TheGreenBow IPSec VPN Client

Configuration Guide

ZyXEL ZyWALL 35 firmware 4.01

WebSite: http://www.thegreenbow.com

Contact: support@thegreenbow.com

Table of contents

1. Introduction

1.1 Goal of this document

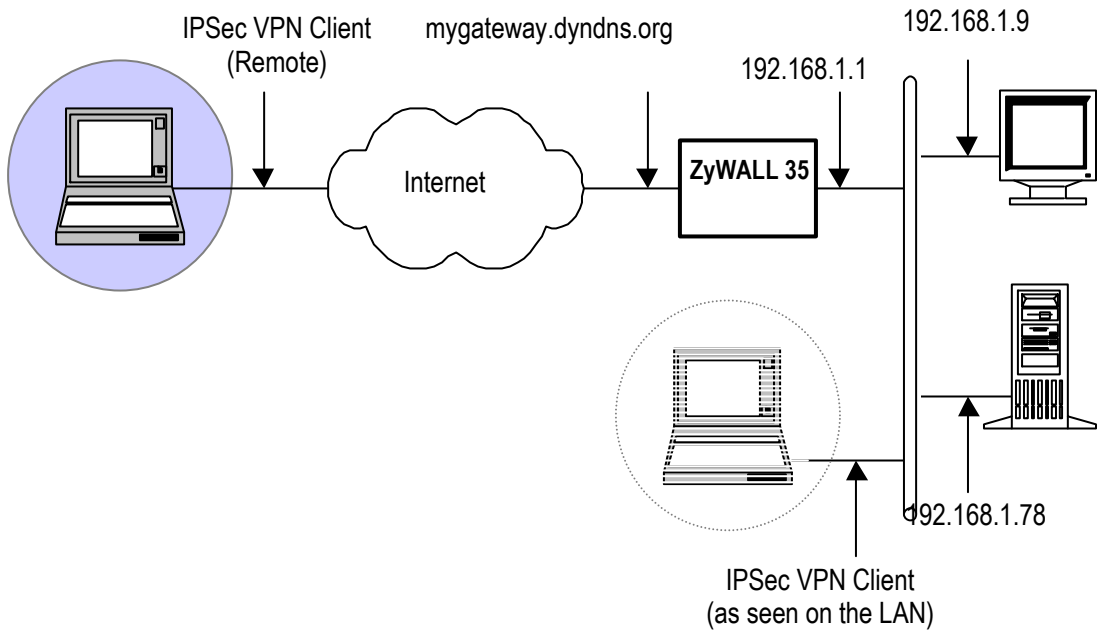
This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a ZyXEL ZyWALL 35 firmware 4.01 using certificates. We'll be using ZyWALL built in Certification Authority.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the ZyXEL firewall. The VPN client is connected to the Internet with a DSL connection or from a LAN. All the addresses in this document are given for example purpose.

A Road Warrior connection also needs to be configured. The following example makes use of these values:

- External IP of the ZyWALL: mygateway.dyndns.org (or public IP address)
- LAN 192.168.1.0/255.255.255.0

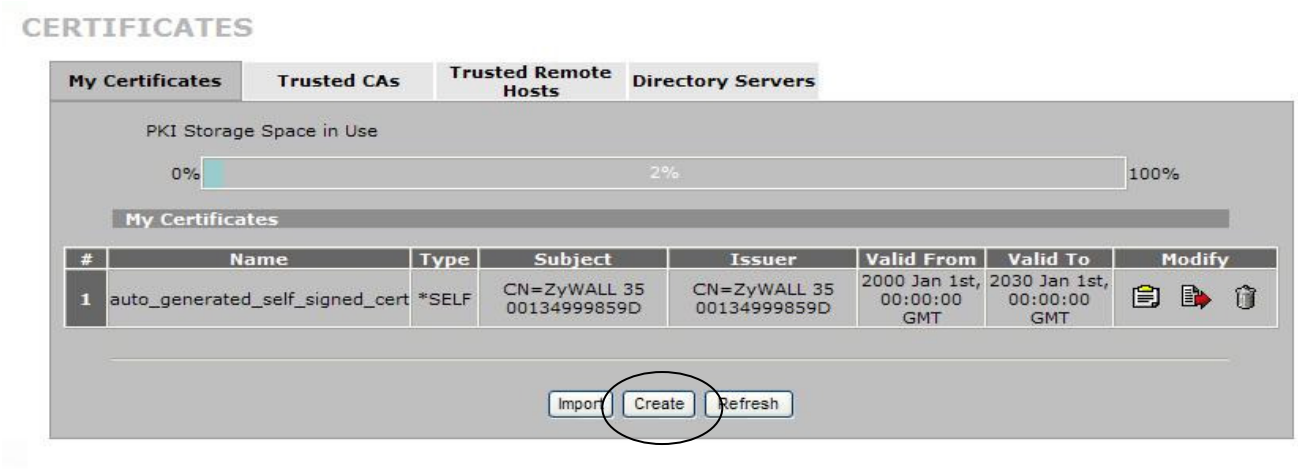


2 Setup ZyWALL35

2.1 Prepare ZyWALL's built in Certification Authority

Root certificate is created the first time the ZyWALL is powered on. This is an automatic process.

