (min.) [VPN] ..... 208

Timeout Timer [OSPF and RIP]. 488

Timezone [Configuration Service] ..... 56

Toggle Release View [phion management centre] ..... 421

Toggle Trace [phion management centre]. 415

Tools [phion management centre]. 465

Numerics | A B C D E F G H I K L M N O P Q R S T U V W X Y Z

Top Level Logdata [phion management centre] .....	450	URL [Getting Started] .....	10,
Top most directory [FTP Gateway] .....	353	[VPN] .....	232
TOS [Configuration Service] .....	87	URL Config [Proxy] .....	330
TOS Policy [VPN] .....	226,	URL Extensions [Proxy] .....	330
[VPN] .....	228	URL Fetching [Proxy] .....	326
Total Poll Time [phion management centre] .....	413	URL Path Config [Proxy] .....	330
Trace Reachable Statistics [phion management centre] .	413	URL Path Extensions [Proxy] .....	330
Traffic Limit [Configuration Service] .....	87	URL-Path [VPN] .....	209
Transaction ID Encoding [Configuration Service] .....	59	Usage Policy [Configuration Service] .....	118
Transaction Timeout [Voice over IP] .....	360	Usage pull-down [VPN] .....	214
Transfer Source Address [Configuration Service] .....	56	USB Device on Box [Getting Started] .....	14
transfer-source-ip [DNS] .....	319	Use Assigned IP [Configuration Service] .....	74,
Translated HA IP [Configuration Service] .....	118	[Configuration Service] .....	76,
Transmission Mode [Configuration Service] .....	117,	[Configuration Service] .....	77
[phion management centre] .....	451	Use Black List Tests [Mail Gateway] .....	260
Transparent Failover State Sync [Firewall] .....	155	Use Box Certificate/Key [Configuration Service] .....	116
Transport [VPN] .....	221,	Use Channel Bonding [Configuration Service] .....	75
[phion management centre] .....	467	Use Compression [phion management centre] .....	449
Transport Protocol [Configuration Service] .....	67	Use DCC [Mail Gateway] .....	260
Tree Name [Configuration Service] .....	85	Use Dynamic DNS [Configuration Service] .....	72,
Trickle HTTP 1.0 [Anti-Virus] .....	370	[Configuration Service] .....	73,
Trickle Period (sec) [Anti-Virus] .....	370	[Configuration Service] .....	75,
Trickle Size Low Watermark (MB) [Anti-Virus] .....	370	[Configuration Service] .....	77
Trusted Clients [phion management centre] .....	449	Use Event ID [Eventing] .....	309
Trusted Local Networks [phion management centre] .....	426	Use Forward Address [Firewall] .....	159
Tunnel Check Interval (s) [VPN] .....	208	Use Free Format [DHCP] .....	279,
Tunnel Client Application [VPN] .....	233	[OSPF and RIP] .....	491
Tunnel Details [Configuration Service] .....	67	Use Group Policies [VPN] .....	231,
Tunnel Parameter Template [VPN] .....	222	[SSH Gateway] .....	365
Tunnel Probing [VPN] .....	214,	Use HTML Tag Removal [Mail Gateway] .....	250
[VPN] .....	216,	Use HTTP-Proxy [Anti-Virus] .....	368
[VPN] .....	222,	Use IP BARP Entries [Firewall] .....	184
[phion management centre] .....	467	Use IPsec dynamic IP [VPN] .....	208
Tunnel Timeout [VPN] .....	215,	Use Kernel Ruleset [Firewall] .....	128
[VPN] .....	216,	Use Linear Mode [Configuration Service] .....	102
[VPN] .....	222,	Use Local Box Time [Proxy] .....	329
[phion management centre] .....	467	Use Local Database [Proxy] .....	344
Tunnel TTL [Configuration Service] .....	79	Use Local Time [Proxy] .....	345,
Type [Firewall] .....	142,	[FTP Gateway] .....	354
[Firewall] .....	146,	Use local virus scanner [FTP Gateway] .....	353
[Firewall] .....	152,	Use Max. Tunnels [VPN] .....	231
[VPN] .....	206,	Use MSAD-groups with NTLM [Configuration Service] .....	112
[Eventing] .....	312,	Use NTP [Getting Started] .....	12
[DNS] .....	318,	Use ospf [VPN] .....	210
[OSPF and RIP] .....	490,	Use Policy Routing [Configuration Service] .....	79
[OSPF and RIP] .....	491	Use POP3 [Mail Gateway] .....	249
Type of Logfile [Configuration Service] .....	104	Use port 443 [VPN] .....	207
Type of Proxy [Configuration Service] .....	67	Use Provider DNS [Configuration Service] .....	72,
		[Configuration Service] .....	73,
		[Configuration Service] .....	75,
		[Configuration Service] .....	77
		Use Pyzor [Mail Gateway] .....	260
		Use Razor V2 [Mail Gateway] .....	260
		Use RCS [phion management centre] .....	414
		Use Reverse Address [Firewall] .....	159
		Use Self-Signed Certificate [VPN] .....	231,
		[Proxy] .....	338
		Use Service Names for Statistics [Firewall] .....	129
		Use Site to Site Tunnels for Authentication [VPN] .....	207
		Use Special Routing Table [OSPF and RIP] .....	485,
		[OSPF and RIP] .....	488
		Use Special Routing Tables [OSPF and RIP] .....	486
		Use SSL [Configuration Service] .....	112,
		[Configuration Service] .....	113,
		[VPN] .....	209
		Use SSL Encapsulation [Configuration Service] .....	117
		Use Table [Configuration Service] .....	79
		Use Target Address [Firewall] .....	159
		Use Template [VPN] .....	213
		Use Time Received [phion management centre] .....	449
		Use Tunnels for Authentication [phion management centre] .....	416
		Used by [VPN] .....	213
		Used Driver [Configuration Service] .....	64
		Used Root Certificates [VPN] .....	218
		Used Subnet [DHCP] .....	274
		Used VPN Protocol [Configuration Service] .....	67
		User [Firewall] .....	154,
		[VPN] .....	209,
		[Proxy] .....	326,
		[phion management centre] .....	472
		User Access ID [Configuration Service] .....	72,
		[Configuration Service] .....	73,
		[Configuration Service] .....	75,
		[Configuration Service] .....	77

## U

UDP Incoming Address [Proxy] .....	325
UDP Limit Exceeded [Firewall] .....	129
UDP Listen Port [DHCP] .....	273
UDP Outgoing Address [Proxy] .....	325
UDP Port [DHCP] .....	286,
[phion management centre] .....	448
UDP/Src Limit Exceeded [Firewall] .....	129
UMTS Enabled [Configuration Service] .....	76
UMTS Modem Card [Configuration Service] .....	76
Unattended Installation [Getting Started] .....	14
Unblock Update [phion management centre] .....	399
Undelivered Entries [Mail Gateway] .....	256
Unit [Configuration Service] .....	59
Unknown Clients [DHCP] .....	274
Unknown Downloads Template [Anti-Virus] .....	371
Unreachable Command [Configuration Service] .....	69
Unrestricted IPs [Proxy] .....	346,
[Proxy] .....	347
Unrestricted Users [Proxy] .....	346,
[Proxy] .....	347
Unstructured Address [Configuration Service] .....	59
Unstructured Name [Configuration Service] .....	59
Untrusted Update [phion management centre] .....	399
Update [Eventing] .....	312
Update Direction [OSPF and RIP] .....	488
Update every [phion management centre] .....	472
Update Every (min) [Anti-Virus] .....	368
Update Now [phion management centre] .....	399
Update Policy [Configuration Service] .....	102
Update Static Leases [DHCP] .....	277
Update Timer [OSPF and RIP] .....	488
Upload Unknown URLs [Proxy] .....	344



User Access Sub-ID [Configuration Service] ..... 72,  
 [Configuration Service] ..... 75  
 User Authentication [VPN] ..... 211,  
 [Proxy] ..... 330,  
 [Proxy] ..... 346  
 User Defined Rule Event [Mail Gateway] ..... 256  
 User Groups [Firewall] ..... 134,  
 [VPN] ..... 232  
 User ID [VPN] ..... 213,  
 [SSH Gateway] ..... 365,  
 [phion management centre] ..... 448  
 User Info Helper Scheme [Configuration Service] ..... 112,  
 [Configuration Service] ..... 113,  
 [Configuration Service] ..... 114  
 User List [Firewall] ..... 189,  
 [Proxy] ..... 328,  
 [FTP Gateway] ..... 354  
 User List Policy [Firewall] ..... 189,  
 [Proxy] ..... 328,  
 [FTP Gateway] ..... 354  
 User Name [Configuration Service] ..... 59  
 User Names [SSH Gateway] ..... 366  
 User Real-Time Check (OCSP) [Proxy] ..... 338  
 User specific [FTP Gateway] ..... 353  
 User Visible Name [SSH Gateway] ..... 366  
 Userlinks [VPN] ..... 234  
 Username [VPN] ..... 211,  
 [VPN] ..... 233,  
 [Anti-Virus] ..... 368  
 Username Length [FTP Gateway] ..... 353  
 Users [Proxy] ..... 330  
 Using Time Server [Control Centre] ..... 39

**V**

Validate Password [phion management centre] ..... 460  
 Value [VPN] ..... 219  
 Vendor [DHCP] ..... 276  
 Verbose [DHCP] ..... 283  
 Verbose Logging [Configuration Service] ..... 104,  
 [Configuration Service] ..... 111  
 Version Control System [phion management centre] ..... 473  
 View [SNMP] ..... 481  
 View as list [phion management centre] ..... 466  
 View Configuration [phion management centre] ..... 415  
 View License Data [phion management centre] ..... 414  
 View Rule Set [phion management centre] ..... 415  
 View Stripped Attachments [phion management centre] ..... 415  
 View Trace Output [phion management centre] ..... 415  
 Views [phion management centre] ..... 465  
 Virscan Service Permissions [phion management centre] ..... 415  
 Virtual Device [Configuration Service] ..... 87  
 Virtual IP (VIP) [Configuration Service] ..... 67  
 Virtual Link ID (ABR) [OSPF and RIP] ..... 487  
 Virtual Link Params [OSPF and RIP] ..... 487  
 Virus Protection [Mail Gateway] ..... 253  
 Visible Hostname [Proxy] ..... 325  
 Visible Interface Name [Configuration Service] ..... 63  
 Visible Name [VPN] ..... 232,  
 [VPN] ..... 233  
 VJ Connection-ID [Configuration Service] ..... 75  
 VJ TCP Header [Configuration Service] ..... 75  
 VLAN Description [Configuration Service] ..... 65  
 VLAN ID [Configuration Service] ..... 65  
 VPN Device Index [VPN] ..... 222,  
 [VPN] ..... 227  
 VPN Group [Firewall] ..... 190  
 VPN HW Modules [Firewall] ..... 128  
 VPN Interface [Configuration Service] ..... 67  
 VPN Local IP [Configuration Service] ..... 67  
 VPN Name [Firewall] ..... 190  
 VPN Point of Entry [Configuration Service] ..... 67  
 VPN Port [Configuration Service] ..... 67  
 VPN Rate Limit [Firewall] ..... 128  
 VPN Rules [VPN] ..... 214,  
 [VPN] ..... 216  
 VPN Server [Configuration Service] ..... 67  
 VPN Server Key [Configuration Service] ..... 67  
 VPN Server Permissions [phion management centre] ..... 415  
 VPN-Type [VPN] ..... 214

**W**

Waiting Period [Configuration Service] ..... 67  
 Waiting Period (s/probe) [Configuration Service] ..... 78

Warning Period [Configuration Service] ..... 91  
 Warning period before expiration [phion management centre] ..... 434  
 Watch Control Daemon [Configuration Service] ..... 111  
 Watch SSH Daemon [Configuration Service] ..... 111  
 Water is transparent [phion management centre] ..... 471  
 Web Resources [VPN] ..... 232  
 WEBDAV Address [VPN] ..... 233  
 WEBDAV Resources [VPN] ..... 232  
 WEBDAV Sharename [VPN] ..... 233  
 Weekday/Hour [Configuration Service] ..... 87  
 Weight [Firewall] ..... 146  
 Weight Number [Configuration Service] ..... 69  
 Welcome message [FTP Gateway] ..... 354  
 Went Operational [Configuration Service] ..... 53  
 When using BULK transports [VPN] ..... 225  
 When using QUALITY transports [VPN] ..... 225  
 White List [Proxy] ..... 345  
 White List Peers [Mail Gateway] ..... 254  
 White List Senders [Mail Gateway] ..... 254  
 Whitelist From [Mail Gateway] ..... 260  
 Whitelist To [Mail Gateway] ..... 260  
 Wild [phion management centre] ..... 399  
 Wildcard Support [Configuration Service] ..... 72,  
 [Configuration Service] ..... 73,  
 [Configuration Service] ..... 75,  
 [Configuration Service] ..... 77  
 Windows Domain Name [Proxy] ..... 327  
 WINS [VPN] ..... 214,  
 [VPN] ..... 217  
 WINS Server [Configuration Service] ..... 113,  
 [DHCP] ..... 276,  
 [DHCP] ..... 283  
 Workgroup Name [Configuration Service] ..... 112  
 World Texture from [phion management centre] ..... 471  
 Write [phion management centre] ..... 420  
 Write Cache-Log [Proxy] ..... 325  
 Write Store-Log [Proxy] ..... 325  
 Write USB stick [Getting Started] ..... 14  
 WWW root [Firewall] ..... 188

**X**

X509 Certificate [VPN] ..... 217  
 X509 Certificate & Login+Password Authentication [Firewall] ..... 190  
 X509 Certificate Authentication [Firewall] ..... 190  
 X509 Key Usage [Configuration Service] ..... 59  
 X509 Login Extraction Field [VPN] ..... 218  
 xDSL Enabled [Configuration Service] ..... 71  
 XML Services Management [phion management centre] ..... 415

**Y**

Yearly Schedule [Configuration Service] ..... 103  
 Your Level [phion management centre] ..... 420

**Z**

Zone Keys [DHCP] ..... 278  
 Zone Type [Configuration Service] ..... 56,  
 [DHCP] ..... 278  
 Zoom out/in [phion management centre] ..... 466

## 7. Table Directory

Table 0-1	Text conventions of the documentation .....	4
-----------	---	---

### 1 Getting Started

Table 1-1	USB stick - Formatting .....	10
Table 1-2	Types of DEMO versions in netfence 4.2 .....	11
Table 1-3	Availability of services on Appliance Models .....	16
Table 1-4	Contents of the Overview segment .....	18
Table 1-5	Comparison CIDR - phion notation .....	25

### 2 Control Centre

Table 2-1	Status icons flagging tabs in the Control window .....	28
Table 2-2	Connection status icons .....	28
Table 2-3	Server status and configuration .....	29
Table 2-4	Icons for network interface types .....	30
Table 2-5	Icons for network connection status .....	31
Table 2-6	Example: Route handling, networks .....	33
Table 2-7	Example: Route handling, corresponding direct route .....	33
Table 2-8	Example: Route handling, no Source IP address .....	33
Table 2-9	Example: Route handling, gateway routes .....	34
Table 2-10	Example: Route handling, valid source IP address .....	34
Table 2-11	Example configuration for router and firewall .....	35
Table 2-12	Router configuration .....	35
Table 2-13	Routing state on active firewall box .....	35
Table 2-14	Routing state on backup firewall box .....	35
Table 2-15	Routing state on both firewall boxes .....	35
Table 2-16	Routing state on both firewall box .....	35
Table 2-17	Tabular listing of the elements of the process status panel. ....	36
Table 2-18	Version Status - Properties .....	37
Table 2-19	Possible authentication options .....	39
Table 2-20	Box control - BOX SCEP Status - commands .....	40
Table 2-21	Session types overview .....	40

### 3 Configuration Service

Table 3-1	Required software modules sufficient for management and controlled low level operation of a box .....	44
Table 3-2	Lock indicator icons .....	45
Table 3-3	Box configuration window - icons .....	46
Table 3-4	Buttons of configuration window for session management and status retrieval .....	47
Table 3-5	Box specific configuration items .....	50
Table 3-6	Classification of the available sections .....	61
Table 3-7	NICs supporting VLAN technology .....	65
Table 3-8	phion routing rules .....	70
Table 3-9	Traffic Shaping Settings - Virtual Tree commands .....	85
Table 3-10	Traffic Shaping Settings - Interface commands .....	86
Table 3-11	Traffic Shaping Settings - Shaping connector commands .....	87
Table 3-12	Realtime Information - Shaping .....	87
Table 3-13	Realtime Information - Shaping commands .....	88
Table 3-14	Bandwidth calculation by ratio .....	89
Table 3-15	Bandwidth calculation by total percentage .....	89
Table 3-16	Example 1 - Policy Definition configuration .....	89
Table 3-17	Example 1 - Interfaces configuration .....	90
Table 3-18	Example 2 - Policy Definition configuration .....	90
Table 3-19	Example 2 - Interfaces configuration .....	90
Table 3-20	Authorisations associated with administrator roles .....	91
Table 3-21	Example - Box configuration .....	94
Table 3-22	Service configuration - Statistics dependent or independent from the statistics settings .....	98
Table 3-23	Overview of the five notification schemes on phion systems .....	105
Table 3-24	Overview of the checks watchdog runs .....	109
Table 3-25	Listing of the four available error handling policies offered by the repair utility of the watchdog module .....	109
Table 3-26	Error code to error origin assignment assumed by the repair utility .....	109

### 4 Firewall

Table 4-1	Firewall notions .....	125
Table 4-2	Audit events .....	130
Table 4-3	Rule marks utilised in the rule overview window .....	133
Table 4-4	Currently available modules .....	144
Table 4-5	Example Setup 1 - Rule configuration firewalls A and B .....	147
Table 4-6	Example Setup 2 - Rule configuration firewalls A and B .....	147



Table 4-7	Recommendation for creation of Proxy ARPs	150
Table 4-8	Forward policy comparison	159
Table 4-9	Rule Tester - Test Result icons	164
Table 4-10	Exemplary LAN scenario	165
Table 4-11	Exemplary rule configuration in comparison	167
Table 4-12	Improved rule configuration	168
Table 4-13	Status types and their origin	170
Table 4-14	Overview of possible access cache entries	172
Table 4-15	Reasons for connections denials	174
Table 4-16	Reasons for connection blocks	175
Table 4-17	Reasons for connection drops	175
Table 4-18	Reasons for connection failures	176
Table 4-19	Columns available in the upper section of the Dynamic Rules tab	176
Table 4-20	Columns available in the lower section of the Dynamic Rules tab	176
Table 4-21	Columns in the protected IPs tab	177
Table 4-22	Rule state overview	177
Table 4-23	Possible tracing conditions	178
Table 4-24	Bridging characteristics in comparison	181
Table 4-25	Structural breakdown of bridging units	182
Table 4-26	Overview of bridging operational information in the Bridging ARPs tab	187
Table 4-27	Broad-Multicast action type rule configuration	187
Table 4-28	Monitoring parameters overview	192
Table 4-29	RPC - comparison passive / active	193
Table 4-30	Monitoring parameters overview	198

## 5 VPN

Table 5-1	Client - Server communication options	200
Table 5-2	Comparison of different tunnel transport modes	203
Table 5-3	VPN configuration - Introduce and Configure	205
Table 5-4	Involved objects within a phion VPN framework	220
Table 5-5	Example for TI Learning Policy	225
Table 5-6	Possible "last connection" states	230
Table 5-7	SSL tunnels	235
Table 5-8	Fully Transparent Tunnel - VPN Configuration on VPN server 1	238
Table 5-9	Fully Transparent Tunnel - VPN configuration on VPN server 2	238
Table 5-10	Stealth Tunnel - VPN Configuration on VPN server 1	238
Table 5-11	Stealth Tunnel - VPN configuration on VPN server 2	238
Table 5-12	Relationship between Local and Partner networks	239
Table 5-13	Redundant VPN tunnel - Example	240
Table 5-14	Redundant VPN tunnel - Example parameter settings	240
Table 5-15	Redundant VPN tunnel - Direct Routes for VPN server 1	240
Table 5-16	Redundant VPN tunnel - Direct Routes for VPN server 2	240

## 6 Mail Gateway

Table 6-1	Items of the Navigations Bar's main element "Configuration"	246
Table 6-2	E-mail client configuration	249
Table 6-3	SMTP levels	251
Table 6-4	Variables used in the Expert Settings section	251
Table 6-5	Operators used in the Expert Settings section	251
Table 6-6	IF statements used in the Expert Settings section	251
Table 6-7	Actions used in the Expert Settings section	252

## 7 DHCP

Table 7-1	Example - Configuration parameters for Subnet1	280
Table 7-2	Example - Configuring Address Pool 1 for Subnet1	280
Table 7-3	Example - Configuring Address Pool 2 for Subnet1	280
Table 7-4	Example - Configuration parameters for Subnet2	281
Table 7-5	Example - Configuring Address Pool 1 for Subnet2	281
Table 7-6	Example - Configuration parameters for Known Clients 1	281
Table 7-7	Example - Configuration parameters for Known Clients 2	281

## 8 Log Viewer

Table 8-1	Navigation arrows and their function	291
Table 8-2	Log Entry types	292
Table 8-3	Event Log Message - Attributes	292
Table 8-4	Event Log Message- ID and text	292
Table 8-5	Log file entries related to clock skew detection	293
Table 8-6	Log file entries related to synchronisation of polling list and database	293
Table 8-7	Log file entries related to synchronisation of polling list and database	293
Table 8-8	Log file entries related to synchronisation between HA-databases - Scenarios which will stop task MAIN	293

Table 8-9	Log file entries related to synchronisation between HA-databases - Scenarios which will not stop task MAIN .....	294
-----------	--	-----

## 9 Statistics

Table 9-1	Services responsible for statistics files handling .....	296
-----------	--	-----

## 10 Eventing

Table 10-1	Overview of events in the Events tab .....	307
Table 10-2	Font styles characterising event settings .....	307
Table 10-3	SNMP Parameters .....	310
Table 10-4	SNMP notifications .....	311

## 11 DNS

Table 11-1	Supplementary DNS configuration objects overview .....	322
------------	--	-----

## 12 Proxy

Table 12-1	Short overview of metacharacters in regular expressions .....	329
Table 12-2	Actions configuration .....	334
Table 12-3	Example: squid.conf file - httpd_accel directive .....	336
Table 12-4	Example: squid.conf file - corresponding options .....	336
Table 12-5	URL categories overview .....	348

## 13 FTP Gateway

## 14 Voice over IP

Table 14-1	SIP Monitoring parameters overview .....	362
------------	--	-----

## 15 SSH Gateway

## 16 Anti-Virus

## 17 High Availability

Table 17-1	State table with working communication .....	376
Table 17-2	Communication between HA partners; ARPs are independent from a HA system. ....	376
Table 17-3	Designing a HA System - Used IP addresses .....	379
Table 17-4	Designing a HA system - Translated HA IP .....	379
Table 17-5	Designing a HA system - network routes .....	379

## 18 phion management centre

Table 18-1	management centre services overview .....	389
Table 18-2	Possible settings of authentication levels on the box itself .....	392
Table 18-3	Example - Log file of a System Startup .....	393
Table 18-4	Colour coding of status icons .....	397
Table 18-5	Icons used in the title bars of range, cluster and box section .....	397
Table 18-6	Icons used in the Configuration Updates tab .....	399
Table 18-7	Update Status flags overview .....	399
Table 18-8	Session types overview .....	400
Table 18-9	Data listed in the Floating Licenses tab .....	400
Table 18-10	Data listed in the Stat Collect tab .....	401
Table 18-11	Data listed in the Box Execution tab .....	402
Table 18-12	Popular Scripts .....	405
Table 18-13	Data listed in the columns of the Scanner Versions tab .....	405
Table 18-14	Data listed in the system list of the Software Update tab .....	405
Table 18-15	Data listed in the task list of the Software Update tab .....	408
Table 18-16	Moving/Copying Managed Boxes, Servers and Services .....	424
Table 18-17	Default user rights overview .....	432
Table 18-18	Administration scopes overview .....	433
Table 18-19	Error analysis of poll sessions .....	442
Table 18-20	Filtering policy - MC-managed box .....	453
Table 18-21	Filtering policy - self-managed box .....	453
Table 18-22	Definition of V3 Extensions (RFC 3280) .....	463
Table 18-23	VPN world - Hotkey .....	472
Table 18-24	VPN world - Mouse functions .....	472
Table 18-25	VPN world - Colour legend for box .....	472
Table 18-26	VPN world - Colour legend for tunnel .....	472
Table 18-27	Columns available in the RCS Versions window .....	474
Table 18-28	Columns available in the RCS Report window .....	475

**19 SNMP**

**20 OSPF and RIP**

Table 20-1	Feature differences between OSPF and RIP .....	485
Table 20-2	Example for IP Prefix List Filter - prefix list .....	491
Table 20-3	Example for IP Prefix List Filter - group of prefixes .....	491
Table 20-4	Configuration example .....	491

**21 Licensing**

Table 21-1	Host key examples .....	500
Table 21-2	Important phion specifics in a node-locked license for a self-managed gateway .....	501
Table 21-3	Important phion specifics in a node-locked box license for a management centre .....	501
Table 21-4	Important phion specifics in a node-locked master license for a management centre .....	501
Table 21-5	Important phion specifics in a pool license issued for multiple MC-administered boxes .....	502
Table 21-6	Important phion specifics in a VPN pool license .....	502
Table 21-7	Licence centre - required information .....	506
Table 21-8	Classification of incoming and outgoing interfaces .....	510

**22 System Information**

Table 22-1	Basic overview of the phion Linux system and its licensing concepts. ....	512
Table 22-2	Ports overview .....	515
Table 22-3	Layer-IDs overview .....	516
Table 22-4	Class-IDs overview .....	516
Table 22-5	Operational Events overview .....	517
Table 22-6	Security Events overview .....	519

**23 Appendix**

Table 23-1	netfence industrial - Box Services > Firewall Settings .....	530
Table 23-2	netfence industrial - Box > Tuning .....	530
Table 23-3	netfence industrial - Box Services > Statistics .....	530
Table 23-4	netfence industrial - Box Misc > Watchdog .....	530
Table 23-5	netfence industrial - Box > Network .....	530
Table 23-6	netfence industrial - Box > Settings .....	530
Table 23-7	netfence industrial - Box > Bootloader .....	530
Table 23-8	netfence integra XS - Box Services > Firewall Settings .....	531
Table 23-9	netfence integra XS - Box > Tuning .....	531
Table 23-10	netfence integra XS - Box Services > Statistics .....	531
Table 23-11	netfence integra XS - Box Misc > Watchdog .....	531
Table 23-12	netfence integra S - Box Services > Firewall Settings .....	531
Table 23-13	netfence integra S - Box > Tuning .....	531
Table 23-14	netfence integra S - Box Services > Statistics .....	531
Table 23-15	netfence integra S - Box Misc > Watchdog .....	531
Table 23-16	netfence M5 - Box Services > Statistics .....	532
Table 23-17	netfence M5 - Box > Tuning .....	532
Table 23-18	netfence M5 - Box Services > Statistics .....	532
Table 23-19	netfence M5 - Box Misc > Watchdog .....	532
Table 23-20	netfence M3 - Box Services > Firewall Settings .....	532
Table 23-21	netfence M3 - Box > Tuning .....	532
Table 23-22	netfence M3 - Box Services > Statistics .....	532
Table 23-23	netfence M3 - Box Misc > Watchdog .....	532
Table 23-24	netfence M1 - Box Services > Firewall Settings .....	533
Table 23-25	netfence M1 - Box > Tuning .....	533
Table 23-26	netfence M1 - Box Services > Statistics .....	533
Table 23-27	netfence M1 - Box Misc > Watchdog .....	533
Table 23-28	phion MR - Box Services > Firewall Settings .....	533
Table 23-29	phion MR - Box > Tuning .....	533
Table 23-30	phion MR - Box Services > Statistics .....	533
Table 23-31	phion MR - Box Misc > Watchdog .....	533
Table 23-32	phion M5 - Box Services > Statistics .....	534
Table 23-33	phion M5 - Box > Tuning .....	534
Table 23-34	phion M5 - Box Services > Statistics .....	534
Table 23-35	phion M5 - Box Misc > Watchdog .....	534
Table 23-36	phion M3 - Box Services > Firewall Settings .....	534
Table 23-37	phion M3 - Box > Tuning .....	534
Table 23-38	phion M3 - Box Services > Statistics .....	534
Table 23-39	phion M3 - Box Misc > Watchdog .....	534
Table 23-40	phion M1 - Box Services > Firewall Settings .....	535
Table 23-41	phion M1 - Box > Tuning .....	535
Table 23-42	phion M1 - Box Services > Statistics .....	535
Table 23-43	phion M1 - Box Misc > Watchdog .....	535

Table 23-44	netfence sectorwall - Box Services > Firewall Settings	535
Table 23-45	netfence sectorwall - Box > Tuning	535
Table 23-46	netfence sectorwall - Box Services > Statistics	535
Table 23-47	netfence sectorwall - Box Misc > Watchdog	535
Table 23-48	netfence contegrity - Box Services > Firewall Settings	536
Table 23-49	netfence contegrity - Box > Tuning	536
Table 23-50	netfence contegrity - Box Services > Statistics	536
Table 23-51	netfence contegrity - Box Misc > Watchdog	536
Table 23-52	netfence standard - Box > Network	536
Table 23-53	netfence standard - Box > Settings	536
Table 23-54	netfence standard - Box > Bootloader	536
Table 23-55	nf-850 - Box > Network	537
Table 23-56	nf-850 - Box > Settings	537
Table 23-57	nf-850 - Box > Bootloader	537
Table 23-58	nf-780 - Box > Network	537
Table 23-59	nf-780 - Box > Settings	537
Table 23-60	nf-780 - Box > Bootloader	537
Table 23-61	nf-431 - Box > Network	538
Table 23-62	nf-431 - Box > Settings	538
Table 23-63	nf-431 - Box > Bootloader	538
Table 23-64	nf-421 - Box > Network	538
Table 23-65	nf-421 - Box > Settings	538
Table 23-66	nf-421 - Box > Bootloader	538
Table 23-67	nf-420 - Box > Network	539
Table 23-68	nf-420 - Box > Settings	539
Table 23-69	nf-420 - Box > Bootloader	539
Table 23-70	nf-240 - Box > Network	539
Table 23-71	nf-240 - Box > Settings	539
Table 23-72	nf-240 - Box > Bootloader	539
Table 23-73	nf-180 - Box > Network	540
Table 23-74	nf-180 - Box > Settings	540
Table 23-75	nf-180 - Box > Bootloader	540
Table 23-76	S5 - Box > Network	540
Table 23-77	S5 - Box > Settings	540
Table 23-78	S5 - Box > Bootloader	540
Table 23-79	S6 - Box > Network	541
Table 23-80	S6 - Box > Settings	541
Table 23-81	S6 - Box > Tuning	541
Table 23-82	S6 - Box Services > Statistics	541
Table 23-83	S6 - Box > Bootloader	541
Table 23-84	S25 - Box > Network	541
Table 23-85	S25 - Box > Settings	541
Table 23-86	S25 - Box > Bootloader	541
Table 23-87	S20 - Box > Network	542
Table 23-88	S20 - Box > Settings	542
Table 23-89	S20 - Box > Bootloader	542
Table 23-90	S16 - Box > Network	542
Table 23-91	S16 - Box > Settings	542
Table 23-92	S16 - Box > Bootloader	542
Table 23-93	S16 - Box Services > Statistics	542
Table 23-94	S15 - Box > Network	543
Table 23-95	S15 - Box > Settings	543
Table 23-96	S15 - Box > Bootloader	543
Table 23-97	S10 - Box > Network	543
Table 23-98	S10 - Box > Settings	543
Table 23-99	S10 - Box > Bootloader	543
Table 23-100	M50 - Box > Network	544
Table 23-101	M50 - Box > Settings	544
Table 23-102	M50 - Box > Bootloader	544
Table 23-103	M50 - Box Services > Statistics	544
Table 23-104	M300 - Box > Network	544
Table 23-105	M300 - Box > Settings	544
Table 23-106	M300 - Box > Bootloader	544
Table 23-107	M300a - Box > Network	545
Table 23-108	M300a - Box > Settings	545
Table 23-109	M300a - Box > Bootloader	545
Table 23-110	M3000 - Box > Network	545
Table 23-111	M3000 - Box > Settings	545
Table 23-112	M3000 - Box > Bootloader	545
Table 23-113	M200 - Box > Network	546
Table 23-114	M200 - Box > Settings	546
Table 23-115	M200 - Box > Bootloader	546
Table 23-116	M200a - Box > Network	546
Table 23-117	M200a - Box > Settings	546

