NETGEAR®

ProSecure Unified Threat Management (UTM) Appliance

Reference Manual

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at visit us at *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/app/answers/detail/a_id/984*.

Product Updates

Product updates are available on the NETGEAR website at *http://prosecure.netgear.com* or *http://kb.netgear.com/app/home*.

ProSecure Forum

Go to *http://prosecure.netgear.com/community/forum.php* for information about the ProSecure forum and to become part of the ProSecure community.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, ProSecure, Smart Wizard, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments

202-10780-01	1.0	September 2011	• Addition of the UTM9S with the following major new features:
			  - xDSL module (see *Chapter 1, Introduction* and *Chapter 3, Manually Configuring Internet and WAN Settings*)
			  - Wireless module (see *Chapter 1, Introduction* and *Appendix B, Wireless Module for the UTM9S*)
			  - ReadyNAS integration, quarantine options, and quarantine logs (see *Connect to a ReadyNAS and Configure Quarantine Settings (UTM9S Only)*, *Query the Quarantine Logs (UTM9S Only)*, and *Appendix D, ReadyNAS Integration*
			  - PPTP server (see *Configure the PPTP Server (UTM9S Only)*)
			  - L2TP server (see *Configure the L2TP Server (UTM9S Only)*)
			• Update of the VPN client sections with the new VPN client (see *Chapter 7, Virtual Private Networking Using IPSec Connections*)

202-10674-02	1.0	March 2011	• Addition of the UTM150.
			• Removal of platform-specific chapters and sections because the UTM5, UTM10, and UTM25 now support the same web management interface menu layout that was already supported on the UTM50. The *major* changes for the UTM5, UTM10, and UTM25 are documented in *Chapter 3, Manually Configuring Internet and WAN Settings*, and in the following sections:
			    - *Set Web Access Exception Rules*
			    - *Configure Authentication Domains, Groups, and Users*
			• Added new features (for all UTM models). The *major* new features are documented in the following sections:
			    - *Electronic Licensing*
			    - *VLAN Rules*
			    - *Create Service Groups*
			    - *Create IP Groups*
			    - *Manage Digital Certificates for HTTPS Scans*
			    - *Update the Firmware*
			    - *View, Schedule, and Generate Reports*

202-10674-01	1.0	September 2010	• Addition of the UTM50 and UTM50-specific chapters and sections. • Revision of DMZ WAN and LAN DMZ default policies.
202-10482-03	1.0	May 2010	• Applied numerous nontechnical edits. • Added the *Requirements for Entering IP Addresses* section. • Added a note about the processing of normal email traffic in the *Configure Distributed Spam Analysis* section. • Updated the *NTP* section.
202-10482-02	1.0	January 2010	Updated the web management interface screens, made the manual platform-independent, added a model comparison table, and removed performance specifications (see marketing documentation for such specifications).
202-10482-01	1.0	September 2009	Initial publication of this reference manual.

Contents

Chapter 1   Introduction

Chapter 2   Using the Setup Wizard to Provision the UTM in Your Network

Chapter 3   Manually Configuring Internet and WAN Settings

Chapter 4   LAN Configuration

Chapter 5   Firewall Protection

Chapter 6   Content Filtering and Optimizing Scans

Chapter 8 Virtual Private Networking
Using SSL Connections

Chapter 9 Managing Users, Authentication, and VPN Certificates

Chapter 10 Network and System Management

Chapter 11   Monitoring System Access and Performance

Chapter 12 Troubleshooting and Using Online Support

Appendix A xDSL Module for the UTM9S

Appendix B Wireless Module for the UTM9S

Appendix C   Network Planning for Dual WAN Ports (Multiple WAN Port Models Only)

Appendix D   ReadyNAS Integration

Appendix E   Two-Factor Authentication

Appendix F   System Logs and Error Messages

Appendix G   Default Settings and Technical Specifications

Appendix H   Notification of Compliance (Wired)

Appendix I   Notification of Compliance (Wireless)

Index

Introduction

1

This chapter provides an overview of the features and capabilities of the NETGEAR ProSecure™ Unified Threat Management (UTM) Appliance. This chapter contains the following sections:

- *What Is the ProSecure Unified Threat Management (UTM) Appliance?*
- *Key Features and Capabilities*
- *Service Registration Card with License Keys*
- *Package Contents*
- *Hardware Features*
- *Choose a Location for the UTM*

> **Note:** For more information about the topics covered in this manual, visit the NETGEAR support website at *http://support.netgear.com*.