Go to "Security" menu, then "Certificates" to obtain this screen:

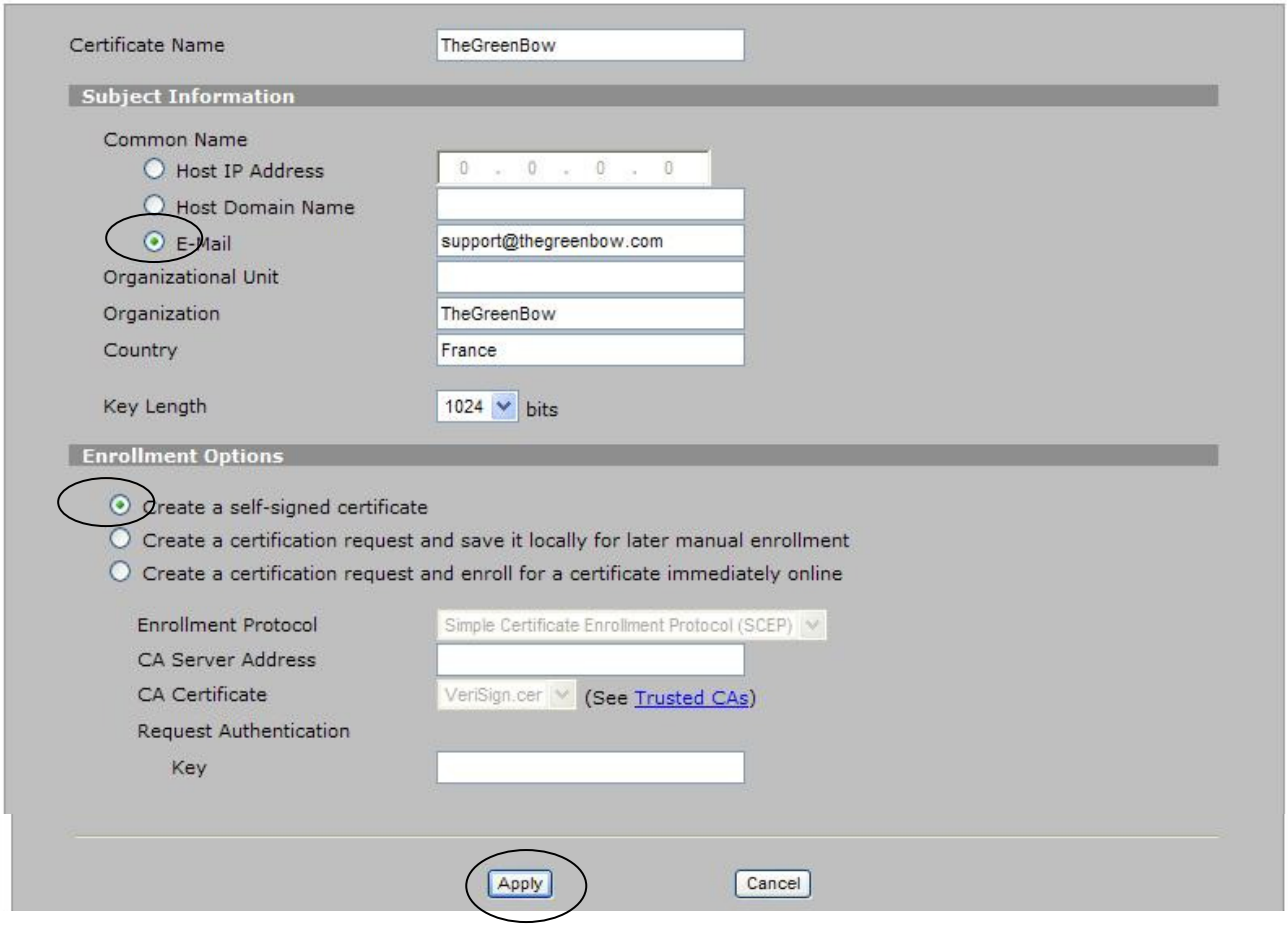


Press "Create" to configure a host to net ipsec connection

2.2 Create a Roadwarrior certificate

Enter the certificate name, and choose the subject informations type : email or ip address or host domain name

In this example we chose to use email adress



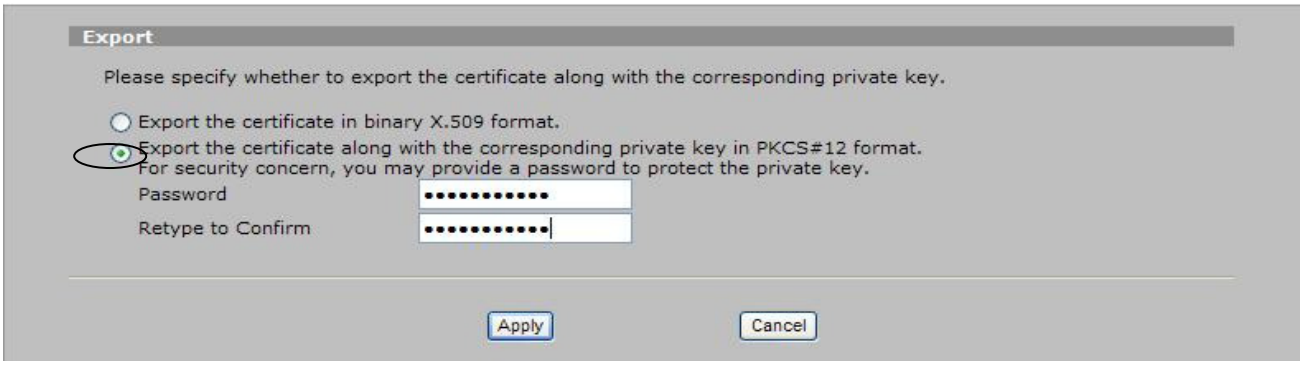
Choose the enrollment options. In our example, we are using ZyWALL built in certifications authority, therefore create a self-signed certificate must be selected.