Table 23-118	M200a - Box > Bootloader .....	546
Table 23-119	M2000 - Box > Network .....	547
Table 23-120	M2000 - Box > Settings .....	547
Table 23-121	M2000 - Box > Bootloader .....	547
Table 23-122	M100 - Box > Network .....	547
Table 23-123	M100 - Box > Settings .....	547
Table 23-124	M100 - Box > Bootloader .....	547
Table 23-125	M100a - Box > Network .....	548
Table 23-126	M100a - Box > Settings .....	548
Table 23-127	M100a - Box > Bootloader .....	548
Table 23-128	M1000 - Box > Network .....	548
Table 23-129	M1000 - Box > Settings .....	548
Table 23-130	M1000 - Box > Bootloader .....	548
Table 23-131	L2000 - Box > Network .....	549
Table 23-132	L2000 - Box > Settings .....	549
Table 23-133	L2000 - Box > Bootloader .....	549
Table 23-134	L1000 - Box > Network .....	549
Table 23-135	L1000 - Box > Settings .....	549
Table 23-136	L1000 - Box > Bootloader .....	549
Table 23-137	Glossary - A .....	598
Table 23-138	Glossary - C .....	598
Table 23-139	Glossary - D .....	598
Table 23-140	Glossary - E .....	599
Table 23-141	Glossary - F .....	599
Table 23-142	Glossary - G .....	599
Table 23-143	Glossary - H .....	599
Table 23-144	Glossary - I .....	599
Table 23-145	Glossary - K .....	600
Table 23-146	Glossary - L .....	600
Table 23-147	Glossary - M .....	600
Table 23-148	Glossary - N .....	600
Table 23-149	Glossary - O .....	600
Table 23-150	Glossary - P .....	600
Table 23-151	Glossary - R .....	601
Table 23-152	Glossary - S .....	602
Table 23-153	Glossary - T .....	602
Table 23-154	Glossary - U .....	602
Table 23-155	Glossary - V .....	602
Table 23-156	Glossary - W .....	602
Table 23-157	Conditions of Licensing of software which is used in phion netfence .....	608
Table 23-158	Software package listing and licenses .....	622

## 8. Figure Directory

Figure 0-1	Example: Common Settings .....	4
Figure 0-2	Example - section Condition .....	5

### 1 Getting Started

Figure 1-1	Window Box Licenses in read/write mode .....	9
Figure 1-2	Defining Box Type Settings with phion.i .....	11
Figure 1-3	Configuring System Settings with phion.i .....	11
Figure 1-4	Configuring Partition Settings with phion.i .....	12
Figure 1-5	NIC adapter configuration parameters .....	13
Figure 1-6	Configuring USB stick settings with phion.i .....	14
Figure 1-7	Box Type Settings window in Create Kickstart only mode .....	15
Figure 1-8	rawwritewin.exe - Start screen .....	15
Figure 1-9	Login dialogue .....	17
Figure 1-10	phion.a User Interface .....	17
Figure 1-11	Start screen .....	18
Figure 1-12	Dialogue for customising the tool bar .....	19
Figure 1-13	Tool bar .....	20
Figure 1-14	Status bar .....	20
Figure 1-15	phion.a Settings - Boxes .....	21
Figure 1-16	Enter New Box dialogue .....	21
Figure 1-17	phion.a Settings - Client tab .....	22
Figure 1-18	Configuring Advanced Cryptographic Settings .....	23
Figure 1-19	phion.a Settings - Public Host Keys tab .....	24

### 2 Control Centre

Figure 2-1	Tabs in the Control window flagged by status icons .....	28
Figure 2-2	Server Tab .....	29
Figure 2-3	Network Tab .....	30
Figure 2-4	Interface/IPs Tab .....	30
Figure 2-5	Table section .....	32
Figure 2-6	Network diagram illustrating the concept of a pending route .....	33
Figure 2-7	Network diagram, pending direct routes and gateway routes .....	34
Figure 2-8	Example for a screened host setup .....	34
Figure 2-9	Sample process status view .....	36
Figure 2-10	Sample Info Dialogue window .....	36
Figure 2-11	Sample Resources tab .....	37
Figure 2-12	Box Control > Licenses Tab .....	37
Figure 2-13	Network Activation dialogue .....	38
Figure 2-14	View of the box control window .....	38
Figure 2-15	Box Domain Registration dialogue .....	39
Figure 2-16	Typical view of the CPU information panel .....	40

### 3 Configuration Service

Figure 3-1	Interdependencies of the various basic configuration entities .....	43
Figure 3-2	Box configuration window in compressed connection state .....	44
Figure 3-3	Menu after pressing right mouse button on yet unlocked item .....	45
Figure 3-4	Menu after pressing right mouse button on locked item from another session .....	45
Figure 3-5	Configuration Sessions window .....	45
Figure 3-6	Box configuration window - detail .....	45
Figure 3-7	User Interface .....	48
Figure 3-8	Config tree - Emergency Override .....	48
Figure 3-9	Example for an Edit ... / Insert ... / Delete mask .....	48
Figure 3-10	Change / Insert ... / Delete mask .....	49
Figure 3-11	phion.a Configuration list and part of Clipboard content after Copy to Clipboard .....	49
Figure 3-12	Part of Clipboard content and phion.a Configuration list after Merge with Clipboard .....	49
Figure 3-13	Structure of the config tree .....	50
Figure 3-14	Creating a box on an MC .....	52
Figure 3-15	Box config file on an MC-administered box .....	53
Figure 3-16	Administrative Settings - System Access .....	54
Figure 3-17	Administrative Settings - DNS .....	55
Figure 3-18	Administrative Settings - TIME/NTP .....	56
Figure 3-19	Administrative Settings - SMS Control .....	57
Figure 3-20	Administrative Settings - SCEP .....	58
Figure 3-21	Box Identity .....	60
Figure 3-22	Certificate window .....	60
Figure 3-23	Output of a certificate at the command line interface .....	61
Figure 3-24	Box Network configuration .....	61
Figure 3-25	Additional Local Networks configuration .....	62
Figure 3-26	Virtual LAN configuration .....	65
Figure 3-27	Direct route configuration for Virtual LAN .....	66
Figure 3-28	Main Routing configuration .....	69
Figure 3-29	Policy Routing configuration .....	70
Figure 3-30	xDSL/ISDN/DHCP configuration .....	70
Figure 3-31	IP Tunnels configuration .....	79
Figure 3-32	Special Needs configuration .....	80



Figure 3-33	Process list output for a link bundle .....	81
Figure 3-34	Listing of /var/phion/run/boxnet/xDSL .....	81
Figure 3-35	Listing of /var/phion/config/boxnet/xDSL .....	81
Figure 3-36	Enterprise Shaping - Enforcement .....	82
Figure 3-37	Enterprise Shaping - Firewall Rule Parameter .....	83
Figure 3-38	Enterprise Shaping - Example 1: Simple traffic prioritisation .....	83
Figure 3-39	Enterprise Shaping - Example 2: ISP customer bandwidth assignment .....	84
Figure 3-40	Enterprise Shaping - Example 3: Advanced traffic shaping .....	84
Figure 3-41	Traffic Shaping Settings - Virtual Shaping Trees .....	85
Figure 3-42	Traffic Shaping Settings - dialogue box Virtual Device .....	85
Figure 3-43	Traffic Shaping Settings - dialogue box, new virtual interface .....	86
Figure 3-44	Traffic Shaping Settings - dialogue box Device/Tunnel Tree Mapping .....	86
Figure 3-45	Traffic Shaping Settings - dialogue box TINA Tunnel .....	86
Figure 3-46	Traffic Shaping Settings - Shaping Connectors .....	87
Figure 3-47	Traffic Shaping Settings - dialogue box Shape connector .....	87
Figure 3-48	Traffic Shaping Settings - dialogue box Shape Connector Rule .....	87
Figure 3-49	Realtime Information - Shaping .....	87
Figure 3-50	Config Section - Traffic Shaping .....	88
Figure 3-51	Traffic Shaping scenario 1 - Bandwidth configuration for inbound and outbound connections .....	89
Figure 3-52	Traffic Shaping scenario 2 - Prioritisation of applications .....	90
Figure 3-53	License Configuration .....	93
Figure 3-54	Context-menu of the Servers directory .....	94
Figure 3-55	Server configuration (single box) - General .....	95
Figure 3-56	Context menu of the Services directory .....	97
Figure 3-57	Service directory .....	98
Figure 3-58	Example: condensed excerpt from Paul Vixie's man page on crontab .....	103
Figure 3-59	Log Cycling - section File Specific Settings .....	104
Figure 3-60	Configuration Dialogue - Messages .....	105
Figure 3-61	Various configuration instances the phion notification model relies upon .....	105
Figure 3-62	Configuration Dialogue - Access Notification .....	106
Figure 3-63	Configuration Dialogue - Software update .....	108
Figure 3-64	Scheme for external authentication provided by the phion infrastructure daemon .....	111
Figure 3-65	Configuration Dialogue - MSAD Authentication .....	111
Figure 3-66	Configuration Dialogue - Radius .....	114
Figure 3-67	Configuration Dialogue - RSA SECURID .....	114
Figure 3-68	Configuration Dialogue - MSNT .....	114
Figure 3-69	Configuration Dialogue - OCSP .....	115
Figure 3-70	Infrastructure Services - Syslog Streaming - Logdata Filters - section Top Level Logdata .....	116
Figure 3-71	Creating a PAR file .....	119
Figure 3-72	Way of supplying a box with a repository .....	121
Figure 3-73	Show History window .....	121

## 4 Firewall

Figure 4-1	Basic connection diagram describing the notions used throughout the netfence firewall engine .....	125
Figure 4-2	Tree locations of the general firewall settings .....	126
Figure 4-3	Config Section - Eventing Settings .....	129
Figure 4-4	Connection Tracing configuration .....	131
Figure 4-5	Config Section - Firewall Forwarding Settings - Firewall .....	131
Figure 4-6	Schematic of terms involved in establishing a network connection through a phion firewall .....	132
Figure 4-7	Rule set configuration interface .....	134
Figure 4-8	Open navigation bar .....	134
Figure 4-9	New Rule dialogue .....	135
Figure 4-10	Time Object configuration dialogue .....	139
Figure 4-11	Creating/editing a net object called allwebservers .....	140
Figure 4-12	Firewall - Networks window - Listing of Network Objects .....	141
Figure 4-13	Network Object - Type Hostname (DNS Resolved) .....	142
Figure 4-14	Hostname Network Object configuration example .....	142
Figure 4-15	Part of the predefined services for the phion firewall .....	143
Figure 4-16	Service objects TCP-ALL and FTP .....	143
Figure 4-17	Parameter section for TCP and UDP .....	144
Figure 4-18	Connection situation for a UDP connection of tftp kind .....	145
Figure 4-19	Connection situation for a SQL client connecting to an Oracle server .....	145
Figure 4-20	Standard Connections - Edit / Create a Connection Object .....	145
Figure 4-21	Standard Connections - Example Setup 1 .....	147
Figure 4-22	Standard Connections - Example Setup 2 .....	147
Figure 4-23	Simple redundancy through next hop detection .....	148
Figure 4-24	Handling of assisted multipath routing .....	148
Figure 4-25	Configuration example for Source Address Cycling .....	148
Figure 4-26	Configuration example for multipath routing (Packet Load Balancing is set to 'No') .....	149
Figure 4-27	Configuration example for ACPF Assisted Multipath routing (Packet Load Balancing is set to 'Yes') .....	149
Figure 4-28	Address Translation Map configuration .....	149
Figure 4-30	Create a Proxy ARP Object dialogue .....	151
Figure 4-29	Proxy ARPs tab of the firewall configuration window .....	151
Figure 4-31	Firewall - Content Filter window .....	152
Figure 4-32	Creating/editing filter a pattern .....	152
Figure 4-33	Creating/editing filter a pattern .....	152
Figure 4-34	Creating/Editing Filter Groups .....	153
Figure 4-35	Assigning P2P-detection .....	153
Figure 4-36	Advanced Rule Parameters .....	154
Figure 4-37	Advanced Rule Parameters - Multiple Rules Editing .....	156

Figure 4-38	Time restriction dialogue	156
Figure 4-39	Building up a connection with outbound accept policy	157
Figure 4-41	Building up a connection with inbound accept policy	158
Figure 4-42	Simple SYN flooding attack with faked IP addresses on a firewall with inbound accept policy	158
Figure 4-40	Simple SYN flooding attack with faked IP addresses on a firewall with outbound accept policy	158
Figure 4-43	Forward Policy	158
Figure 4-44	Reverse Policy	158
Figure 4-45	Forward / Reverse / Target Address	158
Figure 4-46	ICMP Handling parameters	158
Figure 4-47	ICMP Handling - Example	159
Figure 4-48	Change Dynamic Rule dialogue	159
Figure 4-49	Warning dialogue when trying to delete a referenced object	160
Figure 4-50	Cascading of rules	161
Figure 4-51	Rule for cascading into a rule-sublist	161
Figure 4-52	Local rules	162
Figure 4-53	Local Rule scheme	162
Figure 4-54	Example for overlapping rules	163
Figure 4-55	Rule tester window with all information of consequences of the matching rule	163
Figure 4-56	Example for firewall configuration	165
Figure 4-57	Network situation for a typical LAN to Internet connection	165
Figure 4-58	Network situation for a ftp connection to our FTP server	166
Figure 4-59	Network situation for a ftp connection from our FTP server to another FTP server	166
Figure 4-60	Network situation for a secure connection to the webmail server	166
Figure 4-61	Network situation for a client connection to our webserver farm	166
Figure 4-62	Network situation for remote web server support	166
Figure 4-63	Network situation for sending a mail to the mail server	166
Figure 4-64	Rule for redirection of mail traffic to internal mailserver	166
Figure 4-65	Rule which implements load balancing for the web server farm	167
Figure 4-66	Rule which maps the ftp server to the internet	167
Figure 4-67	Rule for LAN access to the whole world	167
Figure 4-68	Network situation for a typical LAN to Internet connection	168
Figure 4-69	Connection object dialogue window for translation map	168
Figure 4-70	Rule dialogue for the news access rule via explicit source NAT	168
Figure 4-71	Status tab	169
Figure 4-72	Traffic meter	172
Figure 4-73	Access Cache	173
Figure 4-74	Flat network structure before segmentation	180
Figure 4-75	Network segmentation in a Transparent Layer2 bridged environment	180
Figure 4-76	Network segmentation in a Routed Transparent Layer2 bridged environment	181
Figure 4-77	Flat network structure	181
Figure 4-78	Non Transparent Translational Bridging	181
Figure 4-79	Destination MAC spoofing prevention	182
Figure 4-80	Configuration of Transparent Layer2 Bridging	184
Figure 4-81	Bridging Group Setup for Transparent Layer2 Bridging	185
Figure 4-82	Configuration of Transparent Layer2 Bridging	185
Figure 4-83	Bridging Group Setup for Routed Transparent Layer2 Bridging - Example 1	185
Figure 4-84	Configuration of Routed Transparent Layer2 Bridging	185
Figure 4-85	Bridging Group Setup for Routed Transparent Layer2 Bridging	186
Figure 4-86	Configuration of Non Transparent Translational Bridging	186
Figure 4-87	Net Object creation for LAN2 PC	186
Figure 4-88	Bridging Parameters configuration	186
Figure 4-89	Proxy ARP Object - Bridging Parent Network	187
Figure 4-90	Proxy ARP Object - Bridging Host Proxy ARP	187
Figure 4-91	Firewall > Dynamic > Bridging ARPs tab	187
Figure 4-92	Utilising action type Broad-Multicast for Bridging Groups	187
Figure 4-93	Connection buildup using inline authentication	188
Figure 4-94	Connection buildup using offline authentication	188
Figure 4-95	Configuration dialogues - User Object & User Condition	189
Figure 4-96	fwauthd redirection rule	191
Figure 4-97	fwauthd user authentication rule	191
Figure 4-98	Firewall Authentication login screen	191
Figure 4-99	Firewall Authentication succeeded login screen	191
Figure 4-100	General <i>Service Object</i> needed for creating a pass rule to enable passive ONCRPC	193
Figure 4-101	Service Object needed for enabling nfs usage via a portmapper	194
Figure 4-102	RPC Server information configuration dialogue	194
Figure 4-103	General <i>Service Object</i> needed for creating a pass rule to enable active ONCRPC	194
Figure 4-104	<i>Service Object</i> needed for enabling nfs usage via a portmapper	195
Figure 4-105	General <i>Service Object</i> needed for creating a pass rule to enable active&passive ONCRPC	195
Figure 4-106	<i>Service Object</i> needed for enabling nfs usage via a portmapper	195
Figure 4-107	General <i>Service Object</i> needed for creating a pass rule to enable passive DCERPC	196
Figure 4-108	Service Object needed for enabling MS-File Replication Service usage via an end point mapper	197
Figure 4-109	General <i>Service Object</i> needed for creating a pass rule to enable active DCERPC	197

## 5 VPN

Figure 5-1	General scheme of remote access VPN	200
Figure 5-2	Remote Access with the client placed behind a firewall	200
Figure 5-3	Remote Access with the client using a proxy or SOCKS server for routing assistance	201
Figure 5-4	Two corporate networks linked together via VPN tunnel	201
Figure 5-5	Example for a VPN constellation	202
Figure 5-6	Data scheme for VPN groups	202

Figure 5-7	ESP and NoHash	204
Figure 5-8	VPN configuration block diagram	205
Figure 5-9	VPN configuration - Introduce and Configure block diagram	205
Figure 5-10	VPN configuration block diagram - Configure VPN server	206
Figure 5-11	Personal Network configuration dialogue	206
Figure 5-12	VPN configuration with Routed Network (Static Route; virtual network/DMZ)	206
Figure 5-13	VPN configuration with Local (Proxy ARP)	206
Figure 5-14	Server Certificates configuration	207
Figure 5-15	Certificate Revocation tab	208
Figure 5-16	Server certificates with open context menu	209
Figure 5-17	Configuration Dialogue for L2TP	211
Figure 5-18	Configuration Dialogue for Chap Secrets	211
Figure 5-19	VPN configuration block diagram - Configure phion Personal VPN	212
Figure 5-20	Heredity of phion certificates	212
Figure 5-21	Pool License Certificate	212
Figure 5-22	Pool License in plain text format	213
Figure 5-23	Edit personal license information	213
Figure 5-24	Template configuration	214
Figure 5-25	VPN configuration block diagram - Configure Group VPN	215
Figure 5-26	New phion client policy	216
Figure 5-27	New common - Common Settings	216
Figure 5-28	Configuration dialogue - New policy	217
Figure 5-29	Change Group Match Settings	217
Figure 5-30	Preauthentication Details	218
Figure 5-31	Configuration dialogue - Group Policy Condition	218
Figure 5-32	Certificate Conditions configuration	219
Figure 5-33	Configuration dialogue for registry rules	219
Figure 5-34	VPN configuration block diagram - Configure VPN tunnel	220
Figure 5-35	Scheme with the basic notations of VPN tunnelling	220
Figure 5-36	Tunnel configuration	221
Figure 5-37	Traffic Intelligence (TI)	223
Figure 5-38	Transport Selection Policy	223
Figure 5-39	TINA Tunnel with multiple transport modes added	224
Figure 5-40	TI Learning Policy scheme	225
Figure 5-41	IPSec Tunnel configuration - Base configuration tab	227
Figure 5-42	IPSec Tunnel configuration - Authentication tab	228
Figure 5-43	Upload dialogue	230
Figure 5-44	Java runtime version query	236
Figure 5-45	Fully Transparent Tunnel	238
Figure 5-46	Stealth Tunnel	238
Figure 5-47	Star-shaped topology with one HQ and two outposts	239
Figure 5-48	Configuring redundant VPN tunnels - example environment	240

## 6 Mail Gateway

Figure 6-1	MailGW Settings configuration area	246
Figure 6-2	Mail gateway positioning in a network	246
Figure 6-3	POP3 scanning example setup	249
Figure 6-4	Blacklist configuration	254
Figure 6-5	Overview: Spam filtering process	257
Figure 6-6	Header of an e-mail identified as spam	257
Figure 6-7	Flowchart - Spam filter client	258
Figure 6-8	Spam Analysis configuration	259
Figure 6-9	Flowchart - Spam filter Server	259
Figure 6-10	Spam filter configuration dialogue	260
Figure 6-11	Example script for e-mail collection	262
Figure 6-12	Filter settings	263
Figure 6-13	Statistics tree	268

## 7 DHCP

Figure 7-1	Processes structure	272
Figure 7-2	DHCP Enterprise Configuration - Operational Setup	273
Figure 7-3	DHCP Enterprise Configuration - Address Pools	273
Figure 7-4	DHCP Enterprise Configuration - Known Clients	275
Figure 7-5	DHCP Enterprise - Dynamic DNS	278
Figure 7-6	Real Time Information - DHCP	279
Figure 7-7	Example environment	280
Figure 7-8	Example - Configuring CLASS Settings	280
Figure 7-9	Example - Configuring Subnet settings for Subnet1	280
Figure 7-10	DHCP Server Settings with pre-configured settings	282
Figure 7-11	Configuration - IP RANGES	283
Figure 7-12	Configuration - SPECIAL CLIENTS	283
Figure 7-13	Configuration - BASIC OPTIONS	283
Figure 7-14	Real Time Information - DHCP	284
Figure 7-15	Example of use for a DHCP Relay Agent	286
Figure 7-16	DHCP Relay Settings	286
Figure 7-17	Cascading DHCP Relay with interfaces to be configured	287

## 8 Log Viewer

Figure 8-1	LogGUI .....	290
Figure 8-2	Navigation section of the LogGUI .....	291
Figure 8-3	Log Sequence Number in Relation to System Time .....	292

## 9 Statistics

Figure 9-1	Statistics user interface .....	296
Figure 9-2	Tree structure of the Statistics module .....	296
Figure 9-3	Control field for type Curve with time axis .....	297
Figure 9-4	Curve type .....	298
Figure 9-5	Time Interval selection .....	298
Figure 9-6	Bar type .....	298
Figure 9-7	Control field .....	299
Figure 9-8	Example for Top list statistics .....	299
Figure 9-9	Configuration dialogue - Statistics - Statistics Cooking .....	300
Figure 9-10	Event chain of a cooking instance .....	301
Figure 9-11	Timed connection statistics starting at 08.03. ....	302
Figure 9-12	Timed connection statistics starting at 09.03. ....	302

## 10 Eventing

Figure 10-1	Event detail window .....	307
Figure 10-2	Severity tab .....	307
Figure 10-3	Notification tab .....	308
Figure 10-4	Server Action tab - Type Mail .....	309
Figure 10-5	Server Action tab - Type Execute Program .....	309
Figure 10-6	Server Action tab - Type SNMP .....	309
Figure 10-7	Example for a SNMP trap .....	310
Figure 10-8	Example for occurring event and settings for Threshold tab .....	310
Figure 10-9	Basic tab .....	311
Figure 10-10	Event monitor .....	311
Figure 10-11	Context menu .....	312
Figure 10-12	Page 1 of the Properties dialogue .....	312
Figure 10-13	Page 2 of the Properties dialogue .....	312
Figure 10-14	Filter dialogue with values according to the example .....	314
Figure 10-15	Add Criterion dialogue .....	314
Figure 10-16	Event monitor in live mode .....	314

## 11 DNS

Figure 11-1	File structure of the DNS service .....	317
Figure 11-2	DNS configuration area .....	317
Figure 11-3	DNS server properties .....	317
Figure 11-4	DNS properties with open advanced window .....	319
Figure 11-5	Configuring a new SOA .....	319
Figure 11-6	Configuring a new name server .....	320
Figure 11-7	Adding a nameserver .....	320
Figure 11-8	Configuring a New Host .....	320
Figure 11-9	Configuring a new mail exchanger .....	321
Figure 11-10	Configuring a new sub-domain .....	321
Figure 11-11	Create reverse lookup zone .....	322

## 12 Proxy

Figure 12-1	Creating the HTTP Proxy service .....	324
Figure 12-2	Creating the HTTP Proxy service .....	324
Figure 12-3	HTTP Proxy Config node in the Configuration Tree .....	324
Figure 12-4	HTTP Proxy Service Parameters - Network .....	325
Figure 12-5	SNMP message handling .....	327
Figure 12-6	Config Section Dialogue - Authentication Settings .....	327
Figure 12-7	Proxy Access Handling Scheme .....	328
Figure 12-8	ACL Time Interval configuration - Example 1 .....	332
Figure 12-9	ACL Time Interval configuration - Example 2 .....	333
Figure 12-10	ACL Entries and Actions configuration example .....	333
Figure 12-11	Configuration of Action webaccess .....	334
Figure 12-12	Proxy neighbour cache configuration - Example setup .....	334
Figure 12-13	Reverse proxy example configuration .....	336
Figure 12-14	Secure Web Proxy GUI - Access tab .....	339
Figure 12-15	Secure Web Proxy GUI - Tickets tab with detail info .....	340
Figure 12-16	Secure Web Proxy GUI - Certificates tab .....	340
Figure 12-17	Overview: URL filtering process .....	342
Figure 12-18	Flowchart - Proventia Web Filter Redirector & Daemon .....	343
Figure 12-19	Local rule granting access from Proventia Web Filter to Proventia Internet Databases .....	347
Figure 12-20	Principle of Load Sharing .....	349
Figure 12-21	Principle of High Availability .....	349

## 13 FTP Gateway

Figure 13-1	FTP-GW Settings .....	352
-------------	-----------------------	-----

## 14 Voice over IP

Figure 14-1	Provisioning the plugin in a service object for the SCCP signalling	356
Figure 14-2	RTP Stream service object with the default service name set to RTP:Skinny	357
Figure 14-3	VoIP infrastructure with 2 virtual subnets	357
Figure 14-4	Creating an Address Translation Map	357
Figure 14-5	Skinny signal protocol firewall rule with Skinny firewall plugin	358
Figure 14-6	RTP firewall rule with network address translation from the voipnat address translation map	358
Figure 14-7	Firewall Forwarding Settings - H.323 Gatekeeper Configuration dialogue	359
Figure 14-8	Network setup without NAT - SIP/RTP	361

## 15 SSH Gateway

Figure 15-1	Configuration dialogue - SSH Proxy	364
-------------	------------------------------------	-----

## 16 Anti-Virus

Figure 16-1	Scanning exceptions	369
Figure 16-2	Schematic overview of proxy integration	369
Figure 16-3	Scan exceptions	370
Figure 16-4	Progress bar	371
Figure 16-5	Schematic overview of mail gateway integration	371
Figure 16-6	Schematic overview of FTP gateway integration	372
Figure 16-7	Disabling virus pattern updates manually	373

## 17 High Availability

Figure 17-1	Load Balancing with a HA system	377
Figure 17-2	HA monitoring without private uplink (HA state exchanged via 10.0.8.0/8 network)	378
Figure 17-3	HA monitoring with private uplink	378
Figure 17-4	Designing a HA system	378
Figure 17-5	Context menu of Box	379
Figure 17-6	Exporting the public key to a file	380
Figure 17-7	Public Host Keys	380
Figure 17-8	Creation of MC-administered HA partners - Step 1	380
Figure 17-9	Creation of MC-administered HA partners - Step 2	380
Figure 17-10	Sync Status of two HA partners	381
Figure 17-11	Emergency Override of a HA Box	381
Figure 17-12	Confirmation query for Emergency Override	381
Figure 17-13	Example for test report	381
Figure 17-14	Synchronising procedure	383

## 18 phion management centre

Figure 18-1	Schematic view of a phion netfence topology with a management centre	389
Figure 18-2	Flowchart - How a netfence gateway becomes a management centre	389
Figure 18-3	Certificates and Keys - Private Encryption	390
Figure 18-4	Certificates and Keys - Public Encryption	390
Figure 18-5	Certificates and Keys - X509 Certificates	390
Figure 18-6	MC trust centre	391
Figure 18-7	Extract from the Box tab in the Box Control window where authentication level can be lowered to interaction-free authentication	392
Figure 18-8	Control - Server tab with required/recommended MC services	393
Figure 18-9	Box Licenses configuration	394
Figure 18-10	phion.a warning when logging in without licenses	394
Figure 18-11	Master License configuration	394
Figure 18-12	MC user interface - Overview	395
Figure 18-13	Group view of elements in the Statistics Collection tab, sorted alphabetically by box name	396
Figure 18-14	Floating Licenses tab showing licenses supplied for all boxes	397
Figure 18-15	Floating Licenses tab only showing licenses supplied for boxes in cluster GLE	397
Figure 18-16	Status Map tab	397
Figure 18-17	Box section context menu	397
Figure 18-18	Example for a Favourites tab with wallpaper and small icons	398
Figure 18-19	Configuration Updates tab	398
Figure 18-20	Floating Licenses tab	400
Figure 18-21	Box Execution tab	401
Figure 18-22	Box List - Edit Object	402
Figure 18-23	Creating a box group object	402
Figure 18-24	Schedule Task window	403
Figure 18-25	Box Execution tab	404
Figure 18-26	Shell Script	404
Figure 18-27	Box Exec with tasks running	404
Figure 18-28	Box log file view	404
Figure 18-29	Rescheduling of a failed task	404
Figure 18-30	Software Update tab - Groups view	405
Figure 18-31	Software Update tab - Groups view	406
Figure 18-32	Software Update tab - Ranges view	406
Figure 18-33	Software Update tab - Boxes view	406
Figure 18-34	Software Update tab - Versions view	406
Figure 18-35	Box Details window	407
Figure 18-36	RPM information window	408
Figure 18-37	Scheduling a new task	408