What Is the ProSecure Unified Threat Management (UTM) Appliance?

The ProSecure Unified Threat Management (UTM) Appliance, hereafter referred to as the UTM, connects your local area network (LAN) to the Internet through one or two external broadband access devices such as cable modems, DSL modems, satellite dishes, or wireless ISP radio antennas, or a combination of those. Dual wide area network (WAN) ports allow you to increase the effective data rate to the Internet by utilizing both WAN ports to carry session traffic, or to maintain a backup connection in case of failure of your primary Internet connection.

As a complete security solution, the UTM combines a powerful, flexible firewall with a content scan engine that uses NETGEAR Stream Scanning technology to protect your network from denial of service (DoS) attacks, unwanted traffic, traffic with objectionable content, spam, phishing, and web-borne threats such as spyware, viruses, and other malware threats.

The UTM provides advanced IPSec and SSL VPN technologies for secure and simple remote connections. The use of Gigabit Ethernet LAN and WAN ports ensures extremely high data transfer speeds.

The UTM is a plug-and-play device that can be installed and configured within minutes.

Key Features and Capabilities

The UTM provides the following key features and capabilities:

- For the single WAN port models, a single 10/100/1000 Mbps Gigabit Ethernet WAN port. For the multiple WAN port models, dual or quad 10/100/1000 Mbps Gigabit Ethernet WAN ports for load balancing or failover protection of your Internet connection, providing increased system reliability or increased data rate.

- Built-in four- or six-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for extremely fast data transfer between local network resources.

- Wireless module (UTM9S only) for either 2.4-GHz or 5-GHz wireless modes.

- xDLS module (UTM9S only) for ADSL and VDSL.

- Advanced IPSec VPN and SSL VPN support.

- Depending on the model, bundled with a one-user license of the NETGEAR ProSafe VPN Client software (VPN01L).

- Advanced Stateful Packet Inspection (SPI) firewall with multi-NAT support.

- Patent-pending Stream Scanning technology that enables scanning of real-time protocols such as HTTP.

- Comprehensive web and email security, covering six major network protocols: HTTP, HTTPS, FTP, SMTP, POP3, and IMAP.

- Malware database containing hundreds of thousands of signatures of spyware, viruses, and other malware threats.

- Very frequently updated malware signatures, hourly if required. The UTM can automatically check for new malware signatures as frequently as every 15 minutes.

- Multiple antispam technologies to provide extensive protection against unwanted mail.

- Easy, web-based wizard setup for installation and management.

- SNMP manageable.

- Front panel LEDs for easy monitoring of status and activity.

- Flash memory for firmware upgrade.

- Internal universal switching power supply.

Multiple WAN Port Models for Increased Reliability or Outbound Load Balancing

The UTM product line offers models with two broadband WAN ports. The second WAN port allows you to connect a second broadband Internet line that can be configured on a mutually exclusive basis to:

- Provide backup and rollover if one line is inoperable, ensuring that you are never disconnected.

- Load balance, or use both Internet lines simultaneously for outgoing traffic. A UTM with dual WAN ports balances users between the two lines for maximum bandwidth efficiency.

See *Appendix C, Network Planning for Dual WAN Ports (Multiple WAN Port Models Only)* for the planning factors to consider when implementing the following capabilities with dual WAN port gateways:

- Single or multiple exposed hosts

- Virtual private networks

Wireless Features

Wireless client connections are supported on the UTM9S with a UTM9SWLSN wireless module installed. The UTM9S supports the following wireless features:

- **2.4-GHz radio and 5-GHz radio**. Either 2.4-GHz band support with 802.11b/g/n/ wireless modes or 5-GHz band support with 802.11a/n wireless modes.

- **WMM QoS priority**. Wi-Fi Multimedia (WMM) Quality of Service (QoS) priority settings to map one of four queues to each Differentiated Services Code Point (DSCP) value.

- **Wireless Distribution System (WDS)**. WDS enables expansion of a wireless network through two or more access points that are interconnected.