Press “Apply”.

Once the certificate creation process is done, the main certificate screen shows:

For later use we need now to export both root and roadwarrior certificates in PKCS12 format.

Click on export icons to go to this screen:



Choose PKCS#12, and enter a password.

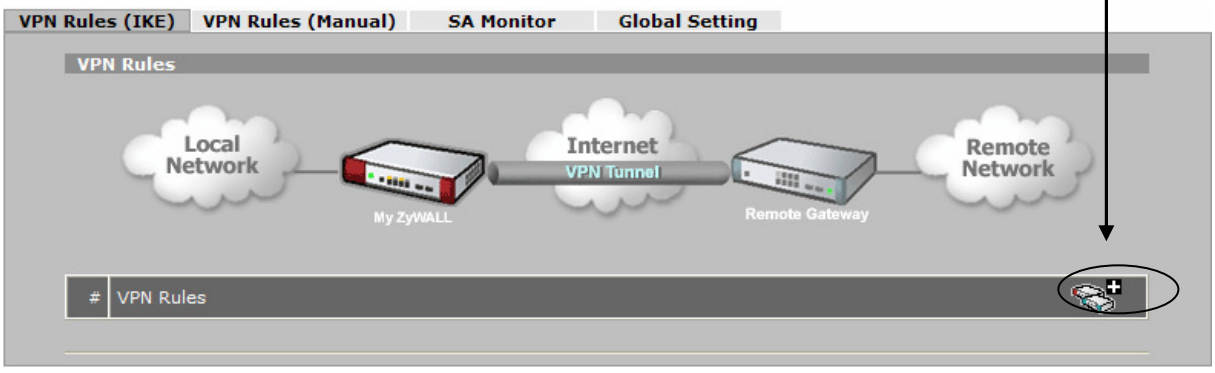
DO THIS FOR BOTH CERTIFICATES.

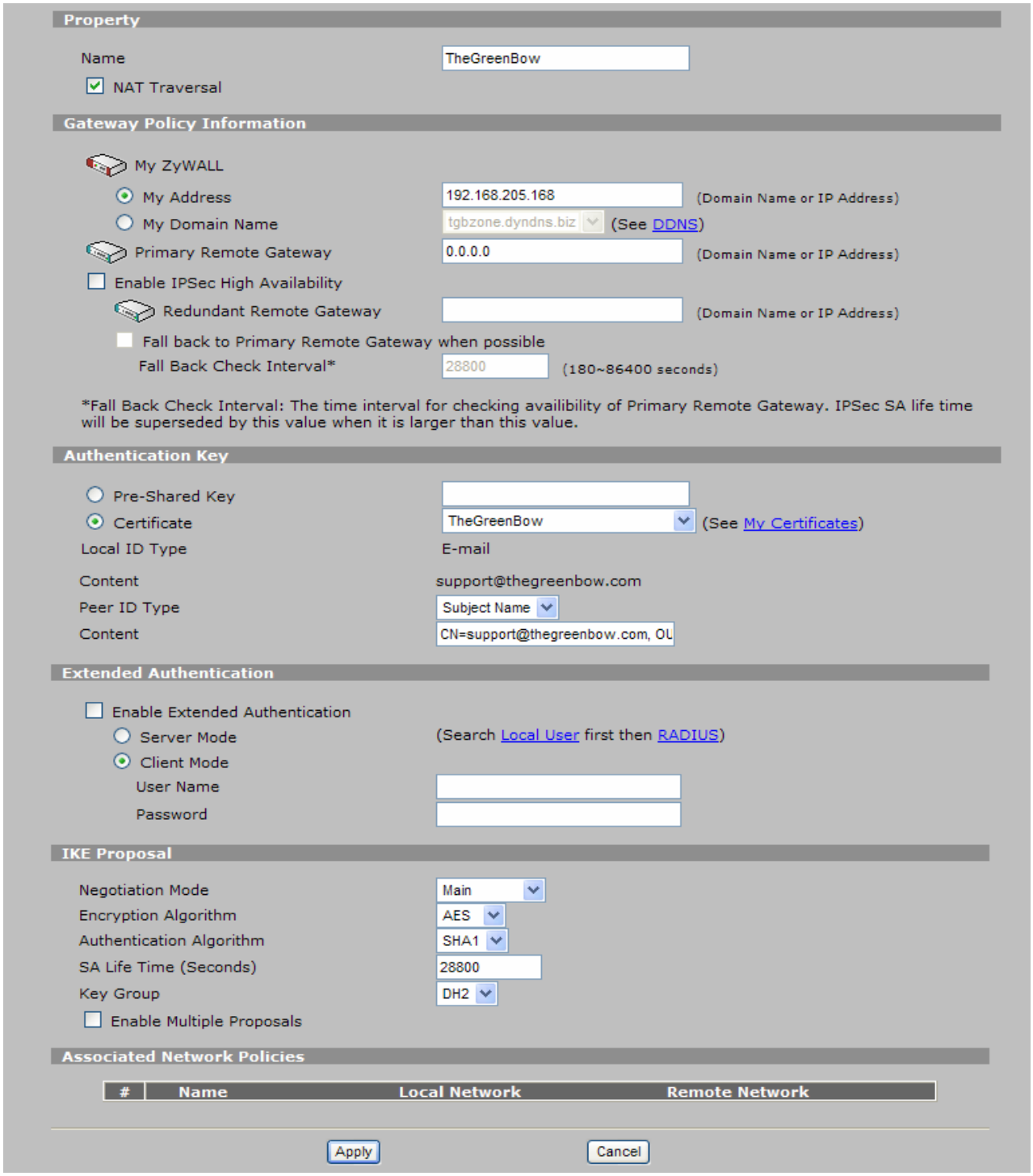
Add “p12” extension on the popup window, or rename certificates after they have been saved.