Figure 18-38	Rescheduling of a failed task	409
Figure 18-39	management centre (MC) - Configuration Service	410
Figure 18-40	MC Config main window - launch control for box	410
Figure 18-41	Pool Licenses - user interface	411
Figure 18-42	MC Identity - Identification	412
Figure 18-43	Create Range - configuration dialogue	416
Figure 18-44	Creating a cluster server with referencing Server IP addresses to network objects	418
Figure 18-45	Adding a Cluster Service	419
Figure 18-46	Box configuration - wizard for creating a box	420
Figure 18-47	Box configuration - launch control for box	420
Figure 18-48	Different types of repositories	421
Figure 18-49	Configuration tree displayed in default view (left) and with toggled release view (right)	421
Figure 18-50	Repository objects flagged with version information	421
Figure 18-51	Migrating a cluster - Step 1	422
Figure 18-52	Migrating a cluster - Step 2	422
Figure 18-53	Example: Mail-Gateway configuration nodes prior to and after Migrate Cluster activation	422
Figure 18-54	Migrating a range - Step 1	423
Figure 18-55	Migrating a range - Step 2	423
Figure 18-56	Migrating multiple clusters/ranges - Step 1	423
Figure 18-57	Migrating multiple clusters/ranges - Step 2	423
Figure 18-58	Migrating a repository object - Step 1	423
Figure 18-59	Migrating a repository object - Step 2	423
Figure 18-60	Cascading the localnet network object	425
Figure 18-61	Cascading the specialnet network object	425
Figure 18-62	Workflow of rule set processing	425
Figure 18-63	Configuration nodes of the cfirewall service - Global section	425
Figure 18-64	Configuration nodes of the cfirewall service - Server section	426
Figure 18-65	Exemplary cfirewall setup	427
Figure 18-66	Content of the Global Rule Set, which is saved in the Range Repository	427
Figure 18-67	Cascading of the specialnet network object	428
Figure 18-68	Rule allowing communication over MS Exchange Server	428
Figure 18-69	Initial network situation	428
Figure 18-70	Network after MC migration	428
Figure 18-71	Further Networks configuration dialogue	429
Figure 18-72	Box VIP Network Ranges	429
Figure 18-73	Shell script "boxactivate" for box network activation	430
Figure 18-74	Workflow for establishing an administration concept	432
Figure 18-75	Admins tab	433
Figure 18-76	Administrator configuration dialogue	433
Figure 18-77	Administrator Details configuration dialogue	434
Figure 18-78	Master Statistic Collection Configuration dialogue	436
Figure 18-79	Range Configuration dialogue	437
Figure 18-80	Cluster Configuration dialogue	437
Figure 18-81	Statistics Cook Settings	438
Figure 18-82	Cook Settings configuration dialogue	438
Figure 18-83	Transfer Settings configuration dialogue	440
Figure 18-84	Transfer Settings - box and server files	441
Figure 18-85	Transfer Settings - partial transfer	442
Figure 18-86	Box event	443
Figure 18-87	Box event propagation to MC	443
Figure 18-88	MC: Box event occurred	443
Figure 18-89	MC: Event status changed	443
Figure 18-90	Box: Event status changed	443
Figure 18-91	MC: Delete Event	443
Figure 18-92	Box: Delete Event	443
Figure 18-93	Example for log reception via port 5144 and/or 5143	446
Figure 18-94	Log processing flowchart	446
Figure 18-95	Example for message delivery to local disk	446
Figure 18-96	Example for a HA sync via private uplink (using the override IPs is mandatory)	447
Figure 18-97	Example for successful active SSL querying	447
Figure 18-98	Example for passive SSL receiving	447
Figure 18-99	Log file structure of service processes overview	452
Figure 18-100	Example 1: Syslog Proxy - Basic Setup	454
Figure 18-101	MC FWAudit Viewer	457
Figure 19	Audit Info Viewer	458
Figure 18-1	Configuration dialogue - PKI	459
Figure 18-2	PKI - User Interface	460
Figure 18-3	Configuration dialogue - General Settings tab	460
Figure 18-4	Import Certificate dialogue	462
Figure 18-5	Export Certificate dialogue	462
Figure 18-6	Export Private Key dialogue	462
Figure 18-7	Export CRL dialogue	462
Figure 18-8	User Interface of a generic forwarder	464
Figure 18-9	User Interface	464
Figure 18-10	Example VPN group	465
Figure 18-11	Open Tunnel Info node	465
Figure 18-12	New filtered for <s0-Borde> vpn-bo/cluster1/10	466
Figure 18-13	Example VPN group displayed as table	466
Figure 18-14	Adding a VPN Service to a VPN Group - Step 1	468
Figure 18-15	Adding a VPN Service to a VPN Group - Step 2	468
Figure 18-16	Open Tunnel Info node and Tunnel configuration dialogue	469
Figure 18-17	Tunnel configuration dialogue	469



Figure 18-18	Tunnel Info node displaying links to transports .....	470
Figure 18-19	netfence VPN world settings .....	471
Figure 18-20	VPN world .....	472
Figure 18-21	Configuration dialogue - RCS .....	473
Figure 18-22	RCS Versions window .....	474
Figure 18-23	Example for selecting versions of interest .....	474
Figure 18-24	Example for selecting versions of interest with selected Full History checkbox .....	475
Figure 18-25	RCS Report window .....	475
Figure 18-26	RCS Change Filter .....	476

**19 SNMP**

Figure 19-1	SNMP service configuration dialogue .....	481
-------------	---	-----

**20 OSPF and RIP**

Figure 20-1	Example setup for OSPF and RIP configuration .....	492
Figure 20-2	Configuring of addresses in the Server Properties .....	493
Figure 20-3	OSPF Routing Settings - Operational Setup .....	493
Figure 20-4	OSPF Routing Settings - OSPF Router Setup .....	493
Figure 20-5	Routing table displaying routes learned through OSPF .....	493
Figure 20-6	Quagga engine output .....	494
Figure 20-7	Configuring Route Redistribution .....	494
Figure 20-8	Configuring Default Route Redistribution .....	495
Figure 20-9	Configuring a parameter template .....	495
Figure 20-10	Creating a link to the parameter template .....	495
Figure 20-11	Configuring route summarisation .....	496
Figure 20-12	Entry in routing table .....	496
Figure 20-13	Configuring RIP settings - RIP Router Setup .....	496
Figure 20-14	Configuring route redistribution .....	496
Figure 20-15	Configuring route redistribution .....	496

**21 Licensing**

Figure 21-1	Example setup .....	499
Figure 21-2	Principle of a node-locked license on a self-managed netfence gateway .....	500
Figure 21-3	Certificate file as shown after box import and activation .....	500
Figure 21-4	Licenses interrelationship between MC and MC-administered boxes .....	501
Figure 21-5	License view of the control window without valid license activated .....	503
Figure 21-6	License view of the control window with valid licenses activated .....	503
Figure 21-7	License view of the control window with an invalid license activated on an MC. ....	504
Figure 21-8	Grace time for floating box licenses .....	504
Figure 21-9	License view of the control window with floating licenses that will expire in 7 days .....	504
Figure 21-10	License view of the control window with deactivated services .....	505
Figure 21-11	Finding out the host key .....	506
Figure 21-12	Exemplary content of a phion license .lic file .....	506
Figure 21-13	View of the Licenses tab after having activated the license key .....	507
Figure 21-14	Policy for redirected destination .....	509
Figure 21-15	Policy for site-to-site tunnels .....	509

**22 System Information**

Figure 22-1	Example - options file .....	513
Figure 22-2	Example - boxadm.conf file .....	513
Figure 22-3	Example - boxnet.conf file .....	514
Figure 22-4	Event Monitor GUI .....	516
Figure 22-5	Event Properties windows .....	516

**23 Appendix**

Figure 23-1	Adding a new column to the view .....	524
Figure 23-2	Search result containing group information .....	524
Figure 23-3	LDAP browser with marked distinguished name .....	524

## 9. Glossary

### A

Table 23-137 Glossary - A

<b>Access Cache</b>	History list of already performed firewall connections / mail jobs / VPN connections.
<b>ACK</b>	Third part of the Three-Way Handshake of a TCP connection (see also SYN/ACK, SYN, <b>FIN</b> , <b>Flag</b> , <b>Handshake</b> )
<b>ACPF</b>	<b>A</b> pplication <b>C</b> ontrolled <b>P</b> acket <b>F</b> orwarding
<b>ACL</b>	Access control list. List of IP addresses which are allowed to manage a box
<b>Admin, Flower</b>	An administrator account which is granted only read rights to a system (see also <b>root</b> )
<b>Admin, Power</b>	An administrator account which is granted full access to a system (see also <b>root</b> )
<b>ADSL</b>	Asymmetric Digital Subscriber Line, technology to allow high speed internet connections over ordinary copper cables via the telephone net (see also <b>Broadband</b> )
<b>Alive Packets</b>	ICMP packets to check the system status (see also <b>HA</b> )
<b>ANSI</b>	ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States.
<b>ARP</b>	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address (MAC address) that is recognized in the local network (see also IP address, <b>MAC</b> ).
<b>Authentication</b>	Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. There is also the possibility to make use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure (PKI) is considered likely to become the standard way to perform authentication on the Internet. (see also <b>Certificate</b> , PKI)

### B

Glossary - B

<b>Bandwidth</b>	Bandwidth (the width of a band of electromagnetic frequencies) is used for defining how fast data flows on a given transmission path (see also <b>Broadband</b> ).
<b>Bash</b>	<b>B</b> ourne <b>A</b> gain <b>S</b> hell, standard linux shell
<b>Bind IP</b>	IP address of the firewall which is used for the further connection (see also <b>Destination IP</b> , Source IP, <b>Connect IP</b> )
<b>Block</b>	Firewall Rule Type: A TCP / UDP / ICMP connection attempt is denied due to a firewall rule match. If there is no firewall rule defined, all connections will be blocked (see also Pass, <b>Redirect</b> , <b>Map</b> ).
<b>Border Firewall</b>	Firewall which has a direct connection to the internet and protects the interior part of a network.
<b>Box Services</b>	Infrastructure services that are providing HA support, real time system monitoring, accounting (statistics) and logging
<b>Box</b>	Lowest layer of phion architecture. Entities and processes belonging to the box layer exist independently of all server processes.
<b>Break Lock</b>	Attempt to break an existing lock of a configuration file by another management session which was made by another administrator
<b>Broadband</b>	Links of high data rate are called broadband connections (see also <b>Bandwidth</b> ).
<b>Broadcast Domain</b>	A network segment which is limited by a network-layer device (for example a router or a phion netfence firewall)
<b>Broadcast</b>	Data is sent to all peers in a broadcast domain

### C

Table 23-138 Glossary - C

<b>Certificate</b>	phion boxes make use of x.509 conformant digital certificates. For a single box without phion trust centre being available the certificate is basically identical to a mere RSA public key.
<b>CGI</b>	<b>C</b> ommon <b>G</b> ateway <b>I</b> nterface is a standard for interfacing external applications with web servers.
<b>Checksum</b>	The sum of a group of data items, which sum is used for checking purposes. <b>Note:</b> A checksum is stored or transmitted with the group of data items and is calculated by treating the data items as numeric values. Checksums are used in error detecting and correcting. The value computed on data to detect error or manipulation during transmission (see also <b>HASH</b> ).
<b>CIFS</b>	The <b>C</b> ommon <b>I</b> nternet <b>F</b> ile <b>S</b> ystem is a further development of the SMB protocol and serves as an addition and improvement to the standard protocols FTP and HTTP.
<b>Clock skew</b>	Clock skews are events that describe an inconsistency in the timed recording of sequences. This can occur when the system time has been changed for example, through which the incremental record of the time stamp is disturbed in the log.
<b>Cluster</b>	Several boxes which belong together logically form a cluster - it is very useful to segment large networks into clusters.
<b>Cluster Server</b>	Server available for a whole cluster
<b>Cluster Service</b>	Service of a cluster server available for whole cluster.
<b>Collision Domain</b>	Network segment which is limited by a data-link layer device (for example a switch)
<b>Connect IP</b>	IP address to which the firewall connects (see also <b>Bind IP</b> , <b>Destination IP</b> , Source IP)
<b>Connection type</b>	UDP / TCP or ICMP connection type.
<b>CPU</b>	Central Processing Unit, another term for processor

### D

Table 23-139 Glossary - D

<b>Daemon</b>	System process (control daemon, cstat daemon)
<b>Decryption</b>	Previously encrypted data has to be decrypted in order to be able to read the original data. The decryption algorithm must be the same as the algorithm used for encryption (see also <b>Encryption</b> ).
<b>Default Gateway</b>	Refer to Route, Default
<b>Destination IP</b>	IP address to which the source connects (see also <b>Bind IP</b> , <b>Connect IP</b> , Source IP)
<b>DHCP</b>	Dynamic Host Configuration Protocol, a DHCP server provides normally information like IP addresses, netmask, routes and DNS servers
<b>DMA</b>	Direct Memory Access
<b>DMZ</b>	Demilitarised Zone, network to put in every from the internet reachable machines (for example Mail-, Web-, or FTP-Servers)
<b>DNS (BIND)</b>	Domain Name Service is used to resolve Domain names to IP addresses, BIND is the Berkeley internet name demon (mostly used DNS server)
<b>DNS, Name Servers</b>	The programs which store information about the domain name space are called name servers.
<b>DNS, Zone Transfer</b>	The transfer of zone information from a master to a slave is called zone transfer
<b>DNS, Zone</b>	Name Servers generally have complete information about some part of the name space, called a zone.
<b>DNS, Zone, Forward</b>	A forward zone is used to direct all queries in it to other servers. The specification of options in such a zone will override any global options declared in the options statement.
<b>DNS, Zone, Hint</b>	The initial set of root nameservers is specified using a hint zone. When the server starts up, it uses the root hints to find a root nameserver and get the most recent list of root nameservers.

Table 23-139 Glossary - D

<b>DNS, Zone, Master</b>	The server has a master copy of the data for the zone and will be able to provide authoritative answers for it.
<b>DNS, Zone, Reverse Lookup</b>	To resolve IP addresses to host names (domains) a Reverse Lookup is performed
<b>DNS, Zone, Slave</b>	A slave zone is a replica of a master zone. The masters list specifies one or more IP addresses that the slave contacts to update its copy of the zone.
<b>DST</b>	Daylight Saving Time (see also <b>UTC, Time Zone</b> )

E

Table 23-140 Glossary - E

<b>EIDE</b>	refer to IDE
<b>Emergency Override</b>	Usually, management centre (MC) maintained boxes can only be configured via the MC, unless an emergency override is performed. This enables configuration changes directly performed via the box configuration.
<b>ENA</b>	Exclusive Network Access, phion VPN option to enable exclusive network access to the phion VPN adapter (see also <b>VPN</b> )
<b>Encryption</b>	Data is changed according to a certain algorithm for security reasons- encrypted data cannot be read.
<b>Ethernet Trunk</b>	A ethernet trunk may be used to bond several ethernet interfaces together to form so called bonding channels or ethernet trunks
<b>Ethernet</b>	Ethernet is the most widely-installed local area network (LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps. Interfaces are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.
<b>Ethernet, Fast</b>	or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems, supporting workstations with 10BASE-T cards. Gigabit Ethernet provides an even higher level of backbone support at 1000 megabits per second (1 gigabit or 1 billion bits per second). 10-Gigabit Ethernet provides up to 10 billion bits per second.

F

Table 23-141 Glossary - F

<b>FIN</b>	The FIN flag ends a TCP connection (see also SYN, SYN/ACK, <b>ACK, FIN, Flag, Handshake</b> )
<b>Firewall</b>	A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. <b>Note:</b> The term also implies the security policy that is used with the programs.  An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to (see also <b>Rule, Rule Set, Gateway</b> ).
<b>Flag</b>	Part of a TCP connection (see also SYN, SYN/ACK, <b>ACK, FIN, Flag, Handshake</b> )
<b>Foreign Lock</b>	A configuration file that has been locked by another administrator
<b>Forwarding, IP</b>	IP forwarding is a mechanism to route IP packets from one network interface to another.
<b>Forwarding, Port</b>	Port forwarding works by mapping a local port on the client to a remote port on the server
<b>FQDN</b>	Fully qualified domain name
<b>FTP</b>	File Transfer Protocol (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. FTP is an application protocol that uses the Internet's TCP/IP protocols.
<b>FDDI</b>	Fibre Distributed Data Interface (FDDI); type of interface used for sending digital data over fibre optic cable. FDDI networks are token-passing networks with up to 100Mbps used as backbones

G

Table 23-142 Glossary - G

<b>Gateway</b>	A gateway is a network point that acts as an entrance to another network
<b>GUI</b>	Graphical User Interface: an application which runs on a graphical desktop oriented operation system (such as Microsoft® Windows®). The GUI of phion netfence software is phion.a.

H

Table 23-143 Glossary - H

<b>HA</b>	High availability on netfence gateways is done by swapping the server from one box to the other. This process is triggered by the control daemon.
<b>Handshake</b>	A TCP connection involves some components called flags, to make a proper TCP connection correct set flags are needed, the so called Three Way Handshaking (see also SYN, SYN/ACK, <b>ACK, FIN, Flag</b> )
<b>HASH</b>	1. The result obtained by subjecting a set of data to an algorithm for purposes of checking the data at the time the algorithm is applied or for use at a later time such as after transmission or retrieval from storage. 2. A value computed on data to detect error or manipulation. (see also <b>Checksum</b> )
<b>Host Keys</b>	Unique keys to verify a machine to a license, usually CPU ID's or MAC addresses (see also <b>MAC, CPU</b> ).
<b>Hot Fix</b>	A hot fix repairs actual problems and could be provided within a short amount of time (see also Service Pack).
<b>HTTP</b>	The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

I

Table 23-144 Glossary - I

<b>ICMP</b>	ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user
<b>IDE</b>	IDE (Integrated Drive Electronics) is a standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices. The IDE interface is based on the IBM PC Industry Standard Architecture (ISA) 16-bit bus standard, but it is also used in computers that use other bus standards. Most computers sold today use an enhanced version of IDE called Enhanced Integrated Drive Electronics (EIDE).
<b>IEN</b>	Internet Engineering Notes
<b>IMAP</b>	Internet Message Access Protocol (IMAP) is a standard protocol for accessing email from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which email is received and held for you by your Internet server.
<b>Inbound</b>	The inbound/outbound policy is a very important parameter to protect servers from SYN flooding attacks on allowed connections. The firewall tries first to establish a connection to the requesting source and then establish the connection between itself and the requested destination (see also <b>Outbound</b> ).
<b>IP address</b>	A 32-bit (4 dot-separated bytes) number to address hosts/networks on the network-layer. One byte presents the numbers 0 to 255.
<b>IP Tunnel</b>	Simple point-to-point tunnels using generic routing or plain IP in IP encapsulation. The box-based tunnels you may configure here do neither offer peer authentication nor encryption support. (see also <b>Box, VPN</b> )
<b>IPsec</b>	IPsec (Internet Protocol Security) is a developing standard for security at the network or packet processing layer of network communication.

J

Numerics | A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

## K

Table 23-145 Glossary - K

<b>Kernel</b>	The essential part of Unix or other operating systems, responsible for resource allocation, low-level hardware interfaces, security ...
<b>Kernel, SMP</b>	Symmetric Multiprocessor Kernel (see also <b>Kernel, Multi Processor</b> )
<b>Kick-Start File</b>	File which contains information about hardware configuration (partitions, keyboard, time-zone, language) and provides them at the installation routine, Red Hat (r) proprietary

## L

Table 23-146 Glossary - L

<b>LDAP</b>	LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and interfaces in a network, whether on the public Internet or on a corporate intranet.
<b>Lease(s)</b>	Used for DHCP; consists of an IP address and corresponding options for lending to a client PC.
<b>License, Evaluation</b>	A freshly installed unlicensed single box runs in evaluation mode. This is a fully functional netfence box, without working box ACLs and with root and phion password phion (see also <b>root, ACL</b> ).
<b>License, Floating</b>	If there is a management centre with a various amount of pool licenses, you can import a floating license. Just introduce a new box, and the floating license is delivered from the management centre (see also <b>management centre, License, Pool</b> )
<b>License, Grace</b>	A single box which was installed with wrong licenses, this will lead to the so called grace period where the box is fully functional, the grace period is configurable, after this time the box changes to evaluation mode.
<b>License, Personal</b>	License to access a VPN network
<b>License, Pool</b>	An arbitrary amount of licenses on a management centre (see also <b>management centre, License, Floating</b> )
<b>License, System</b>	License for phion system processes
<b>License, Valid</b>	A single box with valid licenses.
<b>LACPDU</b>	Link Aggregation Control Protocol Data Unit
<b>Linux</b>	An open-source operating system which is the base of phion netfence software (not the GUI)
<b>Load Balancing</b>	Load (traffic) is split up to several servers in order to improve data rate and reliability
<b>Lock</b>	To avoid the situation that configuration files are edited from several administrators at the same time, a configuration file has to be locked

## M

Table 23-147 Glossary - M

<b>MAC</b>	Media Access Control addresses (see also <b>ARP, Broadcast</b> )
<b>Mail Body</b>	This is the actual content of the email. The mail body begins after the subject and ends at the end of the email. Attachments ... are also part of the mail body.
<b>Mail Envelope</b>	This is the SMTP part of email delivery. Like a real mail envelope it contains sender and recipient address.
<b>Mail Exchange (MX)</b>	official DNS host name of a mail server- a MX server usually contains mail boxes ...
<b>Mail Header</b>	To every email a mail header, which contains sender / recipient / reply-to address, date, email client version, MIME version etc, is added.
<b>Mail Relay</b>	Abuse of a mail gateway to distribute spam mail
<b>management centre</b>	Administrative "headquarters" to administer and configure a multi firewall architecture.
<b>Management IP</b>	The IP address that is used for managing the netfence gateway. Use this IP address to connect yourself with the phion.a administration GUI to the system.
<b>Map</b>	Extensive Destination NAT (of whole subnets) (see also <b>NAT</b> )
<b>Masquerading</b>	Masquerading is used to mask internal IP addresses with an official IP address (see also <b>NAT</b> )

Table 23-147 Glossary - M

<b>MIME</b>	Multipurpose Internet Mail Extension; for adding mail extensions (for example picture attachments which most email client applications display in the mail body), MIME is used.
<b>Module</b>	A kernel module is a special program that can be loaded into (become a part of) the Linux kernel on demand (see also <b>Kernel</b> ).
<b>MSAD</b>	Authentication over a MS Active Directory Server
<b>MSNT</b>	Authentication over a MSNT Server
<b>MTA</b>	Mail Transfer Agent: Service process of the mail gateway service which is responsible for mail delivery to a foreign mail server
<b>Multi Administrator</b>	In an environment with a management centre and several firewalls it is possible that there is more than one administrator with different privileges (see also <b>Admin, Flower, Admin, Power, root, management centre</b> )
<b>Multi Processor</b>	A computer system which has two or more processors connected in the same cabinet, managed by one operating system, sharing the same memory, and having equal access to input/output interfaces. Application programs may run on any or all processors in the system- assignment of tasks is decided by the operating system.
<b>Multicast</b>	Data is sent to multiple peers

## N

Table 23-148 Glossary - N

<b>NAS</b>	Network Access Server
<b>NAT</b>	Network Address Translation is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses.
<b>NBDD</b>	NetBios Datagram Distribution
<b>NetBIOS</b>	Network Basic Input/Output System; very common protocol and is supported on Ethernet and TokenRing. In NetBIOS, TCP and UDP communication are supported. It supports broadcasts and multicasting and three distinct services: Naming, Session, and Datagram.
<b>Netmask</b>	To separate network and host addresses the netmask is used.
<b>NIC</b>	Network Interface Card
<b>NIS</b>	Network Information System; network lookup service consisting of databases and processes to provide information that has to be known throughout a network (for example login names and passwords, host names and IP addresses)
<b>NTP</b>	The Network Time Protocol is a protocol that is used to synchronise computer clock times in a network of computers.

## O

Table 23-149 Glossary - O

<b>Outbound</b>	The inbound/outbound policy is a very important parameter to protect your servers from SYN flooding attacks on allowed connections. The firewall tries to establish a connection to the requested destination and then establishes the connection between itself and the client (see also Inbound).
<b>OSPF</b>	The <b>Open Shortest Path First</b> protocol is a hierarchical interior gateway protocol (IGP) for routing in Internet Protocol, using a link-state in the individual areas that make up the hierarchy. A computation based on Dijkstra's algorithm is used to calculate the shortest path tree inside each area. The current version, Version 3, defined in RFC 2740 (OSPFv3 1999), supports IPv6 only, while OSPF version 2 supports IPv4. (OSPFv2 1998). (see also RIP)

## P

Table 23-150 Glossary - P

<b>PAP</b>	Password Authentication Protocol
------------	----------------------------------

Table 23-150 Glossary - P

<b>PAR</b>	Phion ARchive, phion standard to save configurations via so-called PAR files
<b>Pass</b>	A TCP / UDP / ICMP connection attempt is granted due to a firewall rule match
<b>PAT</b>	Port Address Translation (PAT) is a feature of a network device that translates TCP or UDP communications made between hosts on a private network and hosts on a public network. It allows a single public IP address to be used by many hosts on the private network.
<b>Peer IP</b>	IP address of a foreign host which is source or destination of a connection
<b>phion.a</b>	phion administration tool (see also <b>GUI</b> )
<b>phion.i</b>	phion installation tool
<b>phionctrl</b>	Command line tool to take control of phion processes
<b>phion notation</b>	The phion notation is contrary to the CIDR notation (for example 255.255.255.255 - CIDR: 32, phion:0). ( <b>Getting Started</b> - 5. phion Notation, page 25)
<b>Ping</b>	Command to send ICMP echo requests
<b>PKI</b>	A PKI (public key infrastructure) enables users of a basically insecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organisation and directory services that can store and, when necessary, revoke the certificates.
<b>Point of Entry</b>	MC itself or array of IP addresses (points of entry or POE) which masquerade the MC.
<b>POP3</b>	POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving email. POP3 is a client/server protocol in which email is received and held for you by your Internet server.
<b>Primary Box</b>	In a HA environment the box which runs all servers and services until a serious fault occurs or the system has to be shut down for system maintenance and the secondary box will start servers and services (see also Secondary Box, <b>HA</b> )
<b>Private Key</b>	In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key. See public key infrastructure (PKI) for more information (see also Public Key, PKI).
<b>Processes</b>	A process is a collection of operations which perform certain tasks
<b>Protocol</b>	In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. There are hardware telephone protocols. There are protocols between each of several functional layers and the corresponding layers at the other end of a communication. Both end points must recognise and observe a protocol. Protocols are often described in an industry or international standard.
<b>Proxy</b>	In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. (see also <b>Masquerading, NAT</b> )
<b>Proxy ARP</b>	IP addresses for which the firewall answers to ARP requests, these IP addresses do not "live" on this system
<b>Public Key</b>	In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI) (see also Private Key, PKI)

Q

R

Table 23-151 Glossary - R

<b>RADIUS</b>	RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorise their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.
<b>Range</b>	Several clusters which belong together logically form a range
<b>RAS</b>	Reliability, Availability, Serviceability. Remote Access Service
<b>RDP</b>	Remote Desktop Protocol
<b>Redirect to exe</b>	With firewall rules it is possible to redirect IP addresses to executable files
<b>Redirect with cycling</b>	A kind of load balancing
<b>Redirect</b>	With firewall rules it is possible to redirect IP addresses to other IP addresses.
<b>Redundant</b>	Redundant describes computer or network system components, such as fans, hard disk drives, servers, operating systems, switches, and telecommunication links that are installed to back up primary resources in case they fail.
<b>Repository</b>	Part of the config tree of a management centre (MC) maintained box where configuration settings can be stored.
<b>RIP</b>	The <b>Routing Information Protocol</b> allows network routers to adapt dynamically to changing network connections by swapping information about which networks each router can reach, and how far away those networks are. (see also OSPF)
<b>root Alias</b>	Aliases for the root administrator account
<b>root</b>	Administrator of Unix systems
<b>Round Robin</b>	In computer operation, one method of having different program process take turns using the resources of the computer is to limit each process to a certain short time period, then suspending that process to give another process a turn (or "time-slice"). This is often described as round-robin process scheduling. This term is also used for a simple way of load balancing in a server farm.
<b>Route</b>	In a route is defined which way a packet has to be forwarded (see also <b>Router</b> )
<b>Route, Default</b>	Every traffic where no own routing table exists is routed via the default gateway (see also <b>Router</b> )
<b>Route, Direct</b>	Traffic is routed over an interface
<b>Route, Gateway</b>	Traffic is routed over a gateway
<b>Route, Pending</b>	One of the advanced features of phion boxes is that you may still configure such so-called pending direct routes since they will be hidden from the operating system until an appropriate source address becomes available. In the context of firewalling this would allow you to configure a routing setup that becomes only active when the firewall is active. The advantage of this is that the box as such will never be directly accessible as a target for malicious activity.
<b>Route, Wild</b>	phion specific for a route which is activated direct on a box instead of the network configuration GUI
<b>Router</b>	On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each Internet point-of-presence.
<b>Routing, Policy</b>	Policy routing is a means to implement more complex routing scenarios. Since the firewall configuration (on a per rule basis) allows you to specify the address with which an allowed connection is established policy routing represents an extremely powerful instrument to manage firewalling in topologically complex environments.



Numerics | A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Table 23-151 Glossary - R

<b>RPM</b>	The RedHat Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Each software package consists of an archive of files along with information about the package like its version, a description, ... phion hot fixes and service packs are provided in RPM packages (see also <b>Hot Fix</b> , <b>Service Pack</b> )
<b>Rule</b>	In a firewall rule is defined in which way a request is handled (see also <b>Block</b> , <b>Pass</b> , <b>Redirect</b> )
<b>Rule, Dynamic</b>	A rule which is activated manually and stays active for a configurable amount of time
<b>Rule, Time Dependent</b>	A rule which is only active on determined hours of a day (e.g private surfing only after 5 pm)
<b>Rule Set</b>	The entirety of all firewall rules of a box forms a rule set.
<b>Rule Set, Cascaded</b>	The phion firewall supports the unique feature of cascaded rule sets. For multi-administrator clusters access to parts of the rule set can be restricted for sub-administrators (see also <b>Multi Administrator</b> , <b>management centre</b> , <b>Rule Set</b> ).

## S

Table 23-152 Glossary - S

<b>SCSI</b>	The Small Computer System Interface, is a set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drives, CD-ROM drives, printers, and scanners faster and more flexibly than previous interfaces. (see also <b>ANSI</b> , <b>IDE</b> , <b>EIDE</b> )
<b>Secondary Box</b>	This box checks the primary box, if the primary is unreachable it starts its server and services (see also <b>Primary Box</b> , <b>HA</b> )
<b>Send Changes</b>	By clicking this button, configuration changes are sent from the GUI to the netfence gateway. The changes are not yet activated.
<b>Server</b>	Collection of IP addresses under which the services are made available.
<b>Service Pack</b>	A service pack provides a bunch of updates, the database which holds the version numbers is updated (see also <b>Hot Fix</b> )
<b>Service</b>	Operational services that provide the actual functionality of the netfence gateway
<b>SMB</b>	Server Message Block (protocol)
<b>SMTP</b>	Simple Mail Transport Protocol
<b>SNMP</b>	Simple Network Management Protocol; set of protocols for managing complex networks
<b>Socks 4/5</b>	A protocol for handling TCP traffic through a proxy server. It can be used with virtually any TCP application. There are two main versions of SOCKS - V4 and V5. V5 adds an authentication mechanism for additional security. There are many freeware implementations of both versions. One of the most common V5 implementations is SOCKS5 (see also <b>Proxy</b> , <b>NAT</b> )
<b>Source IP</b>	IP address of the connecting instance (see also <b>Bind IP</b> , <b>Connect IP</b> , <b>Destination IP</b> )
<b>Spool</b>	Service process of the mail gateway service which is responsible for scheduling incoming mail jobs
<b>SSH</b>	Secure Shell, an encrypted remote shell to administer a system, formerly telnet or rlogin was used, but without encryption they are senseless in a secure environment
<b>SSL</b>	Secure Socket Layer
<b>SYN</b>	First part of the Three-Way Handshake of a TCP connection (see also <b>ACK</b> , <b>SYN/ACK</b> , <b>FIN</b> , <b>Flag</b> , <b>Handshake</b> )
<b>SYN/ACK</b>	Second part of the Three-Way Handshake of a TCP connection (see also <b>ACK</b> , <b>SYN</b> , <b>FIN</b> , <b>Flag</b> , <b>Handshake</b> )

## T

Table 23-153 Glossary - T

<b>TCP</b>	Transmission Control Protocol
<b>Time Server</b>	To synchronise several machines to the same time a time server is needed (see also <b>NTP</b> )
<b>Time Statistics</b>	Type of statistics which reflect traffic / data / connections over a certain period of time.