- **Access control**. The Media Access Control (MAC) address filtering feature can ensure that only trusted wireless stations can use the UTM to gain access to your LAN.

- **Hidden mode**. The SSID is not broadcast, assuring that only clients configured with the correct SSID can connect.

- **Secure and economical operation**. Adjustable power output allows more secure or economical operation.

DSL Features

DSL is supported on the UTM9S with a UTM9SDSL xDSL module installed. The UTM9S automatically detects the following types of DSL connections:

- ADSL, ADSL2, and ADLS2+

- VDSL and VDSL2

Annex A, Annex B, and Annex M are supported to accommodate PPPoE, PPPoA, and IPoA ISP connections.

Advanced VPN Support for Both IPSec and SSL

The UTM supports IPSec and SSL virtual private network (VPN) connections.

- IPSec VPN delivers full network access between a central office and branch offices, or between a central office and telecommuters. Remote access by telecommuters requires the installation of VPN client software on the remote computer.

    - IPSec VPN with broad protocol support for secure connection to other IPSec gateways and clients.

    - Depending on the model, bundled with a one-user license of the NETGEAR ProSafe VPN Client software (VPN01L).

- SSL VPN provides remote access for mobile users to selected corporate resources without requiring a preinstalled VPN client on their computers.

    - Uses the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, to provide client-free access with customizable user portals and support for a wide variety of user repositories.

    - Allows browser-based, platform-independent remote access through a number of popular browsers, such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.

    - Provides granular access to corporate resources based on user type or group membership.

A Powerful, True Firewall

Unlike simple NAT routers, the UTM is a true firewall, using Stateful Packet Inspection (SPI) to defend against hacker attacks. Its firewall features have the following capabilities:

- **DoS protection**. Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death and SYN flood.

- **Secure firewall**. Blocks unwanted traffic from the Internet to your LAN.

- **Schedule policies**. Permits scheduling of firewall policies by day and time.

- **Logs security incidents**. Logs security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

Stream Scanning for Content Filtering

Stream Scanning is based on the simple observation that network traffic travels in streams. The UTM scan engine starts receiving and analyzing traffic as the stream enters the network. As soon as a number of bytes are available, scanning starts. The scan engine continues to scan more bytes as they become available, while at the same time another thread starts to deliver the bytes that have been scanned.

This multithreaded approach, in which the receiving, scanning, and delivering processes occur concurrently, ensures that network performance remains unimpeded. The result is that file scanning is up to five times faster than with traditional antivirus solutions—a performance advantage that you will notice.

Stream Scanning also enables organizations to withstand massive spikes in traffic, as in the event of a malware outbreak. The scan engine has the following capabilities:

- **Real-time protection**. The patent-pending Stream Scanning technology enables scanning of previously undefended real-time protocols, such as HTTP. Network activities susceptible to latency (for example, web browsing) are no longer brought to a standstill.

- **Comprehensive protection**. Provides both web and email security, covering six major network protocols: HTTP, HTTPS, FTP, SMTP, POP3, and IMAP. The UTM uses enterprise-class scan engines employing both signature-based and distributed spam analysis to stop both known and unknown threats. The malware database contains hundreds of thousands of signatures of spyware, viruses, and other malware.

- **Objectionable traffic protection**. The UTM prevents objectionable content from reaching your computers. You can control access to the Internet content by screening for web services, web addresses, and keywords within web addresses. You can log and report attempts to access objectionable Internet sites.

- **Automatic signature updates**. Malware signatures are updated as frequently as every hour, and the UTM can check automatically for new signatures as frequently as every 15 minutes.

Security Features

The UTM is equipped with several features designed to maintain security:

- **PCs hidden by NAT**. NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the computers on the LAN.

- **Port forwarding with NAT**. Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the UTM allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request. You can specify forwarding of single ports or ranges of ports.

- **DMZ port**. Incoming traffic from the Internet is usually discarded by the UTM unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can use the dedicated demilitarized zone (DMZ) port to forward the traffic to one PC on your network.