2.3 Create a Roadwarrior vpn tunnel

Go to VPN tab and click the “add gateway policy” button

:





In “Gateway Policy Informations”, the wan address (“My Address”) is a private subnet address. Replace it by a static wan public address if you have one, or enter a dynamic dns name in “My Domain Name”.

In “Authentication Key” select the roadwarrior certificate previously created.

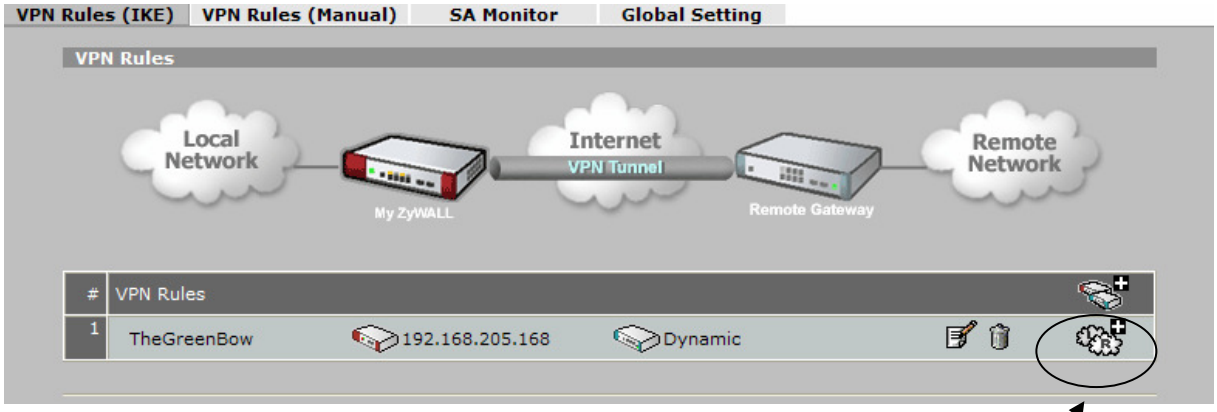
Local ID will be automatically defined from the certificate created. In our example it is email address.

Remote ID: choose a type from the drop down menu and enter a value. It can be setup to “any”. But to increase security, choose “subject name” and in the value field, copy and paste the subject of roadwarrior certificate (you can find it on “certificates” page)

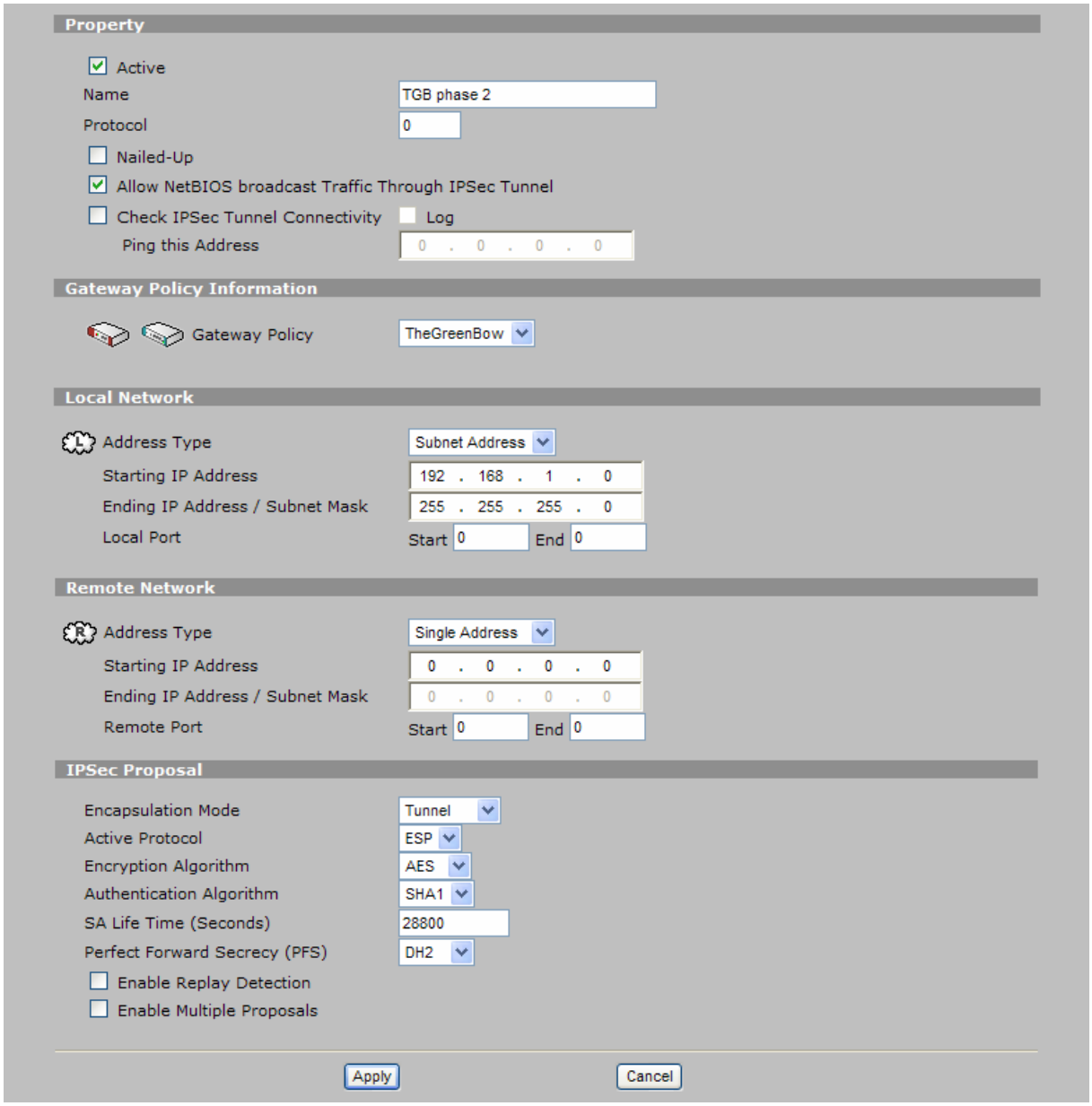
To increase security, “Extended Authentication” can be used by entering a user name and password. In this case the vpn client should be configured accordingly in phase1 advanced by checking x-auth popup OR entering a username and password (login and pwd are sent automatically without any popup).