Table 23-153 Glossary - T

<b>Time Zone</b>	Time zone where a box is geographically (for example GMT - Greenwich Mean Time)
<b>Token Ring</b>	A token ring network is a local area network in which all computers are connected in a ring or star topology and a binary digit or token-passing scheme is used in order to prevent the collision of data between two computers.
<b>Top Statistics</b>	Type of statistics which reflect traffic / data / connections from peers. Top statistics can be separated in Source and Destination statistics

## U

Table 23-154 Glossary - U

<b>UDP</b>	User Datagram Protocol
<b>Undo</b>	Click this button to perform a complete rollback of an altered configuration. This will only work before clicking the Commit button
<b>Unicast</b>	Data is sent to one peer only
<b>UTC</b>	Universal Time Coordinated or Greenwich Mean Time (GMT) (see also <b>DST</b> , <b>Time Zone</b> )

## V

Table 23-155 Glossary - V

<b>Virtual LAN</b>	A Virtual LAN is used to simulate several networks on one NIC, and one switch port behaves like more switches.
<b>Virtual management IP</b>	This becomes the primary management IP, where the box is administered by a management centre.
<b>VNC</b>	Virtual Network Computing
<b>VPN</b>	Virtual Private Network
<b>VPN Tunnel Stealth</b>	A second popular example for tunnelling is the so-called stealth mode or half-side transparent tunnel. In this case a local network is granted access to a partner network, but not the other way round. Moreover, it hides its internal IP structure to the partner network.
<b>VPN Tunnel Transparent</b>	The simplest configuration for tunnels is to connect two networks with different address ranges transparently. The effect should be that two networks are connected together just like if there were nothing but an open firewall in between.
<b>VPN Tunnel, Star Shaped</b>	Most real world VPN topologies include a headquarters structure. That means that many VPN tunnels terminate on one VPN server. Traffic between outposts is typically routed via the headquarters. This reduces the number of tunnels to manage.

## W

Table 23-156 Glossary - W

<b>Watchdog</b>	phion routine to control and repair system processes
<b>WebDAV</b>	Web-based Distributed Authoring and Versioning
<b>Wild Cards</b>	To simplify data input, certain characters stand for all other possible characters: "?" replaces a single character- "*" replaces a whole string- wildcards and other characters
<b>WINS</b>	Windows Internet Naming Service; is used for providing name resolution for computers with special arrangement (Server and Client must run MS Windows). Such a service uses an automatically updated database with the names of currently available PCs and IP addresses (see also <b>DHCP</b> ).

## X

## Y

## Z



# 10. Log of Changes

**Note:**

This log of changes shows only changes that took effect on this documentation.  
 Take a look at the **Support Newsletter** for a comprehensive list of the changes in the software (downloadable from **Myphion** area at [www.phion.com](http://www.phion.com)).

## 4.2.1

### 4.2.1 Note

Box Settings - Flash Memory - Flash settings will be ignored for all non-flash RAM-based appliances [Configuration Service] . . . . .	101
Content Inspection - Virus Scanner - description for parameter Enable Trickle Feature and Trickle Period (sec.) revised [Anti-Virus] . . . . .	370
Control - CPU load monitoring - section Performance added [Configuration Service] . . . . .	118
How to ... - note on How to set up a Generic VPN Tunnel added (VIP address as Proxy ARP) [Appendix]. . . . .	528
How to tune netfence - note on NOATIME Mount added (changes will not be saved in the PAR file) [Appendix] . . . . .	525
MailGW Settings - examples - note on example 4 added (script activation) [Mail Gateway]. . . . .	253
Remote Management Access - Tunnel Details - default for parameter Used VPN Protocol changed to VPN2 [Configuration Service]. . . . .	67
Resources tab - description and figure Sample Resources tab revised [Control Centre]. . . . .	36

## 4.2.0

### 4.2.0 Attention

MC - netfence 4.2 does not provide support for managing netfence 3.2 clusters (end-of-support date) [phion management centre]. . . . .	410,
[phion management centre] . . . . .	417

### 4.2.0 Feature

Firewall Audit Log tab added [Firewall]. . . . .	178
MC - Create Box Wizard added [phion management centre] . . . . .	420
MC Control Centre - tab Scanner Versions added [phion management centre]. . . . .	405
MC FWAudit Viewer added [phion management centre]. . . . .	457
Progress Popup (download bar) added [Anti-Virus]. . . . .	370
SSL-VPN added [VPN] . . . . .	231

### 4.2.0 Improvement

Access Cache List - column Out-IF - tunnel and transport is now visualized [Firewall]. . . . .	174
Advanced Rule Parameters - section Quarantine Policy and its parameters added [Firewall] . . . . .	156
Box Network - Interface - Ethernet Trunks - parameter LACPDU Packet Rate added [Configuration Service]. . . . .	65
Box Network - Interfaces - Ethernet Trunks - at parameter Operation Mode option LinkAggregation added [Configuration Service] . . . . .	65
Box Settings - Radius Authentication - parameters for NAS added [Configuration Service]. . . . .	114
Bridging Configuration - section Quarantine Bridging and its parameters added [Firewall] . . . . .	184
Configuration - MailGW settings - parameter Max. SMTP Line Length is now configurable [Mail Gateway]. . . . .	255
Connection monitoring of dynamic links - option StrictLCP for parameter Monitoring Method added [Configuration Service] . . . . .	78
General Firewall Configuration - description for parameter Rule Change Behaviour revised [Firewall] . . . . .	128
General Firewall Settings - Audit Information Generation - parameter Audit Delivery reworked [Firewall]. . . . .	130
General Firewall Settings - Audit Information Generation - parameters for ACPF Msg Buffer added [Firewall]. . . . .	130
MC Control Centre - Software Update tab - Note regarding no scope removed, software was fixed [phion management centre] . . . . .	405
Network - xDSL configuration - parameter Local IP Selection reworked, option Dynamic added [Configuration Service] . . . . .	71
Network - xDSL configuration - section PPTP Connection Details - parameter Max MTU/MRU Size added [Configuration Service] . . . . .	72
Network interface cards - support for Intel EEPro1000 (Intel PCIe) and Intel 10 Gigabit (Intel 82598EB) added [Configuration Service]. . . . .	63
Network tab - Interface/IP - Icon for signal strength added [Control Centre] . . . . .	31
phion.i - Configuring USB Stick Settings with phion.i - parameter Format USB-Stick added [Getting Started] . . . . .	14
phion.i - The phion M USB stick may be used to recover all USB enabled Heavensgate appliances [Getting Started] . . . . .	10
Setting up the box - Networks - DHCP configuration - parameter GRE with Assigned IP added [Configuration Service] . . . . .	74
Setting up the box - Networks - ISDN configuration - parameter GRE with Assigned IP added [Configuration Service] . . . . .	76
Setting up the box - Networks - UMTS - parameter Active 2nd Channel added [Configuration Service]. . . . .	76
Setting up the box - Networks - UMTS - parameter Radio Preference added [Configuration Service] . . . . .	76
Setting up the box - Networks - UMTS configuration - parameter GRE with Assigned IP added [Configuration Service] . . . . .	78
Setting up the box - Networks - xDSL configuration - parameter GRE with Assigned IP added [Configuration Service]. . . . .	73
SSL Settings - description for parameters External Root CA Private Key / External Root CA Certificate revised [Proxy] . . . . .	338
Syslog Streaming - description for parameter Loghost Port revised [Configuration Service] . . . . .	117
Syslog Streaming - description for parameter Peer SSL Certificate revised [Configuration Service]. . . . .	117

TINA tunnel- traffic intelligence - parameter Balance Preferred and Second added [VPN] . . . . .	224
UMTS - support for Huawei E169 card added [Configuration Service] . . . . .	76
UMTS - support for Huawei E630 UMTS card (serial numbers with EE) added [Configuration Service] . . . . .	76
VPN configuration - Client to Site - Phion VPN CA - Pool Licences - parameter VPN-Type added [VPN] . . . . .	214
VPN configuration - L2TP settings - parameters for IPsec Phase 1 Lifetime added [VPN] . . . . .	211
VPN configuration - Server Certificates - Advanced - parameter IPsec Log Level added [VPN]. . . . .	208
VPN configuration - Server Certificates - Advanced - parameter Use IPsec dynamic IP added [VPN]. . . . .	208
VPN GTI - TINA tab - section General Settings - parameter Hide in netfence VPN World added [phion management centre]. . . . .	467
VPN GTI - Tunnel info - tunnel configuration dialogue - checkbox Hide in netfence VPN World added [phion management centre] . . . . .	469
<b>4.2.0 Note</b>	
Configuring IPsec Tunnels - example Cisco Pix removed (moved to documentation phion netfence IPsec Configuration) [VPN] . . . . .	226
Configuring IPsec Tunnels - Note on documentation phion netfence IPsec Configuration added [VPN] . . . . .	226
Example - table Relationship between Local and Partner networks corrected [VPN] . . . . .	239
Global Domain Parameters - Note on parameter Default Recipient DB added [Mail Gateway] . . . . .	247
Global Domain Parameters - Note on parameter Default Recipients Lookup added [Mail Gateway] . . . . .	247
Global Domain Parameters - Note on parameter Default Recipients Lookup using LDAP or MSAD added [Mail Gateway]. . . . .	247
How to make a phion M appliance centrally manageable - Step 4 - licence name corrected [Appendix] . . . . .	529
IPsec tunnels - parameter Local Address - Note on working with dynamic IPs added [VPN]. . . . .	227
Log Cycling - parameter Range IDs added [Configuration Service]. . . . .	104
Log Cycling - section File Specific Settings revised (naming) [Configuration Service] . . . . .	104
Log Cycling - section Log Cycling Actions revised (naming) [Configuration Service] . . . . .	104
MC Control Centre - Software Update tab - Buttons Lock and Save Group moved to the Action bar [phion management centre]. . . . .	405
MC Control Centre - Software Update tab - Note on character restrictions for group name added [phion management centre]. . . . .	406
MC Control Centre - Software Update tab - Note on group edit rights added [phion management centre] . . . . .	406
MC Control Centre - Software Update tab - Note on group scope and moving ranges, cluster, and boxes added [phion management centre] . . . . .	406
MC Control Centre - Software Update tab - Views - Note on Admin scope added. [phion management centre]. . . . .	406
MC Syslog Server configuration - Relay Filters - section Data Selection - parameter Box Log Pattern revised [phion management centre]. . . . .	451
netfence Management Centre renamed to phion management centre [phion management centre]. . . . .	387
Network tab - Interface/IP - Not all UMTS cards support the signal strength feature [Control Centre] . . . . .	31
Note on clipboard function restriction added [Configuration Service] . . . . .	49
Note on two proxy instances at one box added (configure different ports) [Proxy] . . . . .	324
phion.i - Local administration rights are needed to install files on a USB stick [Getting Started]. . . . .	10
phion.i - restrictions on Kernel parameter field added [Getting Started]. . . . .	13
phion.i - restrictions on parameter No ACPI added [Getting Started]. . . . .	14
Server Configuration (single box) - Note on parameter Enable Monitoring on Secondary added [Configuration Service] . . . . .	95
Service configuration - view Statistic Transfer revised (naming) [Statistics] . . . . .	301
Setting up the box - Connection Monitoring - Note on parameter Monitoring Method ICMP added [Configuration Service] . . . . .	78
Setting up the box - Networks - DHCP Routing - Note on parameter Own Routing Table added [Configuration Service] . . . . .	74
Setting up the box - Networks - ISDN Routing - Note on parameter Own Routing Table added [Configuration Service]. . . . .	76
Setting up the box - Networks - UMTS - parameter Inbound SMS Handling removed [Configuration Service]. . . . .	76
Setting up the box - Networks - UMTS Routing - Note on parameter Own Routing Table added [Configuration Service]. . . . .	77
Setting up the box - Networks - xDSL Routing - Note on parameter Own Routing Table added [Configuration Service] . . . . .	72
Setting up the box - xDSL setup - connection stop script corrected [Configuration Service] . . . . .	71
Spam Filter Settings - Online Tests - Note on parameter Use Black List Tests added [Mail Gateway]. . . . .	260
Spam Filtering - Only netfence spamfilter services may be used as spam engines [Mail Gateway] . . . . .	259
Spamfilter Config - to disable the function Use Black List Tests create a rule [Mail Gateway] . . . . .	260
SSH Proxy configuration - description for parameter Idle Mode corrected [SSH Gateway]. . . . .	365
SSL Settings - Note on parameters Root CA Private Key / Root CA Certificate added [Proxy]. . . . .	338
Standard Log Files - box_Firewall.log - tunnel and transport is only visualized on active kernel rule set [Firewall]. . . . .	179
Statistics Cook Settings - section Cook Settings revised (naming) [phion management centre] . . . . .	438
Statistics Cook Settings - section Statistics Cooking revised (naming) [phion management centre]. . . . .	438
Tracing connections - Note regarding trace conditions for local traffic revised [Firewall]. . . . .	178
Tracing connections - Note regarding trace conditions revised [Firewall]. . . . .	177
VPN configuration - Server Certificates - Advanced - parameter IKE Dead Peer Detection Interval renamed [VPN]. . . . .	208
VPN configuration - Server Certificates - Advanced - parameter IKE Exchange Timeout renamed [VPN] . . . . .	208
VPN configuration - Server Certificates - Advanced - parameter IKE Tunnel Check Interval renamed [VPN] . . . . .	208
VPN GTI settings - parameter My Peer Type - data will be used for both partners (active/passive) of the VPN tunnel [VPN]. . . . .	210

# 11. phion Lizenzbedingungen / phion License Conditions

## 11.1 phion Lizenzbedingungen

### §1 Präambel

- (1) phion AG, Eduard-Bodem-Gasse 1, 6020 Innsbruck, FN: 184392 s (im folgenden kurz "phion" genannt), hat die Software "phion netfence", "phion airlock", "phion management centre" und dazugehörige Software (künftig kurz als "Software" bezeichnet) entwickelt. phion ist Inhaber aller sich aus dem Urheberrecht an der Software ergebenden Leistungsschutz- und Nutzungsrechte an dieser Software.
- (2) Die Software läuft teilweise auf dem mitgelieferten Betriebssystem Linux mit den von phion vorgenommenen Änderungen. Das Betriebssystem und die mitgelieferten Softwarepakete unterliegen eigenen Lizenzen und sind nicht Gegenstand dieser Nutzungsbedingungen. Diese Lizenzen sind teilweise Open Source Lizenzen und es wird daher ausdrücklich festgehalten, dass phion keinerlei Haftung für diese Software übernimmt. Es wird ausdrücklich festgehalten, dass die Software keine Bearbeitung oder Weiterentwicklung des Betriebssystems Linux ist. Die gegenständlichen Nutzungsbedingungen betreffen somit ausschließlich die von phion entwickelte Software.
- (3) Die phion Software wurde unter Einbeziehung einiger bestehender Softwarepakete entwickelt. Die Lizenzbedingungen dieser Software finden sich als Anhang.

### §2 Test der Software

- (1) Die Software "phion netfence" und "phion management centre" ist zu Evaluierungszwecken auf einer CD erhältlich. Die Software auf dieser CD kann kostenlos genutzt und getestet werden. Die Software ist als Evaluierungsversion nicht für den Gebrauch als Netzwerksicherheitssoftware geeignet. Ohne License-Key ist das System vollständig offen für nicht autorisierte Administration. Mit Hilfe des öffentlich bekannt gemachten Passworts "phion" kann das Evaluierungssystem ohne Einschränkungen administriert werden. phion übernimmt keinerlei Haftung für Schäden, die aus der Nutzung der Evaluierungsversion entstehen. Der Einsatz in einer produktiven Umgebung ist untersagt, es sei denn der Kunde erwirbt mittels beiliegendem Bestellformular ein Lizenz-Zertifikat für die Software. Der Erwerb des Lizenz-Zertifikats berechtigt den Kunden, die Software unter Einhaltung dieser Nutzungsbedingungen zeitlich unbegrenzt weiter zu verwenden. Sollte sich der Kunde nicht zum Kauf des Lizenz-Zertifikats entschließen, so ist er auf Wunsch von phion verpflichtet, die Test-CD sowie alle Kopien der Software zu vernichten und auf Wunsch von phion einen entsprechenden Nachweis darüber zu erbringen.
- (2) Es ist ohne schriftliche Genehmigung von phion nicht erlaubt, Ergebnisse der Evaluation oder Produktbeurteilungen zu veröffentlichen.

### §3 Benutzung

- (1) phion gewährt dem Kunden ab der Ausstellung des Lizenz-Zertifikats unter der Bedingung der rechtzeitigen Bezahlung der Lizenzgebühren, auf unbeschränkte Zeit ein nicht ausschließliches Recht zur Installation und Nutzung des Programmes auf einem Datenspeicher. Die Lizenz bezieht sich ausschließlich auf die Nutzung des Programmes durch den Kunden für seine eigenen Datenverarbeitungsprozesse. Der Kunde ist nicht berechtigt, Dritten Zugang zum Programm zu gewähren. Der Kunde verpflichtet sich, die Software gesichert aufzubewahren, sodass ein Zugang und somit ein Kopieren oder Benutzen der Software durch Dritte verhindert wird. Der Kunde erhält das Recht, ausschließlich für sicherungs- oder archivarische Zwecke Kopien des Programmes anzufertigen.
- (2) Der Kunde ist berechtigt das Programm in dem Umfang zu nutzen wie es für die gewöhnliche Nutzung des Programmes erforderlich ist.
- (3) Soweit durch zwingende gesetzliche Vorschriften nicht anderwärtig vorgesehen, ist der Kunde nicht berechtigt, das Programm vom Objektcode zum Quellcode (z.B. durch "Reverse Engineering", Disassemblierung oder Dekompilierung) zu übersetzen.
- (4) Der Kunde ist nicht berechtigt, den Licence-Key aufzubrechen oder zu ändern. Er ist nicht berechtigt, irgendwelche Hinweise im Bezug auf Rechte, Marken oder Ähnlichem, die in dem Programm oder auf dem Medium, auf dem das Programm enthalten ist, angegeben werden, zu verändern, oder zu löschen.
- (5) Der Kunde ist nicht berechtigt, das Programm an Dritte zu übertragen, zu vermieten, zu verleasen, zu verleihen oder auf andere Weise Dritten vorübergehend zur Verfügung zu stellen. Er ist darüber hinaus nicht berechtigt, die Software auf irgendeine Weise zu bearbeiten, zu verändern, oder in andere Computerprogramme zu integrieren.
- (6) Die Lizenz kann über einen Licence-Key an die Hardwarekonfiguration gebunden sein. Bei Änderungen der Hardwarekonfiguration, steht es

phion frei, dem Kunden kostenlos einen weiteren Licence-Key auszustellen. Der Kunde verliert damit das Recht, den ersten Licence-Key weiter zu benutzen. phion ist berechtigt, darüber den Nachweis binnen 14 Tagen nach Erhalt des neuen Licence-Keys zu verlangen.

- (7) Teilweise begrenzen die Lizenzen und Licence-Keys die Anzahl der IP-Adressen, die die Software benutzen. Es ist dem Lizenznehmer untersagt, netzwerktechnische Mittel zum Zweck der Reduzierung der Anzahl der IP-Adressen, die die Firewall benutzen, einzusetzen. Dies betrifft nicht den Einsatz von Application Gateways wie http-Proxies und DNS Forwardern, sondern beispielsweise applikationsunabhängige NAT-Devices, deren primärer Zweck es ist, die IP-Adressen-Zahl an der Firewall zu minimieren.
- (8) Werden aus technischen Gründen dennoch solche Devices eingesetzt, so ist der Lizenznehmer verpflichtet, die Lizenz so zu dimensionieren, dass die Software auch ohne ein solches Device korrekt lizenziert ist.
- (9) Das Produkt "sectorwall" ist ausschliesslich für den Einsatz als Security Gateway innerhalb von Anwendernetzwerken lizenziert und nicht für den Einsatz als Security Gateway zum Internet erlaubt. Es ist daher nicht erlaubt, eine "sectorwall" am Perimeter zum Internet einzusetzen.
- (10) Teilweise begrenzen die Lizenzen und Licence-Keys die Anzahl der Applikationen und Authentisierungsmethoden. Ergreift der Lizenznehmer Maßnahmen, diese Begrenzungen zu umgehen, begeht er damit eine schwere Verletzung dieser Lizenzbedingungen.
- (11) Der Export in Drittländer hat nach den zum Zeitpunkt des Exports/Imports jeweils gültigen EU-Richtlinien stattzufinden. Die alleinige Verantwortung zur Einhaltung dieser Richtlinien liegt beim exportierenden bzw. importierenden Reseller oder Endkunden. Von phion gelieferte Produkte sind zur Benutzung und zum Verbleib innerhalb der EU bestimmt. Die Wiederausfuhr - einzeln oder in systemintegrierter Form - ist für den Kunden genehmigungspflichtig und unterliegt dem jeweiligen Außenwirtschaftsrecht sowie den US Export Regulations, deren Kenntnis und Beachtung dem Kunden obliegt. Der Wiederverkauf an Kunden im nuklearen Bereich, insbesondere im Bereich der Herstellung und des Betriebs von Nukleartechnik, erfordert spezielle Genehmigungen. phion behält sich das Recht vor, die gegenständlichen Bestimmungen zum Export und Import jederzeit anzupassen, sofern es die nationale oder internationale Gesetzgebung erfordert.
- (12) Lizenzen, die auf Hardwareparameter gebunden sind, können auch auf virtuellen Maschinen eingesetzt werden. In diesem Fall kann der Hardwareparameter ein Parameter der virtuellen Maschine sein. In diesem Fall ist das gleichzeitige Betreiben von mehreren virtuellen Instanzen mithilfe desselben Lizenzzertifikats untersagt. Die Einräumung der Möglichkeit zur Nutzung der Lizenz durch Dritte durch Weitergabe von kompletten Systemimages der virtuellen Maschine an Dritte ist nicht zulässig.
- (13) Die Verantwortung für die Auswahl, die Installation und den Gebrauch des Lizenzmaterials und die durch den Einsatz angestrebte Problemlösung liegt beim Lizenznehmer. Der Lizenznehmer ist zudem für Auswahl, Gebrauch und Unterhalt der im Zusammenhang mit der Software eingesetzten Informatiksysteme, weiterer Programme und Datensysteme sowie die dafür erforderlichen Dienstleistungen zuständig und stellt die für den Einsatz der Software geeignete Organisation bereit.
- (14) Der Lizenzgeber hat das Recht, sich unter Wahrung der Geschäfts- und Betriebsgeheimnisse des Lizenznehmers von der Einhaltung des bestimmungsgemäßen Gebrauchs der Software zu überzeugen.

### §4 Kaufpreis

- (1) Wenn im Vertriebsweg nichts anderes vereinbart wird, gilt folgende Regelung:  
Der Kaufpreis für das Computerprogramm samt Lizenz-Zertifikat ist innerhalb von 14 Tagen nach der Auslieferung des Lizenz-Zertifikats, ohne dass es einer weiteren Rechnungslegung für die Fälligkeit des Kaufpreises bedarf, auf das Geschäftskonto von phion zu überweisen. Gerät der Kunde mit der Bezahlung des Kaufpreises in Verzug, ist phion berechtigt, Verzugszinsen in Höhe von 8 Prozent über dem jeweils gültigen Dreimonats-EURIBOR per annum zu berechnen.

### §5 Haftungsbestimmungen

- (1) Einvernehmlich festgehalten wird, dass dem Kunden die Software auf einem Datenträger oder als Download zur Verfügung gestellt wurde. Der Kunde verpflichtet sich, die Funktionsfähigkeit und Mängelfreiheit der zur Verfügung gestellten Software während einer Testphase zu überprüfen und allfällige Mängel analog zu § 377 UGB zu rügen. Mit der Bestellung des Lizenz-Zertifikats gemäß dem Bestellformular, bestätigt der Kunde die Überprüfung der Software und eventuell des Datenträgers auf ihre Mängelfreiheit und bestätigt diese. Einvernehmlich wird für die Testphase in Hinblick auf deren

Testcharakter die Gewährleistung für Sachmängel ausgeschlossen. In jedem Falle ist die Gewährleistung auf sechs Wochen beschränkt.

- (2) Für Konsumenten beträgt die Gewährleistungsfrist zwei Jahre. Die Bestimmungen des Konsumentenschutzgesetzes bleiben in Geltung, soweit es sich um ein Geschäft mit Endverbrauchern handelt. In diesem Fall ist phion berechtigt, ihre Gewährleistungsverpflichtungen durch Austausch der gelieferten Sache zu erfüllen.
- (3) Ferner übernimmt phion keine Gewähr für Fehler, Störungen oder Schäden, die auf unsachgemäße Bedienung, Verwendung ungeeigneter Organisationsmittel, anomale Betriebsbedingungen (insbesondere Abweichungen von den Installationsbedingungen) sowie auf Transportschäden zurückzuführen sind. Für Programme, die durch eigene Programmierer des Kunden bzw. Dritte nachträglich verändert werden, entfällt jegliche Gewährleistung durch phion.
- (4) phion sind keine Rechte Dritter bekannt, die der Einräumung der gewährten Nutzungsrechte an der Software entgegenstehen. Wird der Kunde wegen Verletzung von Immaterialgüterrechten Dritter aufgrund der Nutzung der von phion gelieferten Software oder von Teilen oder Komponenten davon in Anspruch genommen, wird phion den Kunden schad- und klaglos halten, wenn der Kunde phion den Sachverhalt unverzüglich anzeigt und phion alle Verhandlungen überlässt. Der Kunde ist nicht befugt, diesbezüglich irgendwelche Anerkennungserklärungen abzugeben. Der Kunde bevollmächtigt phion zu seiner Vertretung im Bezug auf diesbezügliche Streitigkeiten und verpflichtet sich gemeinsam mit phion geeignete Schritte für die Abwehr der geltend gemachten Ansprüche zu ergreifen.
- (5) Für den Fall, dass berechnigte Ansprüche Dritter geltend gemacht werden, wird phion die notwendigen Vorkehrungen treffen und allenfalls die Rechte erwerben, oder gleichwertige Teile und Komponenten liefern.
- (6) phion haftet für Schäden, sofern ihr oder ihren Mitarbeitern Vorsatz oder grobe Fahrlässigkeit nachgewiesen werden, im Rahmen der gesetzlichen Vorschriften. Die Haftung für leichte Fahrlässigkeit wird einvernehmlich und im gesetzlich zulässigen Ausmaß ausgeschlossen. Der Ersatz von Folgeschäden und Vermögensschäden, nicht erzielten Ersparnissen, Zinsverlust, indirekten Schäden und von Schäden aus Ansprüchen Dritter jeglicher Art gegen phion ist in jedem Fall ausgeschlossen. phion haftet nicht für Schadenersatz bei Daten-, Software- oder Hardwarezerstörung, wenn der Kunde seinen Pflichten zum ordnungsgemäßen EDV-Betrieb und der regelmäßigen Datensicherung nicht bzw. nicht ausreichend nachgekommen ist. Schadenersatzansprüche gegen phion sind, sofern es sich beim Vertragspartner nicht um einen Konsumenten handelt, bei sonstigem Verfall binnen eines Jahres ab Schadenseintritt gerichtlich geltend zu machen.

#### §6 Programmverbesserungen (Updates) und Programmänderungen

- (1) Der Kunde erwirbt mit dem Lizenz-Zertifikat keinerlei Recht auf weitergehende Betreuung durch phion sowie auf die Lieferung von Updates oder Programmweiterungen.
- (2) Selbst wenn die Software keine Lizenzverletzung anzeigt, ist das Update von Systemen, deren Software Subscription nicht mehr aktuell ist, eine schwere Lizenzverletzung und der Kunde ist verpflichtet, Software Subscription, wie in den Software Subscription Bedingungen beschrieben, nachzukaufen.

- (3) Manche Funktionalitäten, vor allem Updates von Content Security Patterns oder ähnlichen Komponenten, die regelmäßig auf den neuesten Stand gebracht werden, stehen nur bei aufrechten Subscriptionrechten zur Verfügung.

#### §7 Kundendaten

- (1) Der Kunde erklärt sich ausdrücklich damit einverstanden, dass ihm betreffende Daten, die phion im Rahmen der Geschäftsverbindung mit dem Kunden bekannt werden, von phion zum Zweck der Benachrichtigung über die Entwicklung von Updates und neuen Programmversionen und zum Angebot von Wartungsverträgen und weitere Angeboten gesammelt und bearbeitet werden.
- (2) Der Kunde nimmt zustimmend zur Kenntnis, dass seine persönlichen Daten von phion zum Zwecke der internen Datenerfassung, Datenverarbeitung und zur Benachrichtigung über die Entwicklung im Zusammenhang mit dem gelieferten Produkt und von Updates und neuen Programmversionen gespeichert und verarbeitet werden. Der Kunde erklärt sich gemäß § 107 TKG ausdrücklich damit einverstanden, derartige Benachrichtigungen auch per email zu empfangen.

#### §8 Urheberrechtlicher Schutz der Software

- (1) Der Kunde nimmt ausdrücklich zur Kenntnis, dass phion Inhaber sämtlicher sich aus dem Urheberrecht ergebender Leistungsschutz- und Nutzungsrechte ist. Im Falle des Verstoßes des Kunden gegen diese Rechte und sonstige zwingende urheberrechtliche Bestimmungen, stehen phion sämtliche im Urheberrechtsgesetz vorgesehenen Rechtsbehelfe zur Verteidigung des urheberrechtlichen Schutzes zu.
- (2) Teile der Software enthalten von Dritten entwickelte Software, die urheberrechtlichen Schutz genießt. Diese Softwarelizenzbestimmungen sind im Anhang dieser Nutzungsbestimmungen angeführt und stellen einen integrierenden Bestandteil dieser Bestimmungen dar.

#### §9 Schlussbestimmungen

- (1) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder unwirksam werden, so wird hierdurch der übrige Teile des Vertrages nicht berührt. Die Vertragspartner werden partnerschaftlich zusammenwirken um eine Regelung zu finden, die den unwirksamen Bestimmungen möglichst nahe kommt.
- (2) Soweit nicht zwingende gesetzliche Bestimmungen entgegenstehen, gelten die zwischen Vollkaufleuten zur Anwendung kommenden gesetzlichen Bestimmungen nach österreichischem Recht, auch dann, wenn der Auftrag im Ausland ausgeführt wird.
- (3) Für eventuelle Streitigkeiten gilt ausschließlich die örtliche Zuständigkeit des sachlich zuständigen Gerichtes in Innsbruck als vereinbart; ist der Kunde Verbraucher im Sinne des KSchG, dessen allgemeiner Gerichtsstand..
- (4) Es wird die Anwendbarkeit ausschließlich österreichischen Rechtes, mit Ausnahme sowohl des UN-Kaufrechts (Vienna Convention on the Sale of Goods) als auch der Verweisungsnormen des Internationalen Privatrechts (IPRG) vereinbart.
- (5) Andere Softwarepakete, die auf der CD enthalten sind, stehen noch unter anderen Lizenzen wie der GPL (GNU General Public License) oder BSD Lizenzen. Diese fallen nicht unter die phion Nutzungsbedingungen. Sie werden unten angeführt.



## 11.2 phion License Conditions

### §1 Preamble

- (1) phion AG, Eduard-Bodem-Gasse 1, 6020 Innsbruck, FN [Business Register Number] 184392 s (hereinafter referred to as "phion") has developed the software "phion netfence", "phion airlock", "phion management centre" and associated software (hereinafter referred to as "Software"). phion is the owner of all proprietary rights to and rights to use the Software which result from the copyright to the Software.
- (2) The Software runs on the operating system Linux which is delivered together with the software. The operating system and the software packages provided along with it are subject to separate licenses and shall not be the subject matter of these Terms and Conditions of Use. It is expressly put on record that the Software does not constitute an edited version or further development of the operating system. These Terms and Conditions of Use therefore exclusively apply to the Software developed by phion.
- (3) The phion Software was developed by inclusion of some existing software packages to which rights of third parties exist. The licensing conditions regarding that software are attached hereto.