Autosensing Ethernet Connections with Auto Uplink

With its internal four- or six-port 10/100/1000 Mbps switch and single or dual (model-dependant) 10/100/1000 WAN ports, the UTM can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit

Ethernet network. The four LAN and one or two WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The UTM incorporates Auto Uplink™ technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a *normal* connection such as to a PC or an *uplink* connection such as to a switch or hub. That port then configures itself correctly. This feature eliminates the need for you to think about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

Extensive Protocol Support

The UTM supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, see *Internet Configuration Requirements* on page 558. The UTM provides the following protocol support:

- **IP address sharing by NAT**. The UTM allows many networked PCs to share an Internet account using only a single IP address, which might be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.

- **Automatic configuration of attached PCs by DHCP**. The UTM dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

- **DNS proxy**. When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.

- **PPP over Ethernet (PPPoE)**. PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection.

- **Quality of Service (QoS)**. The UTM supports QoS, including traffic prioritization and traffic classification with Type of Service (ToS) and Differentiated Services Code Point (DSCP) marking.

Easy Installation and Management

You can install, configure, and operate the UTM within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**. Browser-based configuration allows you to easily configure the UTM from almost any type of operating system, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided, and online help documentation is built into the browser-based web management interface.

- **Autodetection of ISP**. The UTM automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.

- **IPSec VPN Wizard**. The UTM includes the NETGEAR IPSec VPN Wizard so you can easily configure IPSec VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC). This ensures that the IPSec VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.

- **SSL VPN Wizard**. The UTM includes the NETGEAR SSL VPN Wizard so you can easily configure SSL connections over VPN according to the recommendations of the VPNC. This ensures that the SSL connections are interoperable with other VPNC-compliant VPN routers and clients.

- **SNMP**. The UTM supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.

- **Diagnostic functions**. The UTM incorporates built-in diagnostic functions such as ping, traceroute, DNS lookup, and remote reboot.

- **Remote management**. The UTM allows you to log in to the web management interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.

- **Visual monitoring**. The UTM's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the UTM:

- Flash memory for firmware upgrades.

- Technical support seven days a week, 24 hours a day. Information about support is available on the NETGEAR ProSecure website at *http://prosecure.netgear.com/support/index.php*.

Model Comparison

The following table compares the UTM models to show the differences. For performance specifications and sizing guidelines, see NETGEAR's marketing documentation at *http://prosecure.netgear.com*.

Table 1. Differences between the UTM models

Feature	UTM5	UTM9S	UTM10	UTM25	UTM50	UTM150
IPSec VPN tunnels						
Number of supported site-to-site IPSec VPN tunnels (from which the model derives its model number, with the exception of the UTM9S)	5	10	10	25	50	150
Hardware						
LAN ports (Gigabit RJ-45)	4	4	4	4	6	4

Table 1. Differences between the UTM models (continued)

Feature	UTM5	UTM9S	UTM10	UTM25	UTM50	UTM150
WAN ports (Gigabit RJ-45)	1	2	1	2	2	4
DMZ interfaces (configurable)	1	1	1	1	1	1
USB ports	1	1	1	1	1	1
Console ports (RS232)	1	1	1	1	1	1
Flash memory RAM	2 GB 512 MB	2 GB 512 MB	2 GB 512 MB	2 GB 1 GB	2 GB 1 GB	2 GB 1 GB
Modules						
xDSL module with RJ11 port	No	Yes	No	No	No	No
Wireless module	No	Yes	No	No	No	No
Deployment						
VLAN support	Yes	Yes	Yes	Yes	Yes	Yes
Dual WAN auto-rollover mode	No	Yes	No	Yes	Yes	Yes
Dual WAN load balancing mode	No	Yes	No	Yes	Yes	Yes
Single WAN mode	Yes	Yes	Yes	Yes	Yes	Yes

Service Registration Card with License Keys

Be sure to store the license key card that came with your UTM (see a sample card in the following figure) in a secure location. If you do not use electronic licensing (see *Electronic Licensing* on page 64), you need these service license keys to activate your product during the initial setup.

Figure 1.

Note: When you reset the UTM to the original factory default settings after you have entered the license keys to activate the UTM (see *Register the UTM with NETGEAR* on page 62), the license keys are erased. The license keys and the different types of licenses that are available for the UTM are no longer displayed on the Registration screen. However, after you have reconfigured the UTM to connect to the Internet and to the NETGEAR registration server, the UTM retrieves and restores all registration information based on its MAC address and hardware serial number. You do not need to reenter the license keys and reactivate the UTM.