In “IKE Proposal”, choose algorithms (for firmware 4.01, AES and SHA1 are the best choice). The longest key that can be chosen is DH2 (1024 bits).

Press Apply to save settings and return to vpn main screen:



A network policy linked to this gateway policy must be added. Press the add network policy button



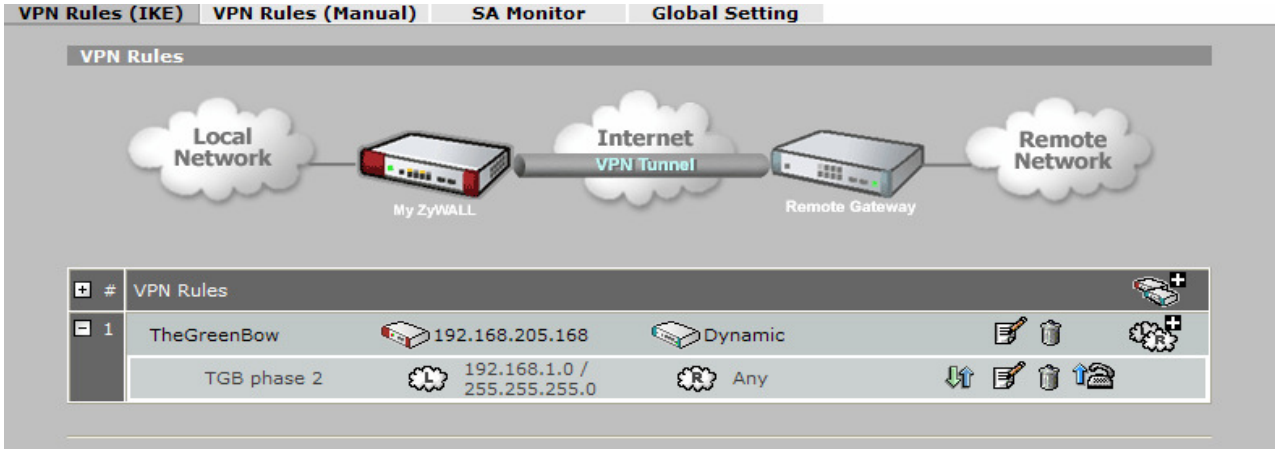
Check “Allow Netbios Broadcast” to be able to browse distant network.

In “Local Network”, define either a single ip address, either an address range or a subnet address, depending on what machine(s) you wish to access through vpn. In this example, a subnet was defined.

In “Remote Network”, leave single address setting with 0.0.0.0, meaning “any” address for the client. If you specify an address here, the vpn client must be set up accordingly, as the router will only accept requests from the address entered.

Choose algorithms and pfs (perfect forward secrecy) settings.

Press “Apply”, the Zywall 35 is now configured.



3 Setup TheGreenBow VPN client 3.1x

3.1 Prepare certificates for TheGreenBow vpn client 3.1x

Transfer both previously created PKCS#12 certificates (on floppy disk or usb stick, or email, or direct copy) to the nomad pc initiator of the vpn tunnel.

Use our tool here: http://www.thegreenbow.fr/bin/tgbvpn_certificates.zip to convert them into “pem” which is the usable certificate format for our vpn client.