### §2 Testing of the Software

- (1) The Software "phion netfence" and "phion management centre" is available for evaluation purposes. The Software may be used and tested free of charge. In its evaluation version it is NOT usable as a software for network security purposes. Without a license key the system is open for non-authorised administration. The publicly known password "phion" warrants administrative access to anyone. The usage of a non-licensed system for productive purposes is strictly forbidden. PHION SHALL NOT BE LIABLE FOR ANY DAMAGE WHICH IS CAUSED BY RUNNING A SYSTEM IN EVALUATION MODE. If Customer does not purchase a license, Customer is obliged to delete all copies of the software and phion is entitled to proof it.
- (2) It is not allowed to publish any results of evaluations without prior written permission by phion.

### §3 Use

- (1) Subject to timely payment of the license fees phion shall grant Customer an exclusive right to install and use the programme on a data storage device from issuance of the license certificate for an indefinite period of time. The license exclusively concerns the use of the programme by Customer for its own data processing processes. Customer shall not be entitled to grant third parties access to the programme. Customer undertakes to keep the Software safe so that access and, thus, copying or using the Software by third parties is prevented. Customer shall be granted the right to make copies of the programme exclusively for backup or archiving purposes.
- (2) Customer shall be entitled to use the programme to the extent necessary for ordinary use of the programme.
- (3) Unless provided otherwise by mandatory statutory provisions, Customer shall not be entitled to translate the programme from object code into source code (e.g. by reverse engineering, disassembling or decompiling).
- (4) Customer shall not be entitled to crack or change the license key. Customer shall not be entitled to modify or delete any notes regarding rights, trademarks or the like which are stated in the programme or on the medium on which the programme is stored.
- (5) Customer shall not be entitled to transfer, let, lease, lend or otherwise temporarily make available the programme to third parties. Moreover, Customer shall not be entitled to process or modify the Software in any way or to integrate it into other computer programmes.
- (6) The license may be linked to the hardware configuration via a license key. In the case of modifications of the hardware configuration phion shall be free to issue another license key to Customer free of charge. Customer shall then lose the right to continue to use the first license key. phion shall be entitled to request evidence thereof within fourteen days of receipt of the new license key.
- (7) Some licences and license keys may restrict the number of IP addresses that are allowed to use the software. It is forbidden to use technical methods to reduce the number of counted IP-addresses. This does not affect the usage of application proxies such as http-proxies or DNS-forwarders or mail-relays, but only NAT-devices with the primary purpose is to hide IP-addresses.
- (8) If such devices are used nonetheless for technological reasons, the licensee shall be obliged to dimension the license in such a way that the Software is correctly licensed also without such a device.
- (9) The product "sectorwall" is licensed solely for usage as a security gateway between internal parts of a licensee's network. It is strictly forbidden to use a "sectorwall" product at the internet perimeter.
- (10) Some licenses and license keys may restrict the number of protected applications or/and users or/and authentication facilities that are allowed to use the software.

- (11) Export to third countries shall be effected in accordance with the EU directives applicable at the time the export/import takes place. The exporting and/or importing reseller or end customer shall be solely responsible for compliance with the said directives. Products delivered by phion are designed for being used and for remaining in the EU. Re-export, be it separately or integrated into a system, shall be subject to approval to be obtained by Customer and shall be subject to the relevant foreign trade legislation and to US Export Regulations for the knowledge of and compliance with which Customer shall be responsible. Reselling to customers in the nuclear area, in particular in the area of manufacturing and operation of nuclear technology, shall require special permits. phion reserves the right to adjust the provisions on export and import at any time if national or international legislation so requires.
- (12) Licenses bound to hardware configuration may also be used on virtual machines. In this case the hardware configuration may be a hardware configuration of the virtual machine. If the license is bound to a hardware parameter of a virtual machine, customer shall not simultaneously operate multiple virtual machine instances using the same license key at the same time. Allowing and/or enabling a third party to operate a virtual machine image by passing on virtual machine images is not permitted.
- (13) The Customer is responsible for the choice, installation and usage of the licensed Software and the intended solution. The Customer is responsible for usage and choice of the technological environment and the necessary services and the organisation to operate the systems properly.
- (14) The Customer has the right to get evidence that the licensed Software is used according to the license conditions. phion has to do this without breaching any industrial and company secrets of the Customer.

### §4 Purchase Price

- (1) Unless otherwise agreed in the course of distribution, the following regulation shall apply:  
The purchase price for the computer programme including the license certificate shall be transferred to the company account of phion within fourteen days of delivery of the license certificate without another invoice for the due purchase price being necessary. If Customer is in default of payment of the purchase price, phion shall be entitled to charge default interest at a rate of 8 % p.a. above the three-months EURIBOR applicable from time to time.

### §5 Liability Provisions

- (1) THE PARTIES MUTUALLY AGREE AND PUT ON RECORD THAT THE SOFTWARE SHALL BE PROVIDED TO CUSTOMER ON A DATA CARRIER OR AS A DOWNLOAD. CUSTOMER UNDERTAKES TO CHECK WORKABILITY AND FREEDOM FROM DEFECTS OF THE PROVIDED SOFTWARE DURING A TEST PHASE AND TO NOTIFY ANY DEFECTS IN ACCORDANCE WITH SECTION 377 UGB [AUSTRIAN BUSINESS CODE]. UPON ORDERING THE LICENSE CERTIFICATE IN ACCORDANCE WITH THE PURCHASE ORDER FORM CUSTOMER CONFIRMS THAT THE SOFTWARE AND THE DATA CARRIER, IF ANY, HAVE BEEN CHECKED FOR FREEDOM FROM DEFECTS AND CONFIRMS THAT FREEDOM FROM DEFECTS EXISTS. WARRANTY FOR DEFECTS IN QUALITY DURING THE TEST PHASE SHALL BE EXCLUDED BY MUTUAL CONSENT IN VIEW OF THE TESTING CHARACTER. IN ANY CASE WARRANTY SHALL BE LIMITED TO SIX WEEKS.
- (2) FOR CONSUMERS THE WARRANTY PERIOD SHALL BE TWO YEARS. THE PROVISIONS OF THE AUSTRIAN CONSUMER PROTECTION ACT SHALL REMAIN IN FORCE TO THE EXTENT THAT A TRANSACTION WITH END CONSUMERS IS CONCERNED. IN THAT CASE PHION SHALL BE ENTITLED TO FULFIL ITS WARRANTY OBLIGATIONS BY REPLACING THE DELIVERED ITEM.
- (3) FURTHERMORE PHION SHALL ASSUME NO WARRANTY FOR ERRORS/BUGS, FAILURES OR DAMAGE WHICH WERE CAUSED BY IMPROPER OPERATION, USE OF UNSUITABLE ORGANISATIONAL RESOURCES, ABNORMAL OPERATING CONDITIONS (IN PARTICULAR DEVIATIONS FROM THE INSTALLATION CONDITIONS) AS WELL AS BY TRANSPORTATION DAMAGE. IN THE CASE OF PROGRAMMES WHICH ARE SUBSEQUENTLY CHANGED BY PROGRAMMERS WORKING FOR THE CUSTOMER OR THIRD PARTIES, PHION SHALL BE UNDER NO WARRANTY WHATSOEVER.
- (4) phion is not aware of any rights of third parties which would prevent the granting of the rights to use the Software granted. If Customer is held liable for infringement of intellectual property rights of third parties due to use of the Software delivered by phion or of parts or components thereof, phion shall indemnify and hold Customer harmless provided that Customer immediately notifies such fact to phion and leaves all negotiations to phion. Customer shall not be allowed to issue any declarations of acknowledgement in this context. Customer shall authorise phion to represent Customer with regard to such disputes and undertakes to take suitable steps jointly with phion in defence of the asserted claims.
- (5) In the case that justified claims of third parties are asserted, phion shall take the necessary steps and, if necessary, acquire rights or deliver equivalent parts and components.
- (6) PHION SHALL BE LIABLE FOR DAMAGE WITHIN THE SCOPE OF THE STATUTORY PROVISIONS IF IT CAN BE PROVEN THAT SUCH DAMAGE

WAS CAUSED BY PHION OR ITS STAFF WILFULLY OR WITH GROSS NEGLIGENCE. LIABILITY FOR ORDINARY NEGLIGENCE SHALL BE EXCLUDED BY MUTUAL AGREEMENT AND TO THE EXTENT PERMITTED BY LAW. COMPENSATION FOR CONSEQUENTIAL DAMAGE AND PECUNIARY LOSS, SAVINGS NOT EARNED, LOSS OF INTEREST, INDIRECT DAMAGE AND FOR DAMAGE FROM THIRD-PARTY CLAIMS OF ANY KIND AGAINST PHION SHALL BE EXCLUDED IN ANY CASE. PHION SHALL NOT BE LIABLE FOR DAMAGES IN CASE OF DESTRUCTION OF DATA, SOFTWARE OR HARDWARE IF CUSTOMER DID NOT FULFIL OR DID NOT SUFFICIENTLY FULFIL ITS OBLIGATIONS OF OPERATING THE EDP PROPERLY AND TO MAKE TIMELY DATA BACKUPS, UNLESS THE CONTRACTING PARTY IS A CUSTOMER, CLAIMS FOR DAMAGES AGAINST PHION SHALL BE ASSERTED WITHIN ONE YEAR OF OCCURRENCE OF THE DAMAGE; OTHERWISE THEY SHALL FORFEIT.

#### §6 Enhancements of Programmes (Updates) and Modifications of Programmes

- (1) BY PURCHASING THE LICENSE CERTIFICATE CUSTOMER SHALL NOT ACQUIRE ANY RIGHT TO FURTHER SUPPORT BY PHION OR TO DELIVERY OF UPDATES OR PROGRAMME EXTENSIONS.
- (2) Using Software Updates on systems where no valid software subscription was purchased is severe infringement of license rights, even the software does not prove the validity of the right to update. The customer is due to purchase the needed Software Subscription as described in the Software Subscription conditions.
- (3) Some functionality may be available only if a valid Software Subscription has been purchased. This is especially the case for content security and similar components which are updated on a regular basis.

#### §7 Customer Data

- (1) Customer expressly agrees that data concerning the Customer which becomes known to phion within the scope of the business relationship with Customer shall be collected and processed by phion for the purpose of information about the development of updates and new programme versions and for offering of maintenance contracts and for other offers.
- (2) Customer acknowledges and agrees that its personal data be stored and processed by phion for the purpose of internal data collection, data processing and for information about the development in connection with the delivered product and of updates and new programme versions. In accordance with Section 107 TKG [Austrian Telecommunications Act] Customer expressly agrees to receipt of such information also by e-mail.

#### §8 Copyright of Software

- (1) Customer expressly acknowledges that phion is the owner of all proprietary rights and rights to use the Software which result from copyright. In case Customer violates such rights and other mandatory copyright provisions, phion shall be entitled to all legal remedies which are provided for under copyright law to defend copyrights protection.
- (2) Parts of the Software contain software developed by third parties which is under copyright protection. Those licensing conditions for software are contained in the Annex to these Terms and Conditions of Use and shall form an integral part hereof.

#### §9 Final Provisions

- (1) If individual provisions of this contract are or become ineffective, the remaining provisions of this contract shall not be affected. The contracting parties shall cooperate as partners in order to find a provision which comes as close as possible to the ineffective provisions.
- (2) Unless mandatory statutory provisions provide otherwise, the statutory provisions of Austrian law applicable to full merchants shall exclusively apply, even if the order is rendered abroad.
- (3) The court having jurisdiction over the subject matter and over Innsbruck shall have exclusive jurisdiction regarding any disputes; if Customer is a consumer as defined by the Austrian Consumer Protection Act, Customer's general place of jurisdiction shall be the legal venue.
- (4) Austrian law shall apply exclusively; UN Sales Law (Vienna Convention on Contracts for the International Sale of Goods) and the conflict of laws rules of the Austrian Statute on Private International Law (IPRG) shall be excluded.
- (5) The delivered software includes software packages which are subject to different types of licenses like GPL or BSD. These are not subject to this license condition and are listed below.

## 11.3 Anhang / Addendum

Lizenzbedingungen von Software, die ganz oder in Teilen in phion netfence verwendet wurden / Terms and Conditions of Licensing of software which is used in phion netfence in whole or in part:

**Table 23-157** Conditions of Licensing of software which is used in phion netfence

Software name	Function	see...
AdoDB	PHP database abstraction layer	page 608
AntiVir	Antivirus	page 609
Apache	Apache Web Server	page 610
Berkeley DB	Database tools	page 611
bind	DNS service	page 611
Broadcom Corporation	Linux driver	page 612
DHCP Relay/DHCP Enterprise	DHCP Relay Agent	page 612
ISAKMP	IPSec engine	page 612
ISS Proventia Web Filter	URL filter	page 612
Microdasys	HTTPS Proxy engine	page 613
OpenLDAP	Authenticator	page 614
OpenSSH	Secure shell	page 615
OpenSSL	Encrypting tools	page 616
PHP	The PHP HTML-embedded scripting language	page 617
PHPMailer	PHP-Mailer-Class for sending SMTP mails	page 617
PostgreSQL	PostgreSQL client programs and libraries	page 617
PuTTY	SSH GUI Client	page 618
RipeMD160	Implementation of the RIPEMD160 hashing algorithm	page 618
SHA2	Implementation of the SHA-256 and SHA-512 hashing algorithm	page 618
SNMPD	SNMP service	page 618
SPAMAssassin	SPAM-Mail detection	page 619
TUN/TAP	Low level support for tunneling	page 619
Vortex and AXL	Library for message exchange	page 620
WinPcap	Trace and display EAP-packets within the entegra client	page 620
WPA Supplicant	802.1x EAP authentication	page 621

### 11.3.1 AdoDB

BSD Style-License  
=====

Copyright (c) 2000, 2001, 2002, 2003, 2004 John Lim  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the John Lim nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

#### DISCLAIMER:

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JOHN LIM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED



AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.2 AntiVir - End-user License Agreement (EULA)

Die im phion Antivirus Service (Software Modulname virscan) enthaltene ausführbare Software **AntiVir SAVAPI** und **AntiVir Webgate**, sowie die Dateien **antivir.gpg** und **antivir.vdf** sind urheberrechtlich geschützt für die Avira GmbH  
Tjark Auerbach  
Geschäftsführender Gesellschafter  
Lindauer Strasse 21 | D-88069 Tett nang  
www.avira.com  
- nachfolgend "Urheber" genannt -.

Der Lizenzgeber für das Softwaremodul virscan, welches oben genannte Software enthält, ist phion AG - nachfolgend Lizenzgeber genannt - als OEM-Integrator. Es kommen somit jedenfalls die allgemeinen Lizenzbestimmungen von phion zur Anwendung. Zusätzlich gelangen untenstehende Bestimmungen hinsichtlich der oben genannten Software der Avira GmbH zur Anwendung. Im Falle von Widersprüchlichkeiten der unten angeführten Bestimmungen mit Bestimmungen der allgemeinen Lizenzbedingungen von phion gelangen die hier angeführten Bestimmungen zur Anwendung.

Die unbefugte Vervielfältigung oder der unbefugte Vertrieb dieser Software oder von Teilen hiervon ist strafbar. Derartige Handlungen können sowohl straf- als auch zivilrechtlich verfolgt werden und schwere Strafen und Schadensersatzforderungen zur Folge haben. Der Lizenzgeber gestattet Ihnen - nachfolgend Lizenznehmer genannt - die Nutzung dieser Software im Rahmen der folgenden Lizenzbedingungen:

#### §1 Gegenstand der Lizenzeinräumung

- (1) Gegenstand des Vertrages ist das vorliegende Computerprogramm, bei der freigeschalteten Vollversion einschließlich der zur Freischaltung erforderlichen Lizenzdatei (die "Software").
- (2) Das Hauptprogramm ist vor Erwerb einer Lizenzdatei lediglich als eingeschränkte Testversion einsetzbar. Um alle Funktionen nutzen zu können, muss der Lizenznehmer eine Lizenzdatei beim Lizenzgeber oder einem autorisierten Händler erwerben. Die Übergabe der Lizenzdatei an den Lizenznehmer erfolgt durch Zusenden eines versiegelten Datenträgers oder auf Veranlassung des Lizenznehmers, sowie in sonstigen Fällen nach Wahl des Lizenzgebers, per Email. Die Dokumentation ist Teil der phion netfence Dokumentation und wird vom Lizenzgeber unabhängig von der Übergabeform der Software als Datei im allgemein üblichen PDF-Format zur Verfügung gestellt.
- (3) Die in der Dokumentation in ihrer Wirkungsweise beschriebene obige Software entspricht dem heutigen Stand der Technik. Der Lizenznehmer wird darauf hingewiesen, dass es nach dem heutigen Stand der Technik nicht möglich ist, Software so herzustellen, dass sie mit allen Anwendungen und in allen Kombinationen (insbesondere mit Software von Drittanbietern) in jedem Fall fehlerfrei arbeitet.
- (4) Die Software darf nicht in Gefahrenbereichen eingesetzt werden, die einen fehlerfreien Dauerbetrieb voraussetzen (Hoch-Risiko-Aktivitäten wie beispielsweise der Betrieb von Kernkraft-Einrichtungen, Waffensystemen, Luftfahrtnavigations- oder -kommunikationssysteme sowie lebenserhaltende Maschinen).

#### §2 Umfang der Benutzung

Der Lizenzgeber gewährt dem Lizenznehmer für die Dauer des Vertrages das einfache, nicht ausschließliche und persönliche Recht, die Software in dem vereinbarten Umfang - insbesondere hinsichtlich der Art und Anzahl der Rechner - zu nutzen (die "Lizenz"). Der Umfang der Lizenz kann der entsprechenden phion Lizenzdatei (x.509v3 kompatibles digitales Zertifikat) für das Softwaremodul entnommen werden, die der Lizenznehmer zusammen mit der Lizenzdatei erhält.

#### §3 Vervielfältigungsrechte und Weitergabe der Software

- (1) Es kommen die Bestimmungen des Punkts 2 der allgemeinen Lizenzbedingungen jedenfalls zur Anwendung.
- (2) Ist aus Gründen der Datensicherheit oder der Sicherstellung einer schnellen Reaktivierung des Computersystems nach einem Totalausfall die turnusmäßige Sicherung des gesamten Datenbestandes einschließlich der eingesetzten Programme unerlässlich und vorgesehen, darf der Lizenznehmer Sicherungskopien in der zwingend erforderlichen Anzahl herstellen. Die betreffenden Datenträger sind entsprechend zu kennzeichnen. Die Sicherungskopien dürfen nur zu rein archivierenden Zwecken eingesetzt werden.
- (3) Der Lizenznehmer ist verpflichtet, den unbefugten Zugriff Dritter auf die Software sowie die Dokumentation durch geeignete Vorkehrungen zu verhindern. Als Dritte gelten auch Tochtergesellschaften des

Lizenznehmers. Die Originaldatenträger sowie die Sicherungskopien sind an einem gegen den Zugriff Dritter gesicherten Ort aufzubewahren.

Die Mitarbeiter des Lizenznehmers sind nachdrücklich auf die Einhaltung der vorliegenden Vertragsbedingungen sowie der Bestimmungen des Urheberrechts hinzuweisen.

- (4) Dem Lizenznehmer ist es nicht gestattet,
  - a. mit Ausnahme der in dieser Vereinbarung ausdrücklich gestatteten Vervielfältigungen sonstige Reproduktionen der Software oder der Dokumentation ganz oder auszugsweise auf gleichen oder anderen Trägern zu fertigen, wozu auch die Ausgabe des Programmcodes auf einen Drucker zählt;
  - b. die Software von einem Computer über ein Netz oder einen anderen Datenübertragungskanal auf einen anderen Computer oder Empfangsgerät zu übertragen, sofern es sich auf der Empfängerseite nicht um einen Computer oder ein sonstiges Empfangsgerät des Lizenznehmers im Rahmen dieses Vertrages handelt;
  - c. ohne schriftliche Einwilligung des Lizenzgebers die Software abzuändern, zu übersetzen, zurückzuentwickeln, zu entkompilieren oder zu disassemblieren, von der Software abgeleitete Werke zu erstellen oder die Dokumentation, soweit dies im Rahmen der vertragsgemäßen Benutzung nicht zwingend erforderlich ist, zu vervielfältigen, zu übersetzen oder abzuändern oder von der Dokumentation abgeleitete Werke zu erstellen;
  - d. Urhebervermerke, Seriennummern sowie sonstige der Programmidentifikation dienende Merkmale zu entfernen, es sei denn der Lizenzgeber hätte dem zuvor schriftlich zugestimmt;
  - e. die Software an Dritte weiterzugeben oder Dritten in irgendeiner anderen Form zugänglich zu machen. Dies gilt auch für Reproduktionen der Software. Als Dritte gelten grundsätzlich auch Tochtergesellschaften des Lizenznehmers; eine Weitergabe der Software innerhalb der Unternehmensgruppe zur ausschließlichen Verwendung am neuen Einsatzort ist nach schriftlicher Zustimmung des Lizenzgebers, die nur aus wichtigem Grund verweigert werden darf, zulässig. In diesem Fall ist die Einhaltung des Umfangs der Benutzung gem. § 2 und § 3 und der sonstigen im vorliegenden Vertrag getroffenen Abreden und eventueller Nebenabreden sicherzustellen. Mit der Weitergabe hat der Lizenznehmer die Software und evtl. Sicherheitskopien am bisherigen Einsatzort innerhalb der Unternehmensgruppe unverzüglich und vollständig zu löschen.
  - f. die Software, die Dokumentation oder Teile hiervon Dritten im Wege der Vermietung oder des Leasings auf Zeit zu überlassen.

#### §4 Sonstige Rechte an der Software

Im Rahmen der Durchführung der vorliegenden Vereinbarung erfolgt ein Vollrechterwerb des Lizenznehmers nur an etwaigen körperlichen Datenträgern, auf denen die Software und die Dokumentation aufgezeichnet sind. Ein Erwerb von Verwertungs- bzw. Nutzungsrechten an der Software und der Dokumentation erfolgt nur insoweit, als dies in der vorliegenden Vereinbarung ausdrücklich vorgesehen ist. Der Lizenzgeber behält sich insbesondere alle Veröffentlichungs-, Vervielfältigungs-, Bearbeitungs-, Übersetzungs- und sonstigen Verwertungsrechte an der Software vor.

#### §5 Dauer des Vertrages und Kündigung

- (1) Der Lizenznehmer ist berechtigt, die Software und die Dokumentation auf unbestimmte Zeit zu nutzen.
- (2) Hiervon unberührt bleibt das Recht beider Parteien zur außerordentlichen Kündigung bei Vorliegen eines wichtigen Grundes. Insbesondere ist der Lizenzgeber bei erheblichen Verstößen gegen vertragliche Verpflichtungen durch den Lizenznehmer zur fristlosen Kündigung berechtigt.
- (3) Nach einer Kündigung ist der Lizenznehmer zur vollständigen Löschung der Software, insbesondere der Originaldatenträger, etwaiger Sicherungskopien und der auf seinem Rechnersystem installierten Dateien der Software sowie zur Rückgabe der Dokumentation verpflichtet. Der Lizenzgeber ist berechtigt, hinsichtlich dieser Löschung eine eidesstattliche Versicherung des Lizenznehmers zu verlangen.

#### §6 Gewährleistung und Mitwirkung des Lizenznehmers

- (1) Es kommen die Bestimmungen des Punkts 4 der allgemeinen Lizenzbedingungen jedenfalls zur Anwendung.
- (2) Bei Abweichungen von der Dokumentation, welche die vertragsgemäße Nutzung erheblich beeinträchtigen, ist der Lizenzgeber nach seiner Wahl zur Ersatzlieferung oder Nachbesserung verpflichtet. Gelingt es dem Lizenzgeber innerhalb einer angemessenen Frist nicht, die Abweichungen durch Ersatzlieferung oder Nachbesserung zu beseitigen oder so zu umgehen, dass dem Lizenznehmer eine vertragsgemäße Nutzung der Software ermöglicht wird oder ist die Ersatzlieferung oder Nachbesserung aus sonstigen Gründen als gescheitert anzusehen, kann der Lizenznehmer nach seiner Wahl eine Herabsetzung der Vergütung (Minderung) verlangen oder die Lizenz für das Programm fristlos gegen Erstattung der bezahlten Vergütung kündigen.
- (3) Bei der Umschreibung, Eingrenzung, Feststellung und Meldung von

Fehlern hat der Lizenznehmer nach Kräften seine Fehlermeldungen und Anfragen zu präzisieren und hierfür kompetente Mitarbeiter einzusetzen. Gegebenenfalls sind vom Händler bzw. vom Lizenzgeber überlassene Checklisten zu verwenden.

### §7 Haftung und Schutzrechte Dritter

- (1) Der Lizenzgeber haftet für von ihm zu vertretende Schäden bis zur fünffachen Höhe des Überlassungsentgeltes für die Software bzw. die Lizenzdatei. Maßgebend ist die Entgelthöhe ohne Umsatzsteuer zum Zeitpunkt des Erwerbs.
- (2) Der Lizenzgeber haftet nicht für mangelnden wirtschaftlichen Erfolg, mittelbare Schäden und Folgeschäden und für Schäden aus Ansprüchen Dritter mit Ausnahme von Ansprüchen aus Verletzung von Schutzrechten Dritter.
- (3) Für die Wiederbeschaffung von Daten und sonstige Schäden aufgrund von Datenverlust haftet der Lizenzgeber nur in der Höhe des typischen Wiederherstellungsaufwandes und nur dann, wenn der Lizenznehmer sichergestellt hat, dass diese Daten im Sinne ordnungsgemäßer Datenverarbeitung aus Datenbeständen, die in maschinenlesbarer Form bereitgehalten werden, mit vertretbarem Aufwand reproduzierbar sind, der Lizenznehmer also insbesondere eine regelmäßige und gefahrenentsprechende Anfertigung von Sicherungskopien durchgeführt hat.
- (4) Die Haftungsbeschränkungen in den Ziffern 1-3 gelten nicht für Schäden, die auf Vorsatz oder grober Fahrlässigkeit des Lizenzgebers, seiner gesetzlichen Vertreter, leitenden Angestellten oder Erfüllungsgehilfen beruhen, sowie für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit.
- (5) Verstößt der Lizenznehmer gegen in der vorliegenden Vereinbarung enthaltene Verwendungsbeschränkungen, insbesondere gegen § 1 Ziff. 3, ist eine Haftung des Lizenzgebers für infolge dieses Verstoßes entstandene Schäden ausgeschlossen.
- (6) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.
- (7) Macht ein Dritter gegenüber dem Lizenznehmer wegen der vertragsgemäßen Verwendung der gültigen, unveränderten Originalfassung der Software oder der Dokumentation Ansprüche aus einer Verletzung von gewerblichen Schutzrechten oder Urheberrechten in der Republik Österreich geltend, wird der Lizenzgeber den Lizenznehmer gegen alle Ansprüche verteidigen. Der Lizenzgeber übernimmt dem Lizenznehmer gerichtlich auferlegte Kosten und Schadensersatzbeträge, sofern der Lizenznehmer den Lizenzgeber von der Geltendmachung solcher Ansprüche unverzüglich benachrichtigt hat und dem Lizenzgeber alle Abwehrmaßnahmen und Vergleichsverhandlungen vorbehalten bleiben.
- (8) Sind gegen den Lizenznehmer Ansprüche gemäß Ziffer 7 oder sonstige Ansprüche wegen einer Verletzung von Schutzrechten Dritter geltend gemacht worden oder zu erwarten, ist der Lizenzgeber berechtigt, auf seine Kosten die Software oder die Dokumentation nach seiner Wahl - in einem für den Lizenznehmer zumutbaren Umfang - zu ändern oder ganz oder in Teilen auszutauschen.
- (9) Ist im Fall des Eingreifens der Ziffern 7 und 8 eine Änderung der Software oder die Erwirkung eines Nutzungsrechts mit angemessenem Aufwand nicht möglich, kann jeder Vertragspartner die Lizenz für die betreffende Software fristlos kündigen.

### §8 Updateservice

Der Lizenznehmer ist nach Erwerb der Lizenzdatei zur kostenlosen Nutzung des Fast Update Service (FUSE) des Urhebers berechtigt. Dauer und Umfang dieser Nutzungsbefugnis richten sich nach der Art der erworbenen Lizenz. Die Teilnahme am Updateservice nach Ablauf der ersten Nutzungsperiode erfolgt gegen zusätzliches Entgelt. Die Höhe des Entgelts richtet sich bei Beginn der neuen Nutzungsperiode nach der jeweils geltenden Preisliste des Lizenzgebers. Die Verlängerung des Updateservice richtet sich nach den getroffenen Vereinbarungen.

### §9 Vergütung des Lizenzgebers

- (1) Falls im Vertriebsweg nichts anderes vereinbart wird, gilt folgende Regelung
  - a. Der Lizenzgeber erhält vom Lizenznehmer bei Erwerb der zur Freischaltung der Software erforderlichen Lizenzdatei eine einmalige Lizenzgebühr, mit der auch eine erworbene Updateberechtigung für die erste Nutzungsperiode abgegolten ist. Die Höhe der Lizenzgebühr ergibt sich aus der bei Bestellung gültigen Preisliste des Lizenzgebers oder aus einer entsprechenden abweichenden Vereinbarung.
  - b. Die Lizenzgebühr gemäß lit. a) ist mit Übergabe der Lizenzdatei an den Lizenznehmer binnen 14 Tagen fällig. Der Lizenznehmer erhält zusammen mit der Lizenzdatei eine Rechnung über den zu zahlenden Betrag. Gerät der Lizenznehmer mit der Bezahlung des Kaufpreises in Verzug, ist der Lizenzgeber berechtigt, Verzugszinsen in Höhe von 8 Prozent über dem jeweils geltenden Dreimonats-EURIBOR per annum zu berechnen.

### §10 Sonstiges

- (1) Änderungen und Ergänzungen dieses Vertrages einschließlich dieser Klausel bedürfen der Schriftform. Mündliche Nebenabreden werden nicht getroffen. Allgemeine Geschäftsbedingungen des Lizenznehmers sind nicht

Bestandteil dieses Vertrages und haben keine Gültigkeit für dieses Vertragsverhältnis.

- (2) Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein oder werden, ohne dass damit die Erreichung des Vertragszweckes im wesentlichen unmöglich gemacht wird, so wird dadurch die Rechtswirksamkeit der übrigen Bestimmungen nicht berührt. Die unwirksame oder nicht durchführbare Bestimmung ist von den Parteien nach Möglichkeit durch eine zulässige und in wirtschaftlicher Hinsicht der unwirksamen Regelung gleichkommende Bestimmung zu ersetzen.
- (3) Auf diesen Vertrag findet das Recht der Republik Österreich Anwendung. Gegenüber Kaufleuten als Lizenznehmer ist der Gerichtsstand der Sitz des Lizenzgebers.
- (4) Bei Lieferung in EG-Länder kann die Berechnung nur dann ohne Mehrwertsteuer erfolgen, wenn der Lizenznehmer seine UST/VAT-ID angegeben hat.

## 11.3.3 Apache

Apache License  
Version 2.0, January 2004  
<http://www.apache.org/licenses/>

### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

#### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50 %) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to

reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
  - a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
  - b) You must cause any modified files to carry prominent notices stating that You changed the files; and
  - c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
  - d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.
5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee

for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

### 11.3.4 Berkeley DB License

Die vorliegende Software verwendet Teile des im BerkeleyDB Projekt entwickelten Software in der Version 1.85 und 1.86. Für diese Teile gelten die nachstehenden Lizenzbedingungen.