Package Contents

The UTM product package contains the following items:

- ProSecure Unified Threat Management (UTM) Appliance
- One AC power cable
- Rubber feet (4)
- One rack-mounting kit (depends on UTM model)
- *ProSecure Unified Threat Management UTM Installation Guide*

- *Resource CD,* including:
  - Application Notes and other helpful information
  - ProSafe VPN Client software (VPN01L) (depends on the UTM model)
- Service Registration Card with license key(s)

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

Hardware Features

The front panel ports and LEDs, rear panel ports, and bottom labels of the UTM models are described in the following sections:

- *Front Panel UTM5 and UTM10*
- *Front Panel UTM25*
- *Front Panel UTM50*
- *Front Panel UTM150*
- *Front Panel UTM9S and Modules*
- *LED Descriptions, UTM5, UTM10, UTM25, UTM50, and UTM150*
- *LED Descriptions, UTM9S and Modules*
- *Rear Panel UTM5, UTM10, and UTM25*
- *Rear Panel UTM50 and UTM150*
- *Rear Panel UTM9S*
- *Bottom Panels with Product Labels*

Front Panel UTM5 and UTM10

Viewed from left to right, the UTM5 and UTM10 front panel contains the following ports:

- One nonfunctioning USB port. This port is included for future management enhancements. The port is currently not operable on the UTM.
- LAN Ethernet ports. Four switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.
- WAN Ethernet port. One independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.

The front panel also contains three groups of status indicator light-emitting diodes (LEDs), including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are explained in detail in *Table 2* on page 27. In addition, the front panel provides some LED explanation to the left of the LAN ports.

Power LED

USB port

Left LAN LEDs

DMZ LED

Left WAN LED

Test LED

Right LAN LEDs

Right WAN LED
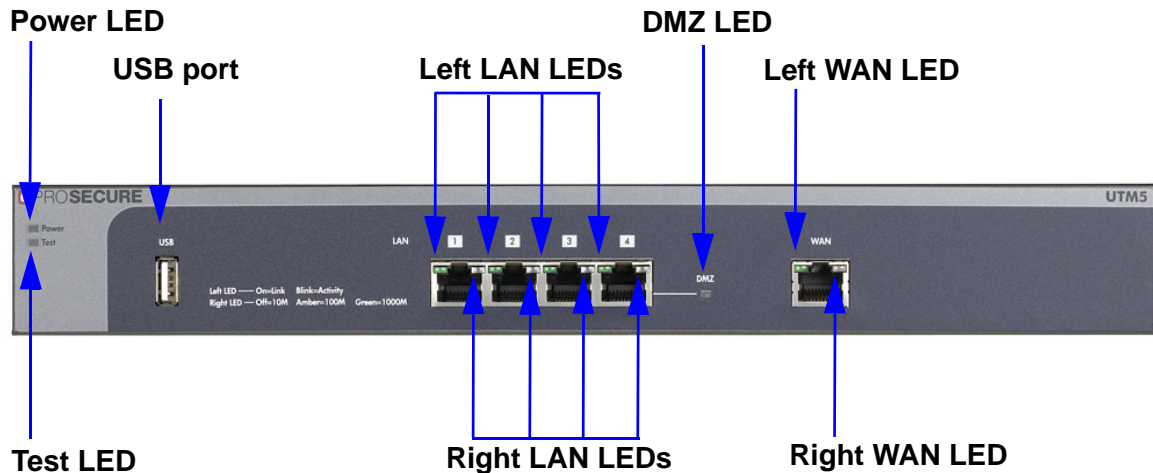
Figure 2. Front panel UTM5 and UTM10

Front Panel UTM25

Viewed from left to right, the UTM25 front panel contains the following ports:

- One nonfunctioning USB port. This port is included for future management enhancements. The port is currently not operable on the UTM.

- LAN Ethernet ports. Four switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.

- WAN Ethernet ports. Two independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.

The front panel also contains three groups of status indicator LEDs, including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are explained in detail in the *Table 2* on page 27. In addition, the front panel provides some LED explanation to the left of the LAN ports.

Power LED

USB port

Left LAN LEDs

DMZ LED

Left WAN LEDs

Test LED

Right LAN LEDs

Right WAN LEDs

Active WAN LEDs