Once the conversion is done 4 files are created for EACH certificate.

rootCA.pem

clientcert.pem

Der_asn1_DN.txt

Local.key

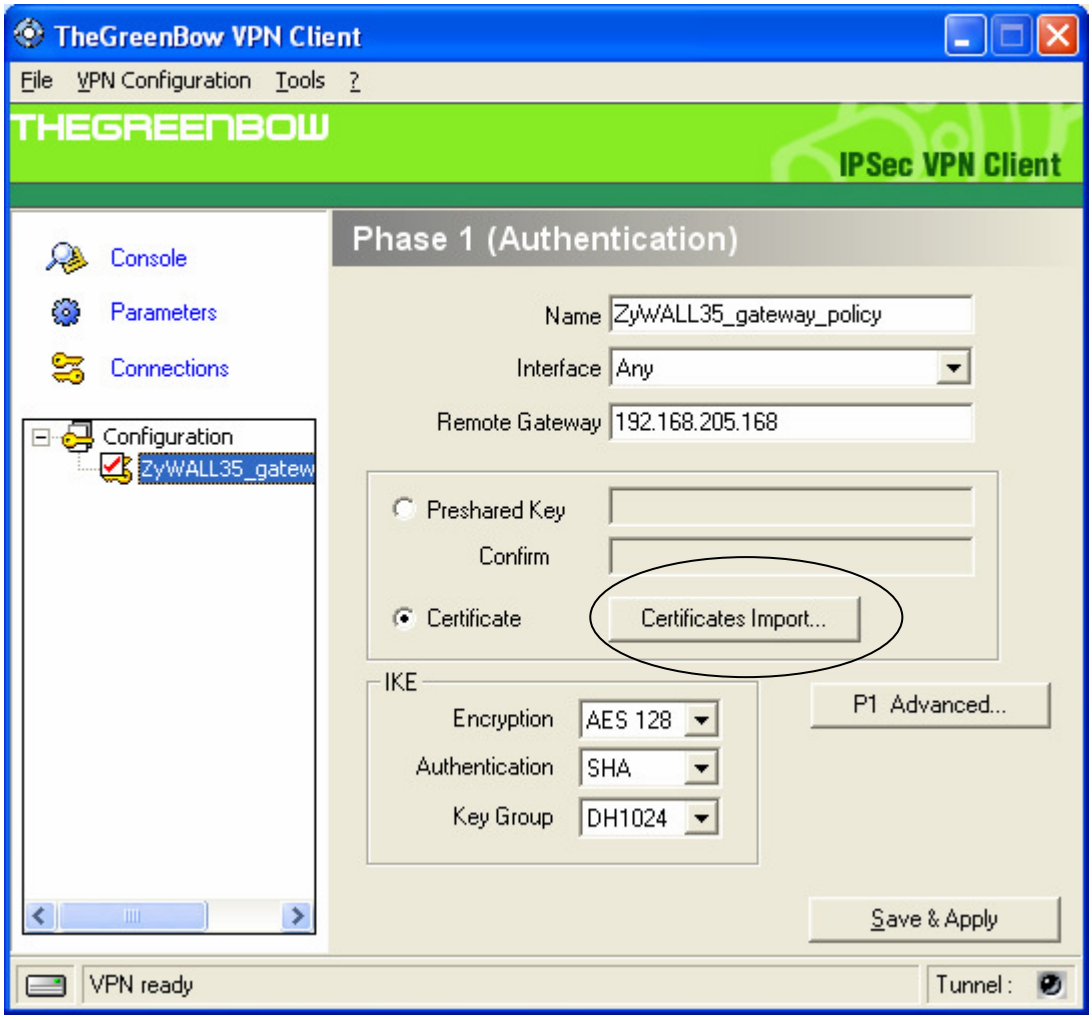
Both conversions will provide same names. Make sure to distinguish Certification Authority pem files from Roadwarrior pem files (by creating 2 folders for example). This will avoid messing with them when importing to the vpn client.

3.2 Phase 1 Configuration

Right click on Configuration in **TheGreenbow** VPN client and select “**New Phase 1**”. Phase 1 settings should match the gateway policy on the ZyXEL.

Choose a name for your connection to ZyWALL and enter the remote gateway which is the WAN IP address of the ZyXEL, or its dynamic dns name if it has been defined.

Select certificate box and press “certificates import”



Press browse for each certificate and go to the locations where pem files were saved previously.

Make sure you select the correct certificate between Certification authority folder and client (roadwarrior) folder.

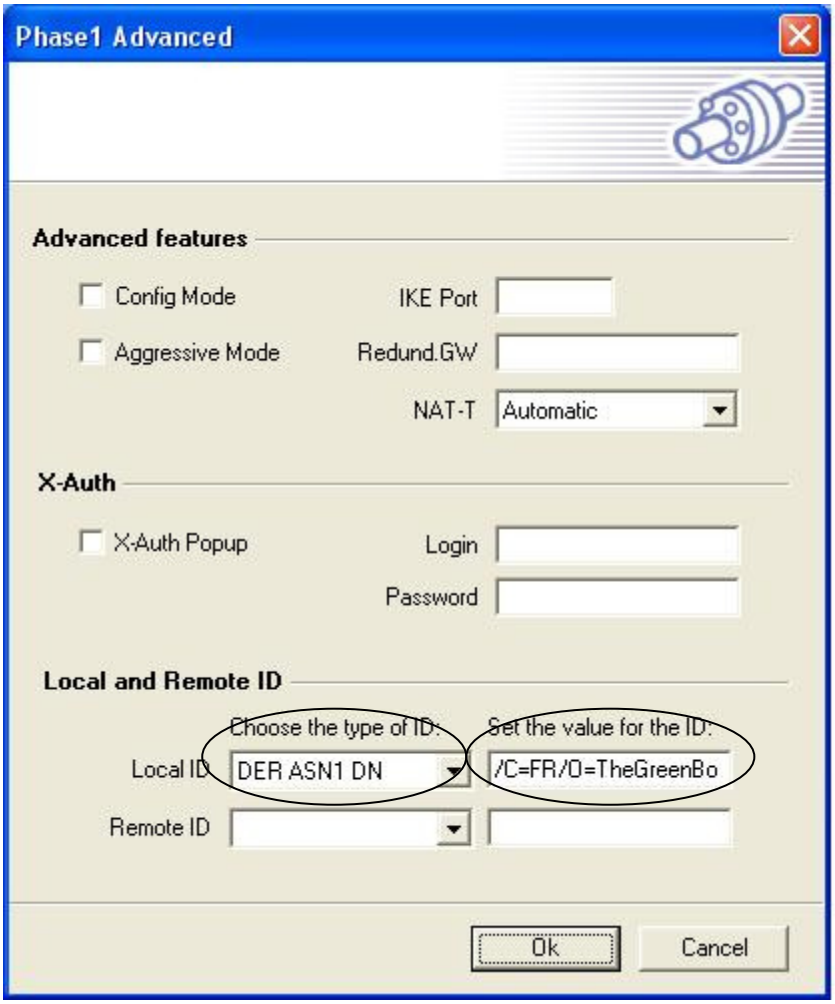
Root certificate file is "**clientCert.pem**" from the **certification authority folder** (don't select rootCA.pem)