Copyright (c) 1990, 1993, 1994, 1995  
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1995, 1996  
The President and Fellows of Harvard University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.5 bind License

Copyright (C) 2004 Internet Systems Consortium, Inc. ("ISC")  
Copyright (C) 1996-2003 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL

DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

\$Id: COPYRIGHT,v 1.6.2.2.8.2 2004/03/08 04:04:12 marka Exp \$

Portions Copyright (C) 1996-2001 Nominum, Inc.  
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

### 11.3.6 Broadcom Corporation - End User Agreement

Die phion netfence Software enthält Software der Broadcom Corporation. Für deren Nutzung gelten folgende Bedingungen.

Software Being Licensed/ Authorized Licensee Product:  
linux driver BCM91PS500A / BCM91PS1000  
Licensee Name: phion AG

END USER AGREEMENT for usage of linux driver BCM91PS500A / BCM91PS1000

**No Warranty.** THE SOFTWARE IS OFFERED "AS IS", AND BROADCOM GRANTS AND LICENSEE RECEIVES NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, BY STATUTE, COMMUNICATION OR CONDUCT WITH LICENSEE, OR OTHERWISE. BROADCOM SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE OR NON-INFRINGEMENT CONCERNING THE SOFTWARE OR ANY UPGRADES TO OR DOCUMENTATION FOR THE SOFTWARE. WITHOUT LIMITATION OF THE ABOVE, BROADCOM GRANTS NO WARRANTY THAT THE SOFTWARE IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION, AND GRANTS NO WARRANTY REGARDING USE OR THE RESULTS THEREFROM INCLUDING, WITHOUT LIMITATION, ITS CORRECTNESS, ACCURACY OR RELIABILITY.

### 11.3.7 DHCP Relay / DHCP Enterprise Server

Following is the copyright on the ISC DHCP Server:

Copyright (c) 2004 Internet Systems Consortium, Inc. ("ISC")  
Copyright (c) 1995-2003 Internet Software Consortium.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of ISC, ISC DHCP, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY INTERNET SYSTEMS CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ISC OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.8 ISAKMP License

Teile der vorliegenden Software verwendet Software aus Isakmp. Für Isakmp gelten die nachstehenden Lizenzbedingungen.

Copyright (c) 1999-2001, Angelos D. Keromytis. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.9 ISS Proventia Web Filter

Die phion netfence Software enthält Software der Internet Security Systems / Atlanta USA. Für deren Nutzung gelten folgende Bedingungen.

ENDBENUTZER-LIZENZVERTRAG FÜR ISS Proventia Web Filter Nutzer

WICHTIG - BITTE SORGFÄLTIG LESEN: Dieser Endbenutzer-Lizenzvertrag ist ein rechtsgültiger Vertrag zwischen Ihnen (entweder als natürlicher oder juristischer Person) und phion AG für das oben bezeichnete Softwareprodukt. Indem Sie das SOFTWAREPRODUKT installieren erklären Sie sich einverstanden, durch die Bestimmungen dieses Lizenzvertrags gebunden zu sein. Falls Sie den Bestimmungen dieses Lizenzvertrags nicht zustimmen, sind Sie nicht berechtigt, das SOFTWAREPRODUKT zu installieren oder zu verwenden. Falls Sie das SOFTWAREPRODUKT erworben haben, können Sie es gegen volle Rückerstattung des Kaufpreises der Stelle zurückgeben, von der Sie es erworben haben.

Das SOFTWAREPRODUKT wird sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge geschützt als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum. Das SOFTWAREPRODUKT wird lizenziert, nicht verkauft.

1. LIZENZIERUNG. Das SOFTWAREPRODUKT wird wie folgt lizenziert:
  - \* Installieren und Verwenden: phion räumt Ihnen das Recht ein, Kopien des SOFTWAREPRODUKTS auf Ihren Computern zu installieren und zu verwenden.
  - \* Sicherungskopien: Sie sind außerdem berechtigt, die für Sicherungs- und Archivierungszwecke notwendigen Kopien des SOFTWAREPRODUKTS anzufertigen.
2. BESCHREIBUNG WEITERER RECHTE UND EINSCHRÄNKUNGEN.
  - Beibehaltung der Copyright-Vermerke. Sie sind nicht berechtigt, die Copyright-Vermerke auf den Kopien des SOFTWAREPRODUKTS zu entfernen oder zu ändern.
  - Vertrieb. Sie sind nicht berechtigt, Kopien des SOFTWAREPRODUKTS an Dritte weiterzuverbreiten.
  - Verbot im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, das SOFTWAREPRODUKT zurückzuentwickeln (Reverse Engineering), zu dekompileieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Beschränkung, dies ausdrücklich gestattet.
  - Vermietung. Sie sind nicht berechtigt, das SOFTWAREPRODUKT zu vermieten, zu verleasen oder zu verleihen.
  - Übertragung. Sie sind berechtigt, alle Ihre Rechte aus diesem Lizenzvertrag auf Dauer zu übertragen, vorausgesetzt, der Empfänger stimmt den Bestimmungen dieses Lizenzvertrags zu.
  - Supportleistungen. phion bietet Ihnen möglicherweise Supportleistungen in Verbindung mit dem SOFTWAREPRODUKT ("Supportleistungen"). Die Supportleistungen können entsprechend den phion Lizenzbestimmungen und -Programmen, die im Benutzerhandbuch, der Dokumentation im "Online"-Format und/oder anderen von phion zur Verfügung gestellten Materialien beschrieben sind, genutzt werden. Jeder ergänzende Softwarecode, der Ihnen als Teil der Supportleistungen zur Verfügung gestellt wird, wird als Bestandteil des SOFTWAREPRODUKTS betrachtet und unterliegt den Bestimmungen dieses Lizenzvertrags. phion ist berechtigt, die technischen Daten, die Sie der phion AG als Teil der Supportleistungen zur Verfügung stellen, für geschäftliche Zwecke, einschließlich der Produktunterstützung und -entwicklung, zu verwenden. phion



verpflichtet sich, solche technischen Daten ausschließlich anonym im Sinne des Datenschutzes zu verwenden.

--Beachtung aller anwendbarer Gesetze. Sie sind verpflichtet, das SOFTWAREPRODUKT nur in Übereinstimmung mit allen anwendbaren Gesetzen zu verwenden.

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist phion berechtigt, diesen Lizenzvertrag zu kündigen, sofern Sie gegen die Bestimmungen dieses Lizenzvertrags verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien des SOFTWAREPRODUKTS zu vernichten.
4. EIGENTUM. Jegliche Eigentumsrechte, einschließlich, jedoch nicht beschränkt auf das Urheberrecht, an dem und in bezug auf das SOFTWAREPRODUKT und jeder Kopie davon liegen bei Internet Security Systems / Atlanta USA oder phion oder deren Lieferanten. Eigentumsrechte und geistiges Eigentum an und in bezug auf den Inhalt, auf den durch das SOFTWAREPRODUKT zugegriffen wird, liegen beim jeweiligen Eigentümer und können durch entsprechende urheberrechtliche oder andere Gesetze über geistiges Eigentum geschützt sein. Dieser Lizenzvertrag gibt Ihnen keine Rechte an solchem Inhalt. Alle nicht ausdrücklich eingeräumten Rechte bleiben phion AG vorbehalten.
5. GEWÄHRLEISTUNGS AUSSCHLUSS. phion schließt ausdrücklich jede Gewährleistung für das SOFTWAREPRODUKT aus. DAS SOFTWAREPRODUKT UND DIE DARAUF BEZOGENE DOKUMENTATION WIRD IHNEN "SO WIE SIE IST" ZUR VERFÜGUNG GESTELLT, OHNE GEWÄHRLEISTUNG IRGEND EINER ART, WEDER AUSDRÜCKLICH NOCH KONKLUDENT, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF KONKLUDENTE GEWÄHRLEISTUNGEN DER TAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DES NICHTBESTEHENS EINER RECHTSVERLETZUNG. DAS GESAMTE RISIKO, DAS AUS DEM VERWENDEN ODER DER LEISTUNG DES SOFTWAREPRODUKTS ENTSTEHT, VERBLEIBT BEI IHNEN.
6. BESCHRÄNKTE HAFTUNG. Bis zum durch anwendbares Recht äußerstenfalls Zulässigen können weder phion noch deren Lieferanten haftbar gemacht werden für irgendwelche besonderen, zufällig entstandenen oder indirekten Schäden oder Folgeschäden (einschließlich, aber nicht beschränkt auf entgangenen Gewinn, Betriebsunterbrechung, Verlust geschäftlicher Informationen oder irgendeinen anderen Vermögensschaden), die aus dem Verwenden oder der Unmöglichkeit, das SOFTWAREPRODUKT zu verwenden, oder durch die Leistung bzw. Nichtleistung von Supportleistungen entstehen, und zwar auch dann, wenn phion zuvor auf die Möglichkeit solcher Schäden hingewiesen worden ist. In jedem Fall bleibt die gesamte Haftung der phion AG auf den Betrag, den Sie für das SOFTWAREPRODUKT bezahlt haben, oder auf EUR 10,- beschränkt, wobei der höhere Betrag maßgebend ist.

### 11.3.10 Microdasys

#### 1. GRANT OF LICENSE

- a) phion AG, Eduard-Bodem-Gasse 1, 6020 Innsbruck, FN [Business Register Number] 184392 (hereinafter referred to as "phion") grants to you a non-exclusive, non-transferable, non-sublicensable license to use phion's SSLPRX service, the respective phion software module.
- b) phion's SSLPRX contains one or more of the following software modules; SCIP, XMLRay, and/or SX-Suite (the "Product" or the "Software"), in binary executable form, which are copyright protected by:

Microdasys Inc.  
Worldwide Headoffice  
385 Pilot Road, Suite A  
Las Vegas, NV 89119, USA  
www.microdasys.com

Microdasys grants to you a non-exclusive, non-transferable, non-sublicensable license to use the Product.

#### 2. PERMITTED USES

- a) Subject to timely payment of license fees phion shall grant you an exclusive right to install and use the programme on a data storage device from issuance of the license certificate for the licensed period of time. The license exclusively concerns the use of the Product by you for your own data processing processes. You shall not be entitled to grant third parties access to the Product. You undertake to keep the Software safe so that access and, thus, copying or using the Software by third parties is prevented.
- b) This Software End User License Agreement ("Agreement") permits you to use one copy of the Product, as a server for up to a number of computers for which you have paid for this license (each, a "Seat"); as a special case you may have been granted a license for an unlimited number of users. A computer serves as a Seat when the user at the Seat accesses or utilizes, directly or indirectly, the Product. Use of software or hardware which reduces the number of

computers directly accessing or utilizing the Product (also known as "pooling" or "multiplexing") will not be deemed to reduce the number of Seats. Each computer indirectly accessing or utilizing the Product is still considered a Seat. You are permitted to install the product on more than one server for load-balancing and High-Availability reasons, provided that the total number of licensed seats accessing either one of these servers is not exceeded.

#### 3. TESTING

The Software is available for evaluation purposes by way of time limited evaluation licenses. The evaluation license required to test the software can be obtained free of charge. The Software must only be used in connection with an implementation of a phion nefence system. The scope of use of the Software will be partly restricted by those systems.

#### 4. COPYRIGHT

- a) All title and copyrights in and to the Product and any copies thereof are owned by Microdasys or its suppliers. The Product is protected by US and Austrian copyright laws, international treaty provisions and all other applicable national laws. The Product is licensed, not sold. All title and intellectual property rights in and to the content which may be accessed through use of the Product are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This agreement grants you no rights to use such content. Therefore, you must treat the Product like any other copyrighted material (e.g. a book or musical recording) except that if the Product is not copy protected, you may make one copy of the Product solely for backup or archival purposes, provided any copy must contain all of the original Product's proprietary notices. You may not copy the Product manual(s), on-line documentation, or any written materials accompanying the Product. If you receive your first copy of the Product electronically, and a second copy on media, the second copy may be used for archival purposes only, and must contain the same proprietary notices which appear on and in the Product. This Agreement does not grant you any right to any enhancement or update.
- b) You expressly acknowledge that Microdasys is the owner of all proprietary rights and rights to use the Product which result from copyright. In case you violate such rights and other mandatory copyright provisions, Microdasys shall be entitled to all legal remedies which are provided for under copyright law to defend copyrights protection.

#### 5. RESTRICTIONS

- a) You may not rent or lease the Product, and may not transfer your rights under this Agreement without obtaining the prior written consent of phion. To the extent such restriction is allowable under law, and unless provided otherwise by mandatory statutory provisions, you shall not be entitled to translate the programme from object code into source code (e.g. by reverse engineering, disassembling or decompiling).
- b) You shall not be entitled to crack or change the license key.
- c) You shall not be entitled to modify or delete any notes regarding rights, trademarks or the like which are stated in the programme or on the media on which the programme is stored.
- d) You may not distribute copies of the Product to third parties unless explicitly authorized to do so by an additional written agreement.
- e) You may not integrate, incorporate or bundle the Product into any other software or include the Product in other software or hardware without receiving the prior written consent of phion.
- f) You must not disclose the results of any benchmark test of the Product to any third party without phion's prior written approval. You must not publish reviews of the Product without prior consent from phion.
- g) You acknowledge that the source code form of the Product remains a confidential trade secret of Microdasys and/or its suppliers. You must maintain all copyright notices on all copies of the Product.
- h) The license may be linked to the hardware configuration via a license key. In the case of modifications of the hardware configuration phion shall be free to issue another license key to you free of charge. You shall then lose the right to continue to use the first license key. phion shall be entitled to request evidence thereof within fourteen days of receipt of the new license key.

#### 6. TERM

The term of this Agreement is perpetual. However, you may terminate your license at any time by destroying all copies of the Product and Product documentation.

#### 7. TERMINATION

Your license will terminate automatically if you fail to comply with the limitations described above. On termination, you must destroy all copies of the Product.

#### 8. NOTE ON SSL SUPPORT

The Product contains support for encrypted programs using SSL. SSL technology is not fault tolerant and is not designed, manufactured, or intended for use or resale as on-line control equipment in hazardous



environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of SSL technology could lead directly to death, personal injury, or severe physical or environmental damage. Generally speaking, and regardless of the SSL support the product is not intended for any uses in which, in which the failure of the product could lead directly to death, personal injury, or severe physical or environmental damage. Furthermore, the Product does not provide complete protection against harmful applications.

YOU ARE EXPLICITLY WARNED THAT THE SECURITY ENHANCEMENT FEATURES OF THE PRODUCT DO NOT PROVIDE TOTAL PROTECTION AGAINST DAMAGING SOFTWARE ROUTINES.

#### 9. LIMITED WARRANTY

Subject to payment of applicable license fees, Microdasys warrants that the Product will perform substantially in accordance with the accompanying Product manual(s) or on-line documentation for a period of 90 days from the date of fee payment. Any implied warranties on the Product are limited to 90 days. Microdasys does not warrant that the Product is error free. Microdasys's entire liability and your exclusive remedy under this warranty shall be, at Microdasys's option, either (a) return of the price paid or (b) repair or replacement of the Product that does not meet this limited warranty and which is returned to Microdasys with a copy of your receipt. This limited warranty is void if failure of the Product has resulted from accident, abuse, or misapplication. Any replacement Product will be warranted for the remainder of the original warranty period or 30 days, whichever is longer.

#### 10. NO OTHER WARRANTIES

EXCEPT AS EXPLICITLY SET FORTH IN THIS AGREEMENT, THE PRODUCT IS PROVIDED "AS IS". NEITHER MICRODASYS NOR PHION WARRANT THAT THE PRODUCT IS ERROR-FREE. ADDITIONALLY, MICRODASYS AND PHION DISCLAIM ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

#### 11. NO LIABILITY FOR CONSEQUENTIAL DAMAGES

IN NO EVENT SHALL MICRODASYS AND PHION OR ITS SUPPLIERS BE LIABLE FOR ANY CONSEQUENTIAL OR INDIRECT DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS MICRODASYS AND PHION, EVEN IF MICRODASYS AND PHION HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION SHALL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS AGREEMENT GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM JURISDICTION TO JURISDICTION

#### 12. EXPORT REGULATIONS

a) This software contains cryptography and is therefore subject to US government export control under the U.S. Export Administration Regulations (EAR). EAR Part 740.13(e) allows the export and reexport of publicly available encryption source code that is not subject to payment of license fee or royalty payment. Object code resulting from the compiling of such source code may also be exported and reexported under this provision if publicly available and not subject to a fee or payment other than reasonable and customary fees for reproduction and distribution. This kind of encryption source code and the corresponding object code may be exported or reexported without prior U.S. government export license authorization provided that the U.S. government is notified about the Internet location of the software. The open source software used in this product is publicly available without license fee or royalty payment, and all binary software is compiled from the open source code. The U.S. government has been notified about this software as explained above. Therefore, the source code and compiled object code may be downloaded and exported under U.S. export license exception (without a U.S. export license) except to the following destinations: Afghanistan (Taliban controlled areas), Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan and Syria. This list of countries is subject to change.

b) Products delivered by phion are designed for being used within and for remaining in the EU. Re-export, be it separately or integrated into a system, shall be subject to export approval. You must comply with all applicable foreign trade legislation and US Export Regulations including valid ECCN numbers. Reselling to customers that operate, manufacture, service or otherwise are involved with any nuclear material for any purpose, shall require special permits. phion reserves the right to adjust the provisions on export and import at any time if national or international legislation so requires.

#### 13. MISCELLANEOUS

a) This Agreement represents the complete agreement concerning

the license between you and Microdasys and supersedes all prior agreements and representations between you and Microdasys.

b) It may be amended only by writing executed by you, Microdasys and phion. If any provision of the Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable.

c) This Agreement is governed by the laws of the United States of America. Should you have any questions concerning this Agreement, or if you desire to contact phion for any reason, please contact the phion affiliate serving your country or write to: phion Inc., 385 Pilot Rd., Suite A, Las Vegas, NV, 89141

d) If individual provisions of this contract are or become ineffective, the remaining provisions of this contract shall not be affected. The contracting parties shall co-operate as partners in order to find a provision which comes as close as possible to the ineffective provisions.

#### 14. RPA

All Certificate Authorities ("CA") have some sort of agreement in place (usually called Relying Party Agreement, "RPA"). We strongly recommend that you read these prior to using any of their services, including but not limited to Certificate Revocation List ("CRL") and Online Certificate Status Protocol ("OCSP") repositories. It is your sole responsibility to retrieve these agreements from each CA's respective website and decide to whether or not to agree to the terms and conditions of the RPA of each CA. You may only use the Microdasys/phion SCIP CRL and OCSP and the Microdasys/phion SCIP Certificate Validation Engine for certificates of those CAs which RPA you have read, understood and agreed to. You are also responsible for re-visiting the websites of the CAs from time to time, to verify whether or not the content of the RPA has been amended. By installing and using the phion SCIP product and the Microdasys/phion CRL and OCSP Engine and Database, you declare that you have read and understood the above and accept its conditions.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

#### 15. PURCHASE PRICE

Unless otherwise agreed in the course of distribution, the following regulation shall apply:

The purchase price for the Program including the license certificate shall be transferred to the company account of phion within fourteen days of delivery of the license certificate without another invoice for the due purchase price being necessary. If you are in default of payment of the purchase price, phion shall be entitled to charge default interest at a rate of 8 % p.a. above the three-months EURIBOR applicable from time to time.

#### 16. ENHANCEMENTS OF PROGRAMMES (UPDATES) AND MODIFICATIONS OF PROGRAMMES

a) BY PURCHASING THE LICENSE CERTIFICATE YOU SHALL NOT ACQUIRE ANY RIGHT TO FURTHER SUPPORT BY phion OR TO DELIVERY OF UPDATES OR PROGRAMME EXTENSIONS.

b) You expressly agree that data concerning you which becomes known to phion within the scope of the business relationship with you shall be collected and processed by phion for the purpose of information about the development of updates and new programme versions and for offering of maintenance contracts and for other offers.

c) You acknowledge and agree that your personal data be stored and processed by phion for the purpose of internal data collection, data processing and for information about the development in connection with the delivered product and of updates and new programme versions. In accordance with Section 107 TKG [Austrian Telecommunications Act] you expressly agree to receipt of such information also by e-mail.

### 11.3.11 The OpenLDAP Public License

Teile der vorliegenden Software verwendet Software aus OpenLDAP. Für OpenLDAP gelten die nachstehenden Lizenzbedingungen.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.



THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.  
(eay@cryptsoft.com).  
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.  
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.  
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
4. "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
5. The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
6. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

### 11.3.12 OpenSSH License

Licensed Software: This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1. Copyright (c) 1995 Tatu Ylonen , Espoo, Finland All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

RSA is no longer included, found in the OpenSSL library  
IDEA is no longer included, its use is deprecated  
DES is now external, in the OpenSSL library  
GMP is no longer used, and instead we call BN code from OpenSSL  
Zlib is now external, in a library  
The make-ssh-known-hosts script is no longer included  
TSS has been removed  
MD5 is now external, in the OpenSSL library  
RC4 support has been replaced with ARC4 support from OpenSSL  
Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "<http://www.cs.hut.fi/crypto/>".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

#### NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2. The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright © 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

- ssh-keygen was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

- The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

```
@version 3.0 (December 2000) Optimised ANSI C code for the Rijndael
cipher (now AES)
@author Vincent Rijmen
@author Antoon Bosselaers
@author Paulo Barreto
```

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright © 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- The progressmeter code used by scp(1) and sftp(1) is copyright by the NetBSD Foundation.

Copyright © 1997-2003 The NetBSD Foundation, Inc. All rights reserved.

This code is derived from software contributed to The NetBSD Foundation by Luke Mewburn.

This code is derived from software contributed to The NetBSD Foundation by Jason R. Thorpe of the Numerical Aerospace Simulation Facility, NASA Ames Research Center.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

- Neither the name of The NetBSD Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

```
Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
```

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.13 OpenSSL License

Die vorliegende Software verwendet Teile der im OpenSSL Projekt entwickelten Software fuer die Nutzung im OpenSSL Toolkit. Fuer diese Teile gelten die nachstehenden Lizenzbedingungen. / Parts of this Software use software developed in the OpenSSL project for usage of the OpenSSL Toolkit. Herefore, the following licensing conditions apply.

#### LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

OpenSSL License

Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).  
Original SSLeay License  
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.  
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:  
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)."  
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:  
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

### 11.3.14 The PHP License, version 3.0

-----  
The PHP License, version 3.0  
Copyright (c) 1999 - 2002 The PHP Group. All rights reserved.  
-----

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.  
Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo".
4. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number.  
Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
5. Redistributions of any form whatsoever must retain the following acknowledgment:  
"This product includes PHP, freely available from <<http://www.php.net/>>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <<http://www.php.net/>>.

This product includes the Zend Engine, freely available at <<http://www.zend.com/>>.

### 11.3.15 PHPMailer

PHPMailer is a PHP-Class for PHP ([www.php.net](http://www.php.net)) providing a package of functions to send emails. PHPMailer is released under the GNU LESSER GENERAL PUBLIC LICENSE. For LGPL license information see Page 625.

### 11.3.16 PostgreSQL

License  
PostgreSQL is released under the BSD license.  
PostgreSQL Database Management System (formerly known as Postgres, then as Postgres95)

Portions Copyright (c) 1996-2005, The PostgreSQL Global Development Group

Portions Copyright (c) 1994, The Regents of the University of California

Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written

agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

### 11.3.17 PuTTY License

Teile der vorliegenden Software verwendet Software aus PuTTY. Für PuTTY gelten die nachstehenden Lizenzbedingungen. / Parts of this Software use software from PuTTY. The following licensing conditions apply to PuTTY.

PuTTY is copyright 1997-2000 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### 11.3.18 RipeMD160

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)  
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).  
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:  
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".  
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an

acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

### 11.3.19 SHA2

Written by Aaron D. Gifford <me@aarongifford.com>

Copyright 2000 Aaron D. Gifford. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) AND CONTRIBUTOR(S) "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) OR CONTRIBUTOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.20 phion SNMPD License

The phion SNMP daemon is based on the net snmp project. The following license conditions are valid for the original part of the software.

Various copyrights apply to this package, listed in 3 separate parts below. Please make sure to take note of all parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT



SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001, Networks Associates Technology, Inc  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the NAI Labs nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001, Cambridge Broadband Ltd.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.21 SpamAssassin (Artistic License)

Ein Teil der vorliegenden Software verwendet Software aus SpamAssassin. Für SpamAssassin gelten die nachstehenden Lizenzbedingungen.

#### Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

#### Definitions:

- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.
- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.

- "Copyright Holder" is whoever is named in the copyright or copyrights for the package.
  - "You" is you, if you're thinking about copying or distributing this Package.
  - "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
  - "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.
1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
  2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.
  3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:
    - a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
    - b) use the modified Package only within your corporation or organization.
    - c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.
    - d) make other distribution arrangements with the Copyright Holder.
  4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:
    - a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.
    - b) accompany the distribution with the machine-readable source of the Package with your modifications.
    - c) accompany any non-standard executables with their corresponding Standard Version executables, giving the nonstandard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
    - d) make other distribution arrangements with the Copyright Holder.
  5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own.
  6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.
  7. C or perl subroutines supplied by you and linked into this Package shall not be considered part of this Package.
  8. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

### 11.3.22 TUN/TAP driver for Mac OS X

A part of this software uses the tun/tap driver for Mac OS X provided by Mattias Nissler. This driver comes along with following terms of license:  
tun/tap driver for Mac OS X



Copyright (c) 2004, 2005 Mattias Nissler <mattias.nissler@gmx.de>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.23 Vortex and AXL

GPL Style-License

Copyright (C) 2007 Advanced Software Production Line, S.L.  
All rights reserved.

phion netfence includes source code from the following projects, which are covered by their own licenses:  
Vortex Library, fully available at <http://www.aspl.es/vortex>  
AXL, fully available at: <http://www.aspl.es/axl>

#### DISCLAIMER:

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JOHN LIM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.3.24 WinPcap

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).  
Copyright (c) 2005 - 2008 CACE Technologies, Davis (California).  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.

This product includes software developed by Yen Yen Lim and North Dakota State University.

-----  
Portions Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
Portions Copyright (c) 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

-----  
Portions Copyright (c) 1995, 1996, 1997 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the Kungliga Tekniska Högskolan and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



-----  
 Portions Copyright (c) 1997 Yen Yen Lim and North Dakota State University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by Yen Yen Lim and North Dakota State University"
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
 Portions Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-----  
 Portions Copyright (C) 1995, 1996, 1997, 1998, and 1999 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
 Portions Copyright (c) 1996 Juniper Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution. The name of Juniper Networks may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

-----  
 Portions Copyright (c) 2001 Daniel Hartmeier All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
 Portions Copyright 1989 by Carnegie Mellon.

Permission to use, copy, modify, and distribute this program for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Carnegie Mellon not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Carnegie Mellon and Stanford University. Carnegie Mellon makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

### 11.3.25 WPA Supplicant

Copyright (c) 2003-2008, Jouni Malinen <j@w1.fi> and contributors All Rights Reserved.

This program is dual-licensed under both the GPL version 2 and BSD license. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## 11.4 Software Package Listing and Licenses

**Table 23-158** Software package listing and licenses

Module	License
anaconda	GPL
anaconda-help	distributable
anaconda-runtime	GPL
anacron	GPL
apr	Apache Software License
apr-util	Apache Software License
arpwatch	BSD
ash	BSD
at	GPL
atk	LGPL
authconfig	GPL
autoconf	GPL
autoconf253	GPL
automake	GPL
automake15	GPL
Basesystem	public domain
Bash	GPL
bash-doc	GPL
bc	GPL
bdflush	Distributable
bind	BSD-like
bind-chroot	BSD-like
bind-devel	BSD-like
bind-utils	BSD-like
binutils	GPL
bison	GPL
bootparamd	BSD
busybox	GPL
busybox-anaconda	GPL
byacc	public domain
bzip2	BSD
bzip2-devel	BSD
bzip2-libs	BSD
cdecl	distributable
chkconfig	GPL
chkfontpath	GPL
cipe	GPL
compat-db	BSDish
compat-egcs	GPL
compat-glibc	LGPL
compat-libstdc++	GPL
console-tools	GPL
cpio	GPL
cpp	GPL
cproto	Public Domain
cracklib	Artistic
cracklib-dicts	Artistic
crontabs	Public Domain
ctags	GPL
curl	MIT/X derivate
curl	MPL
cyrus-sasl	Freely Distributable
cyrus-sasl-md5	Freely Distributable
DAVExplorer	GPL
db1	BSD

**Table 23-158** Software package listing and licenses

Module	License
db1-devel	BSD
db4	GPL
db4-devel	GPL
dbus	AFL/GPL
dbus-glib	AFL/GPL
dbus-python	AFL/GPL
dcc	BSD-like
dev	GPL
dev86	GPL
dhcp	BSD 3-Clause
dhcpcd	GPL
dhcp-relay	BSD 3-Clause
dhcp-server	BSD 3-Clause
diag-ether	GPL
dietlibc	GPL
diffutils	GPL
dmalloc	public domain
dmidecode	GPL
dosfstools	GPL
dump	BSD
e2fsprogs	GPL
eject	GPL
ethtool	GPL
expat	GPL
fbset	GPL
fetchmail	GPL
file	distributable
filesystem	Public Domain
fileutils	GPL
findutils	GPL
flex	BSD
fonts-ISO8859-2	Freely distributable
fonts-ISO8859-2-75dpi	Freely distributable
freeradius	GPLv2+ and LGPLv2+
freetype	GPL - see <a href="http://www.freetype.org">www.freetype.org</a>
freetype-utils	GPL
ftp	BSD
fuse	GPL
gawk	GPL
gcc	GPL
gcc-c++	GPL
gcc-objc	GPL
gd	GNU
gdb	GPL
gdbm	GPL
genromfs	GPL
gettext	GPL/LGPL
getty_ps	Distributable - Copyright 1989,1990 by Paul Sutcliffe Jr.
glib10	LGPL
glib	LGPL
glib2	LGPL
glib2-devel	LGPL
glibc	LGPL
glibc-common	LGPL
glibc-debug	LGPL
glibc-debug	LGPL
glibc-devel	LGPL
glibc-kernheaders	GPL

**Table 23-158** Software package listing and licenses

Module	License
glibc-profile	LGPL
glibc-utils	LGPL
gmp	LGPL
gnugk	GPL
gnupg	GPL
gpm	GPL
grep	GPL
groff	GPL
groff-perl	GPL
grub	GPL
gtk-doc	LGPL
gzip	GPL
hdparm	BSD
hotplug	GPL
httpd	Apache License, Version 2.0
hwbrowser	GPL
hwcrypto	GPL
hwdata	GPL/MIT
hwtool	GPL
ifenslave	distributable
indent	GPL
indexhtml	distributable
info	GPL
initscripts	GPL
intltool	GPL
iproute	GNU GPL
iptables	GPL
iptables-ipv6	GPL
iptraf	GPL
iputils	BSD
irda-utils	GPL
isdn4k-utils	GPL
isdn cards	GPL
jfsutils	GPL
jta	GPL
kernel	GPL
kernel-BOOT	GPL
kernel-doc	GPL
kernel-source	GPL
kon2	distributable
krb5	Copyright(C) 1985-2005 by the Massachusetts Institute of Technology
krb5-libs	Copyright(C) 1985-2005 by the Massachusetts Institute of Technology
ksymoops	GPL
kudzu	GPL
kudzu-devel	GPL
l2tpd	GPL
lcd4linux	GPL
less	GPL
libaio	LGPL
libao	GPL
libcap	BSD-like and LGPL
libcap-devel	BSD-like and LGPL
libcurl4	MIT/X derivate
libelf	distributable
libghttp	LGPL
libglade	LGPL
libglib-2.0_0	LGPL

**Table 23-158** Software package listing and licenses

Module	License
libgmodule-2.0_0	LGPL
libgobject-2.0_0	LGPL
libgsasl	LGPL
libgthread-2.0_0	LGPL
libjpeg	GNU
libltdl	GPL
libltdl-devel	GPL
libole2	GPL
libpcap	BSD
libpng-1.2.8	GPL
librsvg	LGPL
libsic++	LGPL
libstdc++	GPL
libstdc++-devel	GPL
libtermcap	LGPL
libtool	GPL
libtool-libs13	GPL
libtool-libs	GPL
libunicode	LGPL
libusb	LGPL
libuser	LGPL
libvortex	LGPL
libvortex-axl	LGPL
libxml10	LGPL
libxml2_2	MIT
libxml2	MIT
libxml2-devel	MIT
libxml2-python	MIT
libxslt-python	MIT
lilo	MIT
lm_sensors	GPL
locale_config	GPL
lockdev	LGPL
logrotate	GPL
losetup	distributable
lrzsz	GPL
lsik	Free
lsof	Free
ltrace	GPL
lvm	GPL
lynx	GPL
m2crypto	BSD
m4	GPL
make	GPL
MAKEDEV	GPL
man	GPL
man-pages	distributable
mc	GPL
memtest86+	GPL
mgetty	GPL
mingetty	GPL
minicom	GPL
mkbootdisk	GPL
mkinitrd	GPL
mktemp	BSD
mm	Apache Software License
mod_ssl	Apache License, Version 2.0
modutils	GPL
mount	distributable

Table 23-158 Software package listing and licenses

Module	License
mouseconfig	distributable
ncftp	distributable
ncompress	distributable
ncurses4	distributable
ncurses	distributable
ncurses-devel	distributable
netdump	GPL
net-tools	GPL
newt	LGPL
nfreporter	Mixed (see LICENSE)
nss_db	GPL
nss_db-compat	GPL
ntp	distributable
open	GPL
openh323	MPL
openh323-devel	MPL
openldap12	OpenLDAP
openldap	OpenLDAP
openldap-clients	OpenLDAP
openldap-servers	OpenLDAP
openssh	BSD
openssh38	Other License(s), see package
openssh-clients	BSD
openssh-server	BSD
openssl096b	BSDish
openssl	BSDish
p3pmail	Strict
p3scan	GPL
pam	GPL or BSD
pam-devel	GPL or BSD
parted	GPL
passwd	BSD
patch	GPL
patchutils	GPL
pciutils	GPL
pciutils-devel	GPL
pcre	GPL
pcre-devel	GPL
perl	Artistic or GPL
perl-Digest-HMAC	distributable
perl-Digest-SHA1	GPL or Artistic
perl-HTML-Parser	GPL or Artistic
perl-HTML-Tagset	distributable
perl-Net-DNS	distributable
perl-Razor-Agent	Artistic
perl-Time-HiRes	distributable
perl-URI	distributable
php	The PHP license (see "LICENSE" file included in distribution)
phpPgAdmin	GPL
pidentd	Public domain
pinfo	GPL
pkgconfig	GPL
pmake	BSD
popt	GPL
portmap	BSD
postgresql	BSD
postgresql-libs	BSD
ppp	distributable

Table 23-158 Software package listing and licenses

Module	License
pptp	GPL
pptpd	GPL
procmail	GPL or artistic
procps	GPL
properJavaRDP	GPL
psacct	GPL
psmisc	BSD/GPL
psutils	distributable
pump	MIT
pwdb	GPL or BSD
pwlib	MPL
pwlib-devel	MPL
pxe	BSD
python	distributable
python24	PSF
python-clap	GPL
python-devel	distributable
python-docs	distributable
python-popt	GPL
python-tools	distributable
python-xmlrpc	BSDish
pyzor	GPL
quagga	GPL
quagga-contrib	GPL
quagga-devel	GPL
raidtools	GPL
rcs	GPL
readline2.2.1	GPL
readline	GPL
readline-devel	GPL
redhat-lsb	GPL
reiserfs-utils	GPL
rmt	BSD
rootfiles	public domain
rpm	GPL
rpm-build	GPL
rpm-devel	GPL
rpm-python	GPL
rp-pppoe	GPL
rsync	GPL
sac	Freely Distributable
samba	GNU GPL version 2
samba-client	GNU GPL version 2
samba-common	GNU GPL version 2
samba-doc	GNU GPL version 2
sash	GPL
sed	GPL
setup	public domain
sgml-common	GPL
shadow-utils	BSD
sh-utils	GPL
slang	GPL
slocate	GPL
smartsuite	GPL
smstools	GPL v2
spamassassin	Artistic
specspo	GPL
sqlite	Strict
squid	GPL

**Table 23-158** Software package listing and licenses

Module	License
sslrpxsquad	GPL
stat	GPL
strace	BSD
stunnel	GPL
symlinks	distributable
syslinux	BSD
syslog-ng	GPL
sysreport	GPL
tar	GPL
tcl	BSD
tcpdump	BSD
tcp_wrappers	Distributable
tcsh	distributable
telnet	BSD
termcap	Public Domain
texinfo	GPL
textutils	GPL
tightvnc	GPL
time	GPL
tmpwatch	GPL
traceroute	BSD
ttcp	Public Domain
unzip	BSD
usbutils	GPL
usermode	GPL
utempter	MIT
util-linux	distributable
vconfig	distributable
vera_ttf	GPL
vim-common	freeware
vim-minimal	freeware
vixie-cron	distributable
watchdog	GPL
wget	GPL
which	GPL
wireless-tools	GPL
words	freeware
xauth	XFree86
xml-common	GPL
zend-optimizer	GPL
zlib	BSD
zlib-devel	BSD

### 11.4.1 BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS

OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 11.4.2 GNU Lesser General Public License

Version 2.1, February 1999  
 Copyright (C) 1991, 1999 Free Software Foundation, Inc.  
 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA  
 Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

#### 11.4.2.1 Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the

reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

### 11.4.2.2 Terms and Conditions for Copying, Distribution and Modification

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a) The modified work must itself be a software library.
  - b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
  - c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
  - d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an

application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms



of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
  - a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
  - b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues),

conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>  
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to add a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990  
Ty Coon, President of Vice

That's all there is to it!

### 11.4.3 GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA  
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

#### 11.4.3.1 Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program

proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

#### 11.4.3.2 TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
  - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
  - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
  - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - b) Accompany it with a written offer, valid for at least three years, to

give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
- 6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
- 7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

- 8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
- 9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

- 10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

- 11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>  
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989  
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

## 11.4.4 The "Artistic License"

### Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

### Definitions

- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.
- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.
- "Copyright Holder" is whoever is named in the copyright or copyrights for the package.
- "You" is you, if you're thinking about copying or distributing this Package.
- "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
- "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

### Conditions

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.
3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:
  - a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
  - b) use the modified Package only within your corporation or organization.
  - c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.
  - d) make other distribution arrangements with the Copyright Holder.
4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:
  - a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

- b) accompany the distribution with the machine-readable source of the Package with your modifications.
  - c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
  - d) make other distribution arrangements with the Copyright Holder.
5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.
  6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.
  7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these sub-routines do not change the language in any way that would cause it to fail the regression tests for the language.
  8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.
  9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.
  10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

## 11.4.5 MIT License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

\* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* Neither the names of the author(s) nor the names of other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

### Disclaimer

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(Note: The above license is copied from the BSD license at: [www.opensource.org/licenses/bsd-license.html](http://www.opensource.org/licenses/bsd-license.html), substituting the appropriate references in the template.)

(end)



## 11.4.6 Mozilla Public License

Version 1.1

### 1. Definitions.

- 1.0.1 "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.
- 1.1 "Contributor" means each entity that creates or contributes to the creation of Modifications.
- 1.2 "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.
- 1.3 "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.
- 1.4 "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.
- 1.5 "Executable" means Covered Code in any form other than Source Code.
- 1.6 "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.
- 1.7 "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.
- 1.8 "License" means this document.
- 1.9 "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:
  - A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.
  - B. Any new file that contains any part of the Original Code or previous Modifications.
- 1.10 "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.
- 1.10.1 "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.
- 1.11 "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.
- 1.12 "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50 %) of the outstanding shares or beneficial ownership of such entity.

### 2. Source Code License.

- 2.1 The Initial Developer Grant.  
The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:
  - (a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and
  - (b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).
  - (c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.
  - (d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination

of the Original Code with other software or devices.

### 2.2 Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

- (a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and
- (b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).
- (c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.
- (d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

### 3. Distribution Obligations.

#### 3.1 Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

#### 3.2 Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

#### 3.3 Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

#### 3.4 Intellectual Property Matters

(a) Third Party Claims.  
If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

#### (b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API,

Contributor must also include this information in the LEGAL file.

#### (c) Representations

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

#### 3.5 Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

#### 3.6 Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

#### 3.7 Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

#### 4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

#### 5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A, and to related Covered Code.

#### 6. Versions of the License.

##### 6.1 New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

##### 6.2 Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

##### 6.3 Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename

Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

#### 7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABILITY, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

#### 8. TERMINATION.

8.1 This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2 If You initiate litigation by asserting a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3 If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4 In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

#### 9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF



INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

- 10. U.S. GOVERNMENT END USERS.  
The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.
- 11. MISCELLANEOUS.  
This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.
- 12. RESPONSIBILITY FOR CLAIMS.  
As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.
- 13. MULTIPLE-LICENSED CODE.  
Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

**EXHIBIT A -Mozilla Public License.**

"The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/MPL/>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is \_\_\_\_\_.  
The Initial Developer of the Original Code is \_\_\_\_\_.  
Portions created by \_\_\_\_\_ are Copyright (C) \_\_\_\_\_, All Rights Reserved.

Contributor(s): \_\_\_\_\_.

Alternatively, the contents of this file may be used under the terms of the \_\_\_\_\_ license (the "[ ] License"), in which case the provisions of [ ] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [ ] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [ ] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [ ] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

### 11.4.7 NTP License

This file is automatically generated from [html/copyright.htm](http://html/copyright.htm)

**Copyright Notice**

[Dolly the sheep] "Clone me," says Dolly sheepishly

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

```

/*****
 *
 *
 * Copyright (c) David L. Mills 1992-2000
 *
 *
 * Permission to use, copy, modify, and distribute this software and
 * its documentation for any purpose and without fee is hereby
 * granted, provided that the above copyright notice appears in all
 * copies and that both the copyright notice and this permission
 * notice appear in supporting documentation, and that the name
 * University of Delaware not be used in advertising or publicity
 * pertaining to distribution of the software without specific,
 * written prior permission. The University of Delaware makes no
 * representations about the suitability this software for any
 * purpose. It is provided "as is" without express or implied
 * warranty.
 *
 *****/

```

- The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.
1. [1]Mark Andrews <marka@syd.dms.csiro.au> Leitch atomic clock controller
  2. [2]Viraj Bais <vbais@mailman1.intel.com> and [3]Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
  3. [4]Michael Barone <michael,barone@lmco.com> GPSVME fixes
  4. [5]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
  5. [6]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and isogonal code into separate modules.
  6. [7]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
  7. [8]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
  8. [9]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
  9. [10]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
  10. [11]Sven Dietrich <sven\_dietrich@trimble.com> Palisade reference clock driver, NT adj, residuals, integrated Greg's Winnt port.
  11. [12]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
  12. [13]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
  13. [14]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
  14. [15]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
  15. [16]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
  16. [17]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
  17. [18]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
  18. [19]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
  19. [20]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [21]<H.Lambermont@chello.nl> ntpswep
  20. [22]Frank Kardel [23]<Frank.Kardel@informatik.uni-erlangen.de> PARSE <GENERIC> driver (14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup
  21. [24]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
  22. [25]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
  23. [26]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
  24. [27]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
  25. [28]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
  26. [29]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbitr, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
  27. [30]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
  28. [31]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
  29. [32]Tom Moore <tmoore@fieval.daytonoh.ncr.com> i386 svr4 port
  30. [33]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
  31. [34]Derek Mulcahy <derek@toybox.demon.co.uk> and [35]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
  32. [36]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
  33. [37]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
  34. [38]Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
  35. [39]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
  36. [40]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
  37. [41]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
  38. [42]Michael Shields <shields@tembel.org> USNO clock driver
  39. [43]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
  40. [44]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
  41. [45]Kenneth Stone <ken@sdd.hp.com> HP-UX port
  42. [46]Ajit Thyagarajan <ajit@ee.udel.edu>P multicast/anycast support
  43. [47]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
  44. [48]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
  45. [49]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

[50]Home  
[51]David L. Mills <mills@udel.edu>

#### References

1. mailto:marka@syd.dms.csiro.au
2. mailto:vbais@mailman1.intel.com
3. mailto:kirkwood@striderfm.intel.com
4. mailto:michael.barone@lmco.com
5. mailto:karl@owl.HQ.ileaf.com
6. mailto:greg.brackley@bigfoot.com
7. mailto:Marc.Brett@westgeo.com
8. mailto:Piete.Brooks@cl.cam.ac.uk
9. mailto:cliff@ml.csiro.au
10. mailto:casey@csc.co.za
11. mailto:Sven\_Dietrich@trimble.COM
12. mailto:dundas@salt.jpl.nasa.gov
13. mailto:duwe@immd4.informatik.uni-erlangen.de
14. mailto:dennis@mrbill.canet.ca
15. mailto:glenn@herald.usask.ca
16. mailto:iglesias@uci.edu
17. mailto:jagubox.gsfc.nasa.gov
18. mailto:jb@chatham.usdesign.com
19. mailto:jones@hermes.chpc.utexas.edu
20. mailto:Hans.Lambermont@nl.origin-it.com
21. mailto:H.Lambermont@chello.nl
22. www4.informatik.uni-erlangen.de/~kardel
23. mailto:Frank.Kardel@informatik.uni-erlangen.de
24. mailto:dkatz@cisco.com
25. mailto:leres@ee.lbl.gov
26. mailto:lindholm@ucs.ubc.ca
27. mailto:louie@ni.umd.edu
28. mailto:thorinn@diku.dk
29. mailto:mills@udel.edu
30. mailto:moeller@gwdgv1.dnet.gwdg.de
31. mailto:mogul@pa.dec.com
32. mailto:tmoores@fivel.daytonoh.ncr.com
33. mailto:kamal@whence.com
34. mailto:derek@toybox.demon.co.uk
35. mailto:d@hd.org
36. mailto:Rainer.Pruy@informatik.uni-erlangen.de
37. mailto:dirce@zk3.dec.com
38. mailto:wsanchez@apple.com
39. mailto:mrapple@quack.kfu.com
40. mailto:jack@innovativeinternet.com
41. mailto:schnitz@unipress.com
42. mailto:shields@tembel.org
43. mailto:pebbles.jpl.nasa.gov
44. mailto:harlan@pfcs.com
45. mailto:ken@sdd.hp.com
46. mailto:ajit@ee.udel.edu
47. mailto:tsuruoka@nc.fukuoka-u.ac.jp
48. mailto:vixie@vix.com
49. mailto:Ulrich.Windl@rz.uni-regensburg.de
50. file://localhost/backroom/ntp4+/html/index.htm
51. mailto:mills@udel.edu

## 11.4.8 PSF Python Software Foundation License

The Python Software Foundation (PSF) holds the copyright of Python 2.1 and newer versions.

#### PSF LICENSE AGREEMENT FOR PYTHON 2.4

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 2.4 software in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 2.4 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001,

2002, 2003, 2004 Python Software Foundation; All Rights Reserved" are retained in Python 2.4 alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 2.4 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.4.
4. PSF is making Python 2.4 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.4 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.4 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.4, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python 2.4, Licensee agrees to be bound by the terms and conditions of this License Agreement.

## 11.4.9 XFree86 Licenses

Version 1.1 of XFree86 Project Licence.

Copyright (C) 1994-2004 The XFree86®Project, Inc. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution, and in the same place and form as other copyright, license and disclaimer information.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by The XFree86 Project, Inc (http://www.xfree86.org/) and its contributors", in the same place and form as other third-party acknowledgments. Alternately, this acknowledgment may appear in the software itself, in the same form and location as other such third-party acknowledgments.
4. Except as contained in this notice, the name of The XFree86 Project, Inc shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from The XFree86 Project, Inc.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE XFREE86 PROJECT, INC OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## 11.5 phion Software Subscription

### Präambel

Der Kunde hat von phion die Nutzungsberechtigung für bestimmte Softwaremodule der Software "phion netfence", "phion airlock", "entegra", "M", "management centre" oder anderen von phion hergestellten und vertriebenen Softwareprodukten (im folgenden kurz "Software") erworben. Er ist daran interessiert, dass er Weiterentwicklungen der Software erhält und Verbesserungen der Software von phion zur Verfügung gestellt werden. phion ist an einer dauerhaften Kundenbeziehung und daran interessiert, dass die Software auch nach einiger Zeit ihren hohen Ansprüchen genügt. Aus diesen Gründen bietet phion dem Kunden Software Subscription zu folgenden Bedingungen an.

### §1 Voraussetzung für Software Subscription

Der Kunde ist berechtigt, Software Subscription für ein bestimmtes Produkt bei phion zu bestellen, wenn eine der folgenden Bedingungen erfüllt ist (Standard-Bedingungen):

1. Seit dem Erwerb einer Lizenz für den Einsatz des phion Produkts ist nicht mehr als ein Jahr vergangen.
2. Es besteht für das Produkt eine gültige, nicht abgelaufene Software Subscription Vereinbarung.
3. Seit dem Ablauf der letzten gültigen Subscription Vereinbarung ist nicht mehr als ein Jahr vergangen.

In diesen 3 Fällen beginnt die Laufzeit der Software Subscription im ersten Fall mit dem 1. des auf das Erwerbsdatum folgenden Kalendermonat, im zweiten und dritten Fall direkt anschließend an die Beendigung der bestehenden beziehungsweise abgelaufenen Software Subscription Vereinbarung. Entsprechend dem Bestellzeitpunkt innerhalb dieser Fristen folgt, dass das Recht des Kunden auf Updates auf die Restlaufzeit der Software Subscription Vereinbarung beschränkt ist.

Der Kunde ist weiters berechtigt, Software Subscription für ein bestimmtes Produkt bei phion zu bestellen, wenn die folgende Bedingung erfüllt ist:

1. Seit dem Lizenzerwerb oder seit dem Ablauf der letzten gültigen Subscription Vereinbarung ist mehr als ein Jahr vergangen.

In diesem Fall hat der Kunde das Recht, wieder Software Subscription für einen bestimmten Zeitraum zu erwerben, indem er Legacy Subscription erwirbt. Mit dem Erwerb der Legacy Subscription erhält der Kunde dieselben Rechte, als ob er unter Standard Bedingungen Software Subscription erworben hätte. Und damit auch wieder das Recht zu den ersten drei Bedingungen weiterhin Software Subscription zu erwerben.

### §2 Umfang der Software Updates

phion wird dem Kunden die von ihr geschaffenen Weiterentwicklungen und Verbesserungen der Software gemäß den Bestimmungen dieses Vertrages zur Verfügung stellen. Die jeweils aktuellen Lizenzbedingungen der phion gelten sinngemäß auch für Software, die dem Kunden aufgrund einer Software Subscription Vereinbarung zur Verfügung gestellt wird.

Die Software ist durch eine aus drei Zahlen bestehende Bezeichnung nach dem System Version.Major.Minor bestimmt, wobei die erste Zahl die Programmversion, die zweite Major Updates (Anpassungen der Software an geänderte Rahmenbedingungen) und die dritte Minor Updates (Bugfixes und kleinere Änderungen der Software, ohne dass deren Funktionalität wesentlich verändert wird) kennzeichnet.

Die Weiterentwicklung und Verbesserung der Software erfolgt durch die Erstellung von neuen Versionen sowie Major Updates und Minor Updates. phion entscheidet dabei nach eigenem Ermessen, wann und welche Art von Updates erstellt werden und ist nicht verpflichtet, auf jede technische Veränderung mit einem Update zu reagieren.

Die Updates werden dem Kunden nach Markteinführung auf einer CD übergeben oder im Internet zum Download freigegeben. Die Installation der Updates nimmt der Kunde selbst vor.

Der gegenständliche Software-Update Vertrag bezieht sich ausdrücklich, ausschließlich auf die von phion entwickelte Software und nicht auf gegebenenfalls mitgelieferte Open-Source-Software oder sonstige Software, die zwar von phion verwendet wird, nicht jedoch von phion stammt.

Die Updates gelten nur für die gesamte Lizenz und nicht für Teile, die hiervon erworben werden.

### §3 Ausführung des Updates

Für den Fall, dass der Kunde die Programm-Updates installiert, hat er sämtliche Anweisungen von phion hinsichtlich der Installation und

Nutzung der Programm-Updates zu beachten. Eine entsprechende Anleitung wird zur Verfügung gestellt.

### §4 Kompatibilität von Updates

Soweit von Kunden oder Dritten, Anpassungen in der Anwendungslogik von Programmen oder Teilen hiervon vorgenommen werden, gewährleistet phion nicht, dass die Updates vollständig nutzbar sind.

Der Kunde erkennt an, dass der Einsatz von Updates möglicherweise den Einsatz von Konversionsscripts zur Anpassung der bestehenden Datenmodelle an neue Datenmodelle erforderlich macht. Für den Fall, dass die Updates auf der Open-Source-Software nicht störungsfrei funktionieren, übernimmt phion keinerlei Gewährleistung und Haftung für die Funktionsfähigkeit der Updates. Für vom Kunden oder Dritten hergestellte Anpassungen werden keine Konversionsscripts zur Verfügung gestellt.

phion übernimmt keine Gewährleistung, dass die Software nach Durchführung eines Updates oder auch nach einer Neuinstallation der aktuelleren Software mit der bisher für die Software eingesetzten Hardware kompatibel ist.

### §5 Vergütung

Für die Leistungen gemäß dieser Software-Subscription-Bedingungen erhält phion einen Pauschalbetrag. Mit der Bezahlung dieses Betrags erwirbt der Kunde das Recht auf alle Software Updates, die von phion für das von ihm erworbene Produkt innerhalb des festgelegten Zeitraums zur Verfügung gestellt werden. Sollte kein Zeitraum festgelegt werden, so gilt als fixierter Zeitraum ein Kalenderjahr nach Einlangen der Bestellung der Software Subscription bei phion.

Wenn im Vertriebsweg nichts anderes vereinbart wird, gilt folgende Regelung:

Dieser Betrag ist jährlich unmittelbar nach Bestellung und Rechnungslegung zur Zahlung fällig. Im Falle eines Zahlungsverzuges des Kunden ist phion berechtigt, Verzugszinsen in Höhe von 8 % über dem jeweils gültigen Dreimonats-EURIBOR zu verrechnen. Das Recht zur sofortigen Kündigung gemäß § 6 bleibt davon unberührt.

### §6 Gewährleistung

phion leistet lediglich für ausdrücklich zugesagte Eigenschaften der Updates Gewähr. Sollte dabei ein Mangel auftreten, kann phion diesen nach eigener Wahl durch Verbesserung oder Austausch des mangelhaften Updates beheben. Darüber hinausgehende Gewährleistungsansprüche sind ausgeschlossen.

Gewährleistungsansprüche sind insbesondere ausgeschlossen, wenn der Kunde die Software nicht in der von phion vorgegebenen Weise installiert und/oder benützt oder wenn der Kunde oder Dritte Veränderungen an der Software oder betreffend die Integration der Software in das System des Kunden vornehmen. Die Gewährleistungsfrist beträgt 1 Jahr, handelt es sich beim Kunden um einen Konsumenten im Sinne des KSchG, so beträgt die Frist 2 Jahre.

### §7 Haftung

Es gelten die Haftungsbestimmungen der phion Lizenzbedingungen in der jeweils aktuellen Form.

### §8 Laufzeit der Software Subscription und Kündigung

Der Anspruch des Kunden beginnt je nach Voraussetzung (siehe §1) und dauert 1 Kalenderjahr, sofern nicht anderes vereinbart wird. Der Anspruch verlängert sich nicht automatisch und muss unter den Bedingungen von §1 erneuert werden.

Darüber hinaus ist phion berechtigt, laufende Software Subscription mit sofortiger Wirkung aus wichtigem Grund zu kündigen, der insbesondere dann vorliegt, wenn der Kunde gegen Bestimmungen der jeweils aktuellen Lizenzbedingungen der phion oder dieser Software-Subscription-Bedingungen verstößt oder wenn phion aufgrund von technischen oder sonstigen Umständen keine Updates der Softwareversion herstellt, oder dies unwirtschaftlich geworden ist.

### §9 Umfang der Software Subscription

Wird vom Kunden Software Subscription für ein phion Produkt erworben, so muss diese alle von ihm erworbenen Lizenzen umfassen. Es ist nicht möglich, nur teilweise für die erworbenen Lizenzen Software Subscription zu erwerben. Dies gilt auch für neu erworbene Software. Wird trotz Aufforderung die Software Subscription nicht auf die gesamte eingesetzte Lizenzbasis ausgedehnt, gilt dies als wichtiger Grund, bestehende Software Subscription Rechte seitens phion zu kündigen.

### §10 Schlussbestimmungen

Änderungen dieser Software Subscription Bedingungen bedürfen der Schriftform. Das gleiche gilt auch für das Abgehen vom Schriftformerfordernis.

Sollte eine Bestimmung dieses Software Subscription Bedingungen unwirksam sein oder werden, beeinträchtigt ein solcher Mangel die übrigen Bestimmungen dieses Vertrages nicht. Die mangelhafte Bestimmung gilt als durch eine wirksame Bestimmung ersetzt, die den wirtschaftlichen und rechtlichen Auswirkungen, die die Vertragsparteien von der mangelhaften Bestimmung erwartet haben, am nächsten kommt.

Alle Rechte und Pflichten aus diesem Vertragsverhältnis auf die

etwaigen Rechtsnachfolger der Vertragspartner über. phion hat darüber hinaus das Recht, alle Rechte und Pflichten aus diesem Vertrag an einen Dritten zu überbinden.

Für eventuelle Streitigkeiten gilt ausschließlich die örtliche Zuständigkeit des sachlich zuständigen Gerichtes in Innsbruck als vereinbart; ist der Kunde Verbraucher im Sinne des KSchG, dessen allgemeiner Gerichtsstand.

Es wird die Anwendbarkeit ausschließlich österreichischen Rechtes, mit Ausnahme sowohl des UN-Kaufrechts (Vienna Convention on the Sale of Goods) als auch der Verweisungsnormen des Internationalen Privatrechts (IPRG) vereinbart.

## 11.6 phion Software Subscription Conditions

### Preamble

Customer has acquired from phion a license to use certain software modules of the "phion netfence", "phion airlock", "entegra", "M", "management centre" software (hereinafter referred to as "Software"). Customer is interested in receiving further developments and enhancements of the Software from phion. phion is interested in a lasting customer relationship and wants that the Software will satisfy the high demands of Customer also after some time. For the said reasons phion offers Customer software subscription in accordance with the following terms and conditions.

### §1 Prerequisite for software subscription

Customer shall be entitled to order from phion software subscription for a certain product if one of the following conditions (standard conditions) is fulfilled:

1. Not more than one year has passed since the purchase of a licence to use the phion product.
2. There is a valid software subscription agreement regarding the product which has not expired.
3. Not more than one year has passed since expiration of the last valid subscription agreement.

In those three cases the term of the software subscription shall commence on the first day of the calendar month following the date of purchase in the first case, in the second and third case directly following the end of the existing or expired software subscription agreement. In accordance with the date of the purchase order within the said periods it is agreed that the Customer's right to updates shall be limited to the residual term of the software subscription agreement.

Moreover, Customer shall be entitled to order software subscription for a certain product from phion if the following condition is fulfilled:

1. More than one year has passed since the expiration of the last valid subscription agreement.

In that case Customer shall be entitled to purchase software subscription for a certain period by purchasing legacy subscription. By purchasing legacy subscription Customer shall receive the same rights as if he had purchased software subscription under standard conditions, and, thus, again the right to purchase software subscription subject to the first three conditions.

### §2 Scope of software updates

phion shall provide Customer with further developments and enhancements of the software created by phion in accordance with the terms and conditions of this contract. The most recent licensing conditions of phion shall apply mutatis mutandis to software which is provided to Customer on the basis of a software subscription agreement.

The Software is identified by a three-digit number according to the version.major.minor system, the first digit indicating the programme version, the second digit indicating major updates (adaptation of software to changed framework conditions) and the third digit indicating minor updates (bug fixes and minor changes to the Software without materially changing the Software's functionality).

Further development and enhancement of the Software shall be effected by creating new versions, major updates and minor updates. phion shall decide at its own discretion when and what kind of updates will be created and shall not be obliged to respond to every technological change by an update.

Updates shall be provided to Customer on a CD after market launch or shall be released for downloading on the internet. Updates shall always be installed by Customer itself.

This software update agreement shall expressly and exclusively relate to the Software developed by phion and not to open source software or other software delivered along with it, which phion does use, but which does not originate from phion.

The updates shall only apply to the entire license and not for parts thereof which are purchased.

### §3 Installation of updates

In the case that Customer installs the programme updates he shall follow all instructions of phion with regard to installation and use of the programme updates. Relevant instruction shall be provided.

### §4 Compatibility of updates

IF CUSTOMER OR THIRD PARTIES MAKE ADAPTATIONS IN THE APPLICATION LOGIC OF PROGRAMMES OR PARTS THEREOF, PHION

DOES NOT WARRANT THAT THE UPDATES ARE FULLY USEABLE.

CUSTOMER ACKNOWLEDGES THAT USE OF UPDATES MAY NECESSITATE USE OF CONVERSION SCRIPTS TO ADAPT EXISTING DATA MODELS TO NEW DATA MODELS. IN THE CASE THAT UPDATES DO NOT WORK PROPERLY ON THE OPEN SOURCE SOFTWARE PHION SHALL NOT ASSUME ANY WARRANTY OR LIABILITY FOR RUNNABILITY OF THE UPDATES. CONVERSION SCRIPTS SHALL NOT BE PROVIDED WITH REGARD TO ADAPTATIONS MADE BY CUSTOMER OR THIRD PARTIES.

PHION DOES NOT WARRANT THAT THE SOFTWARE IS COMPATIBLE WITH THE HARDWARE USED SO FAR AFTER AN UPDATE HAS BEEN INSTALLED OR AN UPDATED SOFTWARE HAS BEEN NEWLY INSTALLED.

#### **§5 Remuneration**

phion shall receive a flat fee for the services rendered under these terms and conditions of software subscription. Upon payment of the said amount Customer shall acquire the right to all software updates which are provided by phion for the product Customer purchased during the agreed period. If no period has been fixed, one calendar year after phion's receipt of the purchase order for software subscription shall be deemed the period fixed.

Unless otherwise agreed in the course of distribution, the following regulation shall apply:

This amount shall be due for payment annually, immediately after issuance of the purchase order and issuance of the invoice. If Customer is in default of payment, phion shall be entitled to charge default interest at a rate of at least 8 % p.a. above the three-months EURIBOR applicable from time to time. The right to terminate the contract with immediate effect as defined in Clause 6 shall remain unaffected.

#### **§6 Warranty**

phion shall fulfil its warranty obligations only for properties of updates which were expressly promised. If a defect occurs in this context, phion shall repair such defect, at its own discretion, either by improvement or by replacement of the defective update. Any further warranty claims shall be excluded.

Warranty claims shall be excluded in particular if Customer does not install and/or use the Software in the way prescribed by phion or if Customer or third parties notify the Software or with regard to integration of the Software into the Customer's system. The warranty period shall be one year; if Customer is a consumer as defined by the KSchG [Austrian Consumer Protection Act], that period shall be two years.

#### **§7 Liability**

THE PROVISIONS ON LIABILITY OF THE LICENSING CONDITIONS OF

PHION AS AMENDED FROM TIME TO TIME SHALL APPLY.

#### **§8 Term of Software Subscription and Termination**

Customer's claim shall commence in accordance with the relevant prerequisite (see Clause 1) and shall last one calendar year unless otherwise agreed. The claim shall not be renewed automatically and must be renewed in accordance with the conditions of Clause 1.