User certificate file is "clientCert.pem" from the client folder

User private key file is "local.key" from the client folder

Make sure all 3 are imported (showing a small key in before each name) and press OK to go back to main screen of the client.

Choose "P1 advanced":



Local ID must be defined as DER ASN1 DN type.

Copy the content of the file "Der_asn1_dn.txt" located in the **client folder**, and copy it in the value field.

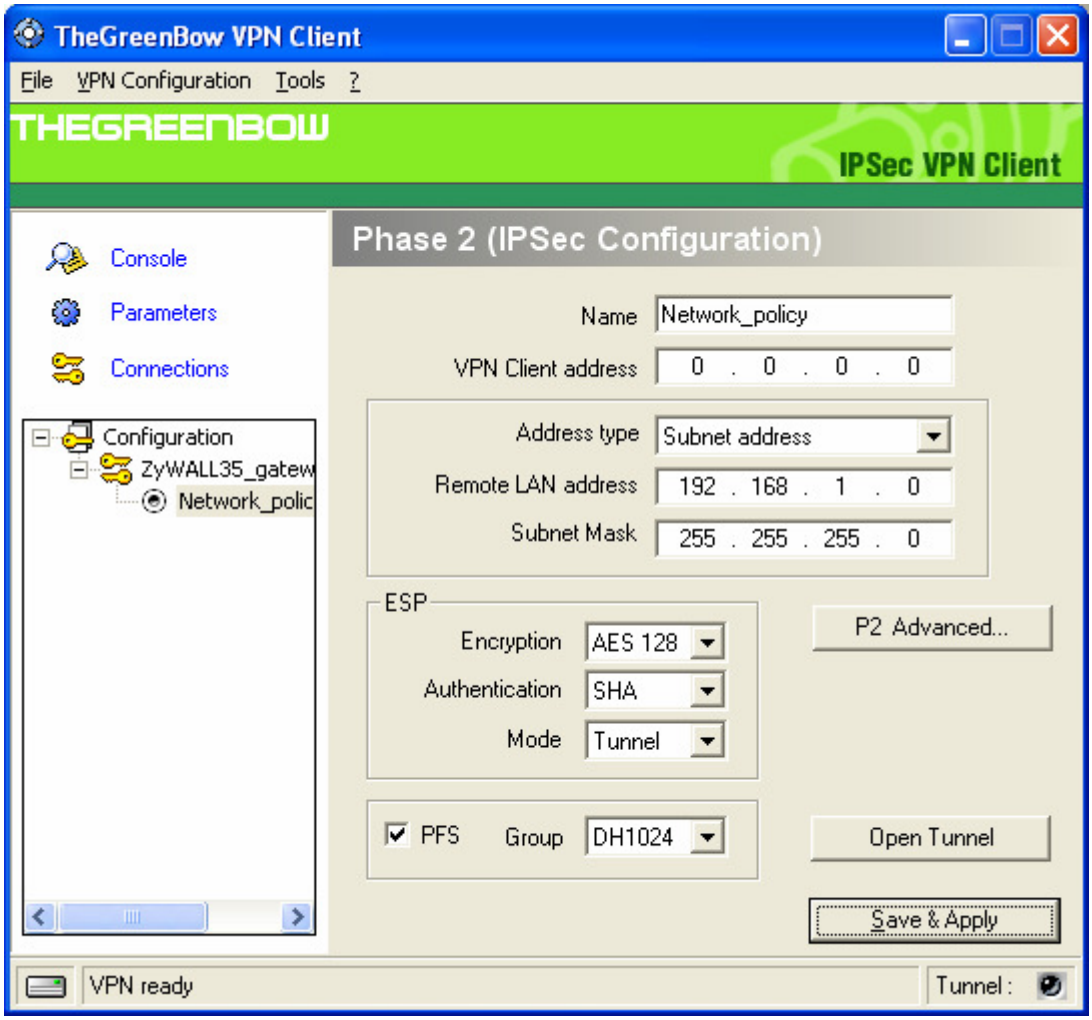
Nothing is needed in Remote ID.

Press OK

3.3 Phase 2 Configuration

Create a phase2: right-click on phase1 and select “add phase 2”

Phase 2 settings should match network policy of the ZyWALL.