Moreover, phion shall be entitled to terminate current software subscription with immediate effect for good cause, which shall include but not be limited to a violation of provisions of the relevant most recent licensing conditions of phion or these terms and conditions of software subscription by Customer or a situation where phion does not make any updates of the software version due to technological or other circumstances or where such creation is no longer economical.

#### **§9 Scope Of Software Subscription**

If Customer purchases software subscription for a phion product, the said subscription shall include all licenses purchased by Customer. It shall not be possible to purchase software subscription only for parts of the purchased licenses. This shall also apply to newly purchased Software. If despite a request the software subscription is not extended to the entire license basis used, this shall constitute a good cause for phion to terminate the existing software subscription rights.

#### **§10 Final Provisions**

Modifications of these terms and conditions of software subscription shall be made in writing. This shall also apply to a waiver of the requirement of written form.

If a provision of these terms and conditions of software subscription is or becomes ineffective, such a defect shall not affect the remaining provisions of this contract. The defective provision shall be deemed replaced by an effective provision which comes as close as possible to the economic and legal effects which the contracting parties expected from the defective provision.

All rights and obligations under this contractual relationship shall pass to the legal successors, if any, of the parties. Moreover, phion shall be entitled to impose all rights and obligations under this agreement on a third party.

The court having jurisdiction over the subject matter and over Innsbruck shall have exclusive jurisdiction regarding any disputes; if Customer is a consumer as defined by the Austrian Consumer Protection Act, Customer's general place of jurisdiction shall be the legal venue.

Austrian law shall apply exclusively; UN Sales Law (Vienna Convention on Contracts for the International Sale of Goods) and the conflict of laws rules of the Austrian Statute on Private International Law (IPRG) shall be excluded.



## 11.7 phion Lizenzbedingungen für Klienten-Applikationen

### §1 Präambel

- (1) phion AG, Eduard-Bodem-Gasse 1, 6020 Innsbruck, FN: 184392 s (im folgenden kurz "phion" genannt), hat die Software phion.a, sowie entegra VPN client und netfence entegra sowie andere Applikationen für Windows oder andere Betriebssysteme entwickelt, die Teil der Produktfamilien "phion netfence", "phion M", "phion airlock" oder weiterer von phion vertriebenen Produktfamilien sind, (künftig kurz als "Software" bezeichnet) entwickelt. phion ist Inhaber aller sich aus dem Urheberrecht an der Software ergebenden Leistungsschutz- und Nutzungsrechte an dieser Software.
- (2) Die Software läuft auf dem jeweiligen Betriebssystem. Das Betriebssystem und die mitgelieferten Softwarepakete unterliegen eigenen Lizenzen und sind nicht Gegenstand dieser Nutzungsbedingungen. Es wird ausdrücklich festgehalten, dass die Software keine Bearbeitung oder Weiterentwicklung des Betriebssystems ist. Die gegenständlichen Nutzungsbedingungen betreffen somit ausschließlich die von phion entwickelte Software.
- (3) Die phion Software wurde unter Einbeziehung einiger bestehender Softwarepakete entwickelt, an denen Rechte Dritter bestehen. Die Lizenzbedingungen dieser Software finden sich als Anhang.

### §2 Test der Software

- (1) Die Software ist zu Evaluierungszwecken erhältlich. Die Software kann an sich kostenlos genutzt und getestet werden. Die Software ist nur im Zusammenhang mit einer Implementierung eines phion netfence Systems sinnvoll einsetzbar. Der Umfang des Gebrauchs der Software wird von diesen Systemen teilweise eingeschränkt.
- (2) phion gibt ausdrücklich keine Gewähr und sichert nicht zu, dass die Software auf einem Betriebssystem lauffähig ist und dies gilt auch für zukünftige Versionen dieser Betriebssysteme.

### §3 Benutzung

- (1) phion gewährt dem Kunden ab der Ausstellung des Lizenz-Zertifikats unter der Bedingung der rechtzeitigen Bezahlung der Lizenzgebühren, auf unbeschränkte Zeit ein nicht ausschließliches Recht zur Installation und Nutzung des Programmes auf einem Datenspeicher. Die Lizenz bezieht sich ausschließlich auf die Nutzung des Programmes durch den Kunden für seine eigenen Datenverarbeitungsprozesse. Der Kunde ist nicht berechtigt, Dritten Zugang zum Programm zu gewähren. Der Kunde verpflichtet sich, die Software gesichert aufzubewahren, sodass ein Zugang und somit ein Kopieren oder Benutzen der Software durch Dritte verhindert wird. Der Kunde erhält das Recht, ausschließlich für sicherungs- oder archivarische Zwecke Kopien des Programmes anzufertigen.
- (2) Der Kunde ist berechtigt das Programm in dem Umfang zu nutzen wie es für die gewöhnliche Nutzung des Programmes erforderlich ist.
- (3) Soweit durch zwingende gesetzliche Vorschriften nicht anderwärtig vorgesehen, ist der Kunde nicht berechtigt, das Programm vom Objektcode zum Quellcode (z.B. durch "Reverse Engineering", Disassemblierung oder Dekompilierung) zu übersetzen.
- (4) Der Kunde ist nicht berechtigt, den Licence-Key aufzubrechen oder zu ändern. Er ist nicht berechtigt, irgendwelche Hinweise im Bezug auf Rechte, Marken oder Ähnlichem, die in dem Programm oder auf dem Medium, auf dem das Programm enthalten ist, angegeben werden, zu verändern, oder zu löschen.
- (5) Der Kunde ist nicht berechtigt, das Programm an Dritte zu übertragen, zu vermieten, zu verleasen, zu verleihen oder auf andere Weise Dritten vorübergehend zur Verfügung zu stellen. Er ist darüber hinaus nicht berechtigt, die Software auf irgendeine Weise zu bearbeiten, zu verändern, oder in andere Computerprogramme zu integrieren.
- (6) Die Lizenz kann über einen Licence-Key an die Hardwarekonfiguration gebunden sein. Bei Änderungen der Hardwarekonfiguration, steht es phion frei, dem Kunden kostenlos einen weiteren Licence-Key auszustellen. Der Kunde verliert damit das Recht, den ersten Licence-Key weiter zu benutzen. phion ist berechtigt, darüber den Nachweis binnen 14 Tagen nach Erhalt des neuen Licence-Keys zu verlangen.
- (7) Der Export in Drittländer hat nach den zum Zeitpunkt des Exports/Imports jeweils gültigen EU-Richtlinien stattzufinden. Die alleinige Verantwortung zur Einhaltung dieser Richtlinien liegt beim exportierenden bzw. importierenden Reseller oder Endkunden. Von phion gelieferte Produkte sind zur Benutzung und zum Verbleib innerhalb der EU bestimmt. Die Wiederausfuhr - einzeln oder in systemintegrierter Form - ist für den Kunden genehmigungspflichtig und unterliegt dem jeweiligen Außenwirtschaftsrecht sowie den US Export Regulations, deren Kenntnis und Beachtung dem Kunden obliegt. Der Wiederverkauf an Kunden im nuklearen Bereich, insbesondere im Bereich der Herstellung und des Betriebs von Nukleartechnik, erfordert spezielle Genehmigungen. phion behält sich das Recht vor, die gegenständlichen Bestimmungen zum Export und

Import jederzeit anzupassen, sofern es die nationale oder internationale Gesetzgebung erfordert.

- (8) Die Verantwortung für die Auswahl, die Installation und den Gebrauch des Lizenzmaterials und die durch den Einsatz angestrebte Problemlösung liegt beim Lizenznehmer. Der Lizenznehmer ist zudem für Auswahl, Gebrauch und Unterhalt der im Zusammenhang mit der Software eingesetzten Informatiksysteme, weiterer Programme und Datensysteme sowie die dafür erforderlichen Dienstleistungen zuständig und stellt die für den Einsatz der Software geeignete Organisation bereit.
- (9) Der Lizenzgeber hat das Recht, sich unter Wahrung der Geschäfts- und Betriebsgeheimnisse des Lizenznehmers von der Einhaltung des bestimmungsgemäßen Gebrauchs der Software zu überzeugen.

### §4 Kaufpreis

- (1) Wenn im Vertriebsweg nichts anderes vereinbart wird, gilt folgende Regelung:  
Der Kaufpreis für das Computerprogramm samt Lizenz-Zertifikat ist innerhalb von 14 Tagen nach der Auslieferung des Lizenz-Zertifikats, ohne dass es einer weiteren Rechnungslegung für die Fälligkeit des Kaufpreises bedarf, auf das Geschäftskonto von phion zu überweisen. Gerät der Kunde mit der Bezahlung des Kaufpreises in Verzug, ist phion berechtigt, Verzugszinsen in Höhe von 8 Prozent über dem jeweils gültigen Dreimonats-EURIBOR per annum zu berechnen.

### §5 Haftungsbestimmungen

- (1) Einvernehmlich festgehalten wird, dass dem Kunden die Software auf einem Datenträger oder als Download zur Verfügung gestellt wurde. Der Kunde verpflichtet sich, die Funktionsfähigkeit und Mängelfreiheit der zur Verfügung gestellten Software während einer Testphase zu überprüfen und allfällige Mängel analog zu § 377 UGB zu rügen. Mit der Bestellung des Lizenz-Zertifikats gemäß dem Bestellformular, bestätigt der Kunde die Überprüfung der Software und eventuell des Datenträgers auf ihre Mängelfreiheit und bestätigt diese. Einvernehmlich wird für die Testphase in Hinblick auf deren Testcharakter die Gewährleistung für Sachmängel ausgeschlossen. In jedem Falle ist die Gewährleistung auf sechs Wochen beschränkt.
- (2) Für Konsumenten beträgt die Gewährleistungsfrist zwei Jahre. Die Bestimmungen des Konsumentenschutzgesetzes bleiben in Geltung, soweit es sich um ein Geschäft mit Endverbrauchern handelt. In diesem Fall ist phion berechtigt, ihre Gewährleistungsverpflichtungen durch Austausch der gelieferten Sache zu erfüllen.
- (3) Ferner übernimmt phion keine Gewähr für Fehler, Störungen oder Schäden, die auf unsachgemäße Bedienung, Verwendung ungeeigneter Organisationsmittel, anomale Betriebsbedingungen (insbesondere Abweichungen von den Installationsbedingungen) sowie auf Transportschäden zurückzuführen sind. Für Programme, die durch eigene Programmierer des Kunden bzw. Dritte nachträglich verändert werden, entfällt jegliche Gewährleistung durch phion.
- (4) phion sind keine Rechte Dritter bekannt, die der Einräumung der gewährten Nutzungsrechte an der Software entgegenstehen. Wird der Kunde wegen Verletzung von Immaterialgüterrechten Dritter aufgrund der Nutzung der von phion gelieferten Software oder von Teilen oder Komponenten davon in Anspruch genommen, wird phion den Kunden schad- und klaglos halten, wenn der Kunde phion den Sachverhalt unverzüglich anzeigt und phion alle Verhandlungen überlässt. Der Kunde ist nicht befugt, diesbezüglich irgendwelche Anerkennungserklärungen abzugeben. Der Kunde bevollmächtigt phion zu seiner Vertretung im Bezug auf diesbezügliche Streitigkeiten und verpflichtet sich gemeinsam mit phion geeignete Schritte für die Abwehr der geltend gemachten Ansprüche zu ergreifen.
- (5) Für den Fall, dass berechtigte Ansprüche Dritter geltend gemacht werden, wird phion die notwendigen Vorkehrungen treffen und allenfalls die Rechte erwerben, oder gleichwertige Teile und Komponenten liefern.
- (6) phion haftet für Schäden, sofern ihr oder ihren Mitarbeitern Vorsatz oder grobe Fahrlässigkeit nachgewiesen werden, im Rahmen der gesetzlichen Vorschriften. Die Haftung für leichte Fahrlässigkeit wird einvernehmlich und im gesetzlich zulässigen Ausmaß ausgeschlossen. Der Ersatz von Folgeschäden und Vermögensschäden, nicht erzielten Ersparnissen, Zinsverlust, indirekten Schäden und von Schäden aus Ansprüchen Dritter jeglicher Art gegen phion ist in jedem Fall ausgeschlossen. phion haftet nicht für Schadenersatz bei Daten-, Software- oder Hardwarezerstörung, wenn der Kunde seinen Pflichten zum ordnungsgemäßen EDV-Betrieb und der regelmäßigen Datensicherung nicht bzw. nicht ausreichend nachgekommen ist. Schadenersatzansprüche gegen phion sind, sofern es sich beim Vertragspartner nicht um einen Konsumenten handelt, bei sonstigem Verfall binnen eines Jahres ab Schadenseintritt gerichtlich geltend zu machen.

### §6 Programmverbesserungen (Updates) und Programmänderungen

- (1) Der Kunde erwirbt mit dem Lizenz-Zertifikat keinerlei Recht auf weitergehende Betreuung durch phion sowie auf die Lieferung von Updates oder Programmweiterungen.
- (2) Selbst wenn die Software keine Lizenzverletzung anzeigt, ist das Update von Systemen, deren Software Subscription nicht mehr aktuell



ist, eine schwere Lizenzverletzung und der Kunde ist verpflichtet, Software Subscription, wie in den Software Subscription Bedingungen beschrieben, nachzukaufen.

- (3) Manche Funktionalitäten, vor allem Updates von Content Security Patterns oder ähnlichen Komponenten, die regelmäßig auf den neuesten Stand gebracht werden, stehen nur bei aufrechten Subscriptionrechten zur Verfügung.

#### §7 Kundendaten

- (1) Der Kunde erklärt sich ausdrücklich damit einverstanden, dass ihn betreffende Daten, die phion im Rahmen der Geschäftsverbindung mit dem Kunden bekannt werden, von phion zum Zweck der Benachrichtigung über die Entwicklung von Updates und neuen Programmversionen und zum Angebot von Wartungsverträgen und weiteren Angeboten gesammelt und bearbeitet werden.
- (2) Der Kunde nimmt zustimmend zur Kenntnis, dass seine persönlichen Daten von phion zum Zwecke der internen Datenerfassung, Datenverarbeitung und zur Benachrichtigung über die Entwicklung im Zusammenhang mit dem gelieferten Produkt und von Updates und neuen Programmversionen gespeichert und verarbeitet werden. Der Kunde erklärt sich gemäß § 107 TKG ausdrücklich damit einverstanden, derartige Benachrichtigungen auch per email zu empfangen.

#### §8 Urheberrechtlicher Schutz der Software

- (1) Der Kunde nimmt ausdrücklich zur Kenntnis, dass phion Inhaber sämtlicher sich aus dem Urheberrecht ergebender Leistungsschutz- und Nutzungsrechte ist. Im Falle des Verstoßes des Kunden gegen diese Rechte und sonstige zwingende urheberrechtliche Bestimmungen, stehen phion sämtliche im Urheberrechtsgesetz vorgesehenen Rechtsbehelfe zur Verteidigung des urheberrechtlichen Schutzes zu.
- (2) Teile der Software enthalten von Dritten entwickelte Software, die urheberrechtlichen Schutz genießt. Diese Softwarelizenzbestimmungen sind im Anhang dieser Nutzungsbestimmungen angeführt und stellen einen integrierenden Bestandteil dieser Bestimmungen dar.

#### §9 Schlussbestimmungen

- (1) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder unwirksam werden, so wird hierdurch der übrige Teile des Vertrages nicht berührt. Die Vertragspartner werden partnerschaftlich zusammenwirken um eine Regelung zu finden, die den unwirksamen Bestimmungen möglichst nahe kommt.
- (2) Soweit nicht zwingende gesetzliche Bestimmungen entgegenstehen, gelten die zwischen Vollkaufleuten zur Anwendung kommenden gesetzlichen Bestimmungen nach österreichischem Recht, auch dann, wenn der Auftrag im Ausland ausgeführt wird.
- (3) Für eventuelle Streitigkeiten gilt ausschließlich die örtliche Zuständigkeit des sachlich zuständigen Gerichtes in Innsbruck als vereinbart; ist der Kunde Verbraucher im Sinne des KSchG, dessen allgemeiner Gerichtsstand..
- (4) Es wird die Anwendbarkeit ausschließlich österreichischen Rechtes, mit Ausnahme sowohl des UN-Kaufrechts (Vienna Convention on the Sale of Goods) als auch der Verweisungsnormen des Internationalen Privatrechts (IPRG) vereinbart.

## 11.8 phion License for Client Applications

### §1 Preamble

- (1) phion AG, Eduard-Bodem-Gasse 1, 6020 Innsbruck, FN [Business Register Number] 184392 s (hereinafter referred to as "phion") has developed the software phion.a and entegra VPN client and netfence entegra as well as other applications for Windows or other operating systems, which are part of the product families "phion netfence", "phion M", "phion airlock" and other by phion distributed product families (hereinafter referred to as "Software"). phion is the owner of all proprietary rights to and rights to use the Software which result from the copyright to the Software.
- (2) The Software runs on the relevant operating system. The operating system and the software packages provided along with it are subject to separate licenses and shall not be the subject matter of these Terms and Conditions of Use. It is expressly put on record that the Software does not constitute a edited version or further development of the operating system. These Terms and Conditions of Use therefore exclusively apply to the Software developed by phion.
- (3) The phion Software was developed by inclusion of some existing software packages to which rights of third parties exist. The licensing conditions regarding that software are attached hereto.

### §2 Testing of the Software

- (1) The Software is available for evaluation purposes. The Software may be used and tested free of charge. The Software can only be reasonably used in connection with implementation of a phion netfence system. The scope of use of the Software will be partly restricted by those systems.
- (2) PHION EXPRESSLY NEITHER REPRESENTS NOR WARRANTS THAT THE SOFTWARE WILL RUN ON AN OPERATING SYSTEM AND THIS SHALL ALSO APPLY TO FUTURE VERSIONS OF THOSE OPERATING SYSTEMS.

### §3 Use

- (1) Subject to timely payment of the license fees phion shall grant Customer an exclusive right to install and use the programme on a data storage device from issuance of the license certificate for an indefinite period of time. The license exclusively concerns the use of the programme by Customer for its own data processing processes. Customer shall not be entitled to grant third parties access to the programme. Customer undertakes to keep the Software safe so that access and, thus, copying or using the Software by third parties is prevented. Customer shall be granted the right to make copies of the programme exclusively for backup or archiving purposes.
- (2) Customer shall be entitled to use the programme to the extent necessary for ordinary use of the programme.
- (3) Unless provided otherwise by mandatory statutory provisions, Customer shall not be entitled to translate the programme from object code into source code (e.g. by reverse engineering, disassembling or decompiling).
- (4) Customer shall not be entitled to crack or change the license key. Customer shall not be entitled to modify or delete any notes regarding rights, trademarks or the like which are stated in the programme or on the medium on which the programme is stored.
- (5) Customer shall not be entitled to transfer, let, lease, lend or otherwise temporarily make available the programme to third parties. Moreover, Customer shall not be entitled to process or modify the Software in any way or to integrate it into other computer programmes.
- (6) The license may be linked to the hardware configuration via a license key. In the case of modifications of the hardware configuration phion shall be free to issue another license key to Customer free of charge. Customer shall then lose the right to continue to use the first license key. phion shall be entitled to request evidence thereof within fourteen days of receipt of the new license key.
- (7) Export to third countries shall be effected in accordance with the EU directives applicable at the time the export/import takes place. The exporting and/or importing reseller or end customer shall be solely responsible for compliance with the said directives. Products delivered by phion are designed for being used and for remaining in the EU. Re-export, be it separately or integrated into a system, shall be subject to approval to be obtained by Customer and shall be subject to the relevant foreign trade legislation and to US Export Regulations for the knowledge of and compliance with which Customer shall be responsible. Reselling to customers in the nuclear area, in particular in the area of manufacturing and operation of nuclear technology, shall require special permits. phion reserves the right to adjust the provisions on export and import at any time if national or international legislation so requires.
- (8) The Customer is responsible for the choice, installation and usage of the licensed Software and the intended solution. The Customer is responsible for usage and choice of the technological environment and

the necessary services and the organisation to operate the systems properly.

- (9) The Customer has the right to get evidence that the licensed Software is used according to the license conditions. phion has to do this without breaching any industrial and company secrets of the Customer.

#### §4 Purchase Price

- (1) Unless otherwise agreed in the course of distribution, the following regulation shall apply:  
The purchase price for the computer programme including the license certificate shall be transferred to the company account of phion within fourteen days of delivery of the license certificate without another invoice for the due purchase price being necessary. If Customer is in default of payment of the purchase price, phion shall be entitled to charge default interest at a rate of 8 % p.a. above the three-months EURIBOR applicable from time to time.

#### §5 Liability Provisions

- (1) THE PARTIES MUTUALLY AGREE AND PUT ON RECORD THAT THE SOFTWARE SHALL BE PROVIDED TO CUSTOMER ON A DATA CARRIER OR AS A DOWNLOAD. CUSTOMER UNDERTAKES TO CHECK WORKABILITY AND FREEDOM FROM DEFECTS OF THE PROVIDED SOFTWARE DURING A TEST PHASE AND TO NOTIFY ANY DEFECTS IN ACCORDANCE WITH SECTION 377 UGB [AUSTRIAN BUSINESS CODE]. UPON ORDERING THE LICENSE CERTIFICATE IN ACCORDANCE WITH THE PURCHASE ORDER FORM CUSTOMER CONFIRMS THAT THE SOFTWARE AND THE DATA CARRIER, IF ANY, HAVE BEEN CHECKED FOR FREEDOM FROM DEFECTS AND CONFIRMS THAT FREEDOM FROM DEFECTS EXISTS. WARRANTY FOR DEFECTS IN QUALITY DURING THE TEST PHASE SHALL BE EXCLUDED BY MUTUAL CONSENT IN VIEW OF THE TESTING CHARACTER. IN ANY CASE WARRANTY SHALL BE LIMITED TO SIX WEEKS.
- (2) FOR CONSUMERS THE WARRANTY PERIOD SHALL BE TWO YEARS. THE PROVISIONS OF THE AUSTRIAN CONSUMER PROTECTION ACT SHALL REMAIN IN FORCE TO THE EXTENT THAT A TRANSACTION WITH END CONSUMERS IS CONCERNED. IN THAT CASE PHION SHALL BE ENTITLED TO FULFIL ITS WARRANTY OBLIGATIONS BY REPLACING THE DELIVERED ITEM.
- (3) FURTHERMORE PHION SHALL ASSUME NO WARRANTY FOR ERRORS/BUGS, FAILURES OR DAMAGE WHICH WERE CAUSED BY IMPROPER OPERATION, USE OF UNSUITABLE ORGANISATIONAL RESOURCES, ABNORMAL OPERATING CONDITIONS (IN PARTICULAR DEVIATIONS FROM THE INSTALLATION CONDITIONS) AS WELL AS BY TRANSPORTATION DAMAGE. IN THE CASE OF PROGRAMMES WHICH ARE SUBSEQUENTLY CHANGED BY PROGRAMMERS WORKING FOR THE CUSTOMER OR THIRD PARTIES, PHION SHALL BE UNDER NO WARRANTY WHATSOEVER.
- (4) phion is not aware of any rights of third parties which would prevent the granting of the rights to use the Software granted. If Customer is held liable for infringement of intellectual property rights of third parties due to use of the Software delivered by phion or of parts or components thereof, phion shall indemnify and hold Customer harmless provided that Customer immediately notifies such fact to phion and leaves all negotiations to phion. Customer shall not be allowed to issue any declarations of acknowledgement in this context. Customer shall authorise phion to represent Customer with regard to such disputes and undertakes to take suitable steps jointly with phion in defence of the asserted claims.
- (5) In the case that justified claims of third parties are asserted, phion shall take the necessary steps and, if necessary, acquire rights or deliver equivalent parts and components.
- (6) PHION SHALL BE LIABLE FOR DAMAGE WITHIN THE SCOPE OF THE STATUTORY PROVISIONS IF IT CAN BE PROVEN THAT SUCH DAMAGE WAS CAUSED BY PHION OR ITS STAFF WILFULLY OR WITH GROSS NEGLIGENCE. LIABILITY FOR ORDINARY NEGLIGENCE SHALL BE EXCLUDED BY MUTUAL AGREEMENT AND TO THE EXTENT PERMITTED BY LAW. COMPENSATION FOR CONSEQUENTIAL DAMAGE AND PECUNIARY LOSS, SAVINGS NOT EARNED, LOSS OF INTEREST, INDIRECT DAMAGE AND FOR DAMAGE FROM THIRD-PARTY CLAIMS OF ANY KIND AGAINST PHION SHALL BE EXCLUDED IN ANY CASE. PHION SHALL NOT BE LIABLE FOR DAMAGES IN CASE OF DESTRUCTION OF DATA, SOFTWARE OR HARDWARE IF CUSTOMER DID NOT FULFIL OR DID NOT SUFFICIENTLY FULFIL ITS OBLIGATIONS OF OPERATING THE EDP PROPERLY AND TO MAKE TIMELY DATA BACKUPS. UNLESS THE CONTRACTING PARTY IS A CUSTOMER, CLAIMS FOR DAMAGES AGAINST PHION SHALL BE ASSERTED WITHIN ONE YEAR OF OCCURRENCE OF THE DAMAGE; OTHERWISE THEY SHALL FORFEIT.

#### §6 Enhancements of Programmes (Updates) and Modifications of Programmes

- (1) BY PURCHASING THE LICENSE CERTIFICATE CUSTOMER SHALL NOT ACQUIRE ANY RIGHT TO FURTHER SUPPORT BY PHION OR TO DELIVERY OF UPDATES OR PROGRAMME EXTENSIONS.
- (2) Using Software Updates on systems where no valid software subscription was purchased is severe infringement of license rights,

even the software does not prove the validity of the right to update. The customer is due to purchase the needed Software Subscription as described in the Software Subscription conditions.

- (3) Some functionality may be available only if a valid Software Subscription has been purchased. This is especially the case for content security and similar components which are updated on a regular basis.

#### §7 Customer Data

- (1) Customer expressly agrees that data concerning the Customer which becomes known to phion within the scope of the business relationship with Customer shall be collected and processed by phion for the purpose of information about the development of updates and new programme versions and for offering of maintenance contracts and for other offers.
- (2) Customer acknowledges and agrees that its personal data be stored and processed by phion for the purpose of internal data collection, data processing and for information about the development in connection with the delivered product and of updates and new programme versions. In accordance with Section 107 TKG [Austrian Telecommunications Act] Customer expressly agrees to receipt of such information also by e-mail.

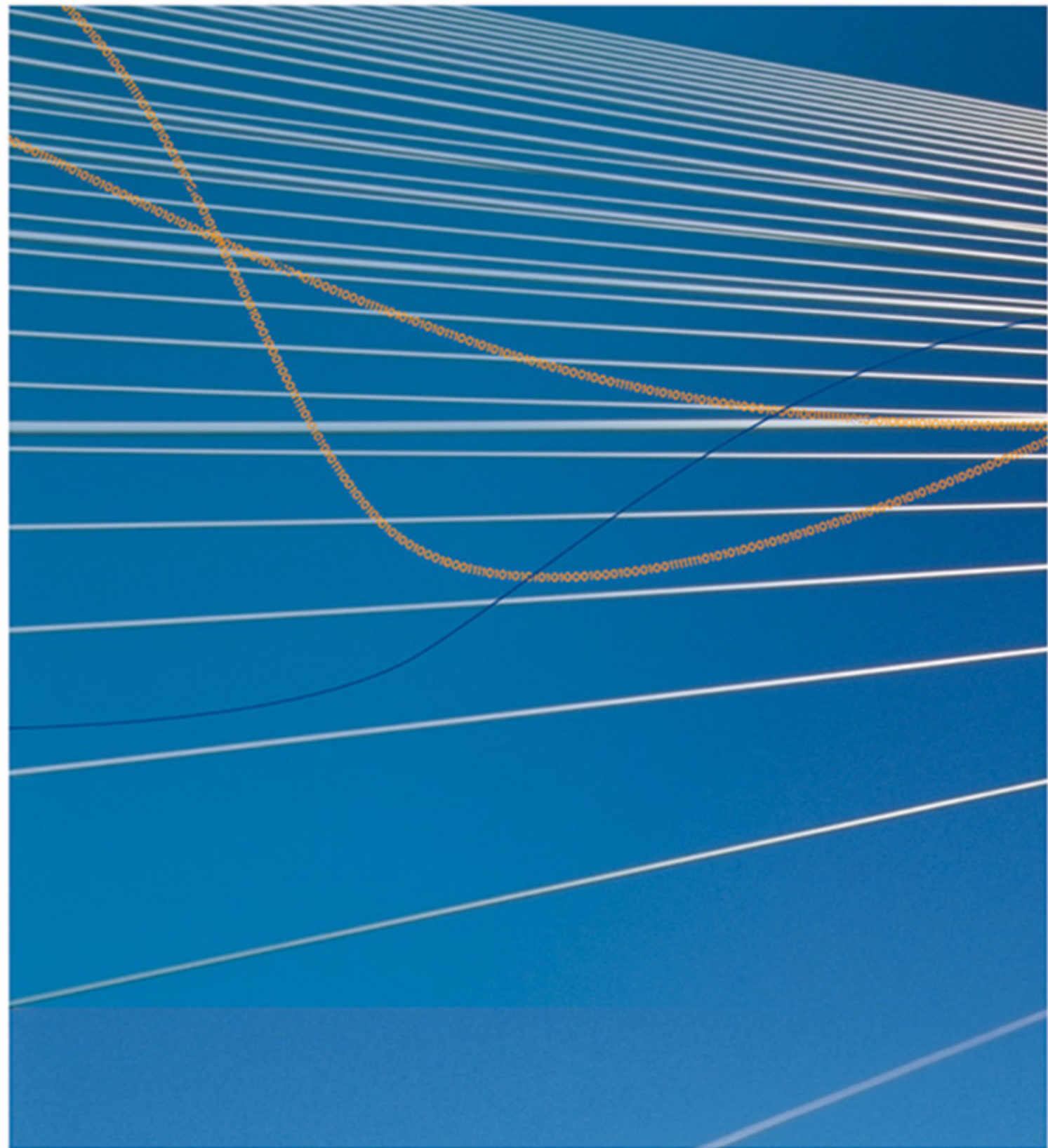
#### §8 Copyright of Software

- (1) Customer expressly acknowledges that phion is the owner of all proprietary rights and rights to use the Software which result from copyright. In case Customer violates such rights and other mandatory copyright provisions, phion shall be entitled to all legal remedies which are provided for under copyright law to defend copyrights protection.
- (2) Parts of the Software contain software developed by third parties which is under copyright protection. Those licensing conditions for software are contained in the Annex to these Terms and Conditions of Use and shall form an integral part hereof.

#### §9 Final Provisions

- (1) If individual provisions of this contract are or become ineffective, the remaining provisions of this contract shall not be affected. The contracting parties shall co-operate as partners in order to find a provision which comes as close as possible to the ineffective provisions.
- (2) Unless mandatory statutory provisions provide otherwise, the statutory provisions of Austrian law applicable to full merchants shall exclusively apply, even if the order is rendered abroad.
- (3) The court having jurisdiction over the subject matter and over Innsbruck shall have exclusive jurisdiction regarding any disputes; if Customer is a consumer as defined by the Austrian Consumer Protection Act, Customer's general place of jurisdiction shall be the legal venue.
- (4) Austrian law shall apply exclusively; UN Sales Law (Vienna Convention on Contracts for the International Sale of Goods) and the conflict of laws rules of the Austrian Statute on Private International Law (IPRG) shall be excluded.





[www.phion.com](http://www.phion.com)

**phion** 

© phion AG  
Eduard-Bodem-Gasse 1  
6020 Innsbruck  
Austria  
Phone +43 (0)508 100  
Fax +43 (0)508 100 20  
[office@phion.com](mailto:office@phion.com)  
[www.phion.com](http://www.phion.com)