Modify Address type by choosing subnet address, and add the remote lan address and mask (must match what was defined on ZyWALL)

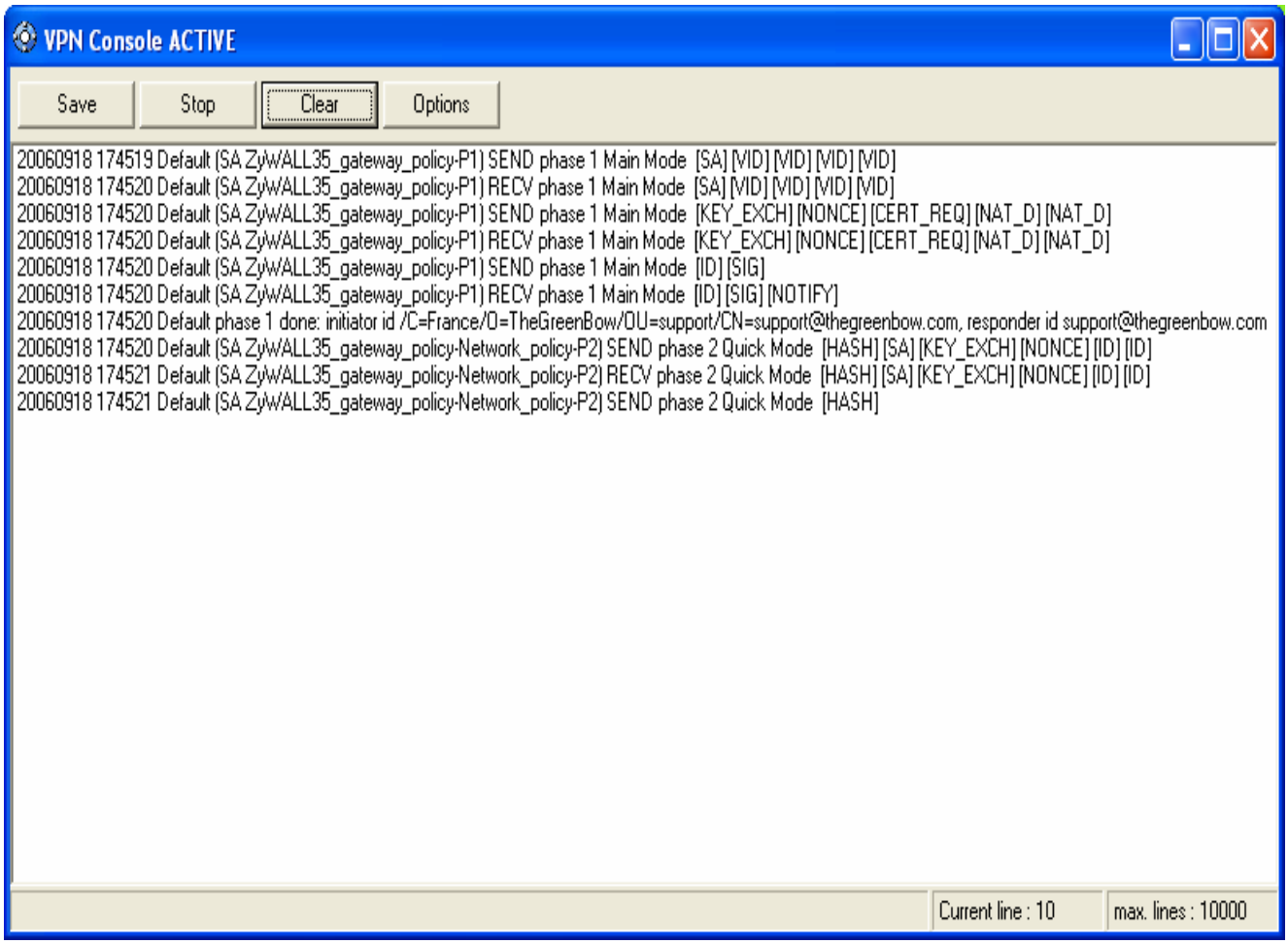
Algorithms, pfs and dh group must match ZyWALL’s settings.

The VPN client address must not belong to the remote subnet range. In our example, we chose 0.0.0.0 meaning the vpn client address is the physical address of the machine either dynamically assigned by isp or lan dhcp. (from a hotel for example)

If the roadwarrior tries to connect from a lan which address is 192.168.1.0, the vpn connection won't establish correctly. In this case you must specify an ip address in another range (10.0.0.1 for example, or 192.168.0.1 or any private ip address you wish taken from another ip range than the lan behind the router)

Phase2 advanced is used to enter alternate dns and/or wins servers addresses from the ones the vpn client is using prior to establish the tunnel.

Successful console log for this vpn connection:



4 VPN IPSec Troubleshooting

4.1 « PAYLOAD MALFORMED » error

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

4.2 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
```

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

4.3 « no keystate » error

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

4.4 « received remote ID other than expected » error

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.

4.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915   Default   (SA   CNXVPN1-CNXVPN1-P2)   SEND   phase   2   Quick   Mode
[SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default CNXVPN1-P1 deleted
```

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

4.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626   Default   (SA   CNXVPN1-CNXVPN1-P2)   SEND   phase   2   Quick   Mode
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type (“Subnet address” and “Single address”). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

4.7 I clicked on “Open tunnel”, but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500, UDP port 4500 and protocol ESP (protocol 50).

4.8 The VPN tunnel is up but I can’t ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP

- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
- Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- We recommend you to install ethereal (http://www.ethereal.com) on one of your target computer. You can check that your pings arrive inside the LAN.

5 Contacts

News and updates on TheGreenBow web site : http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts at +33 1 43 12 39 37 ou by email at info@thegreenbow.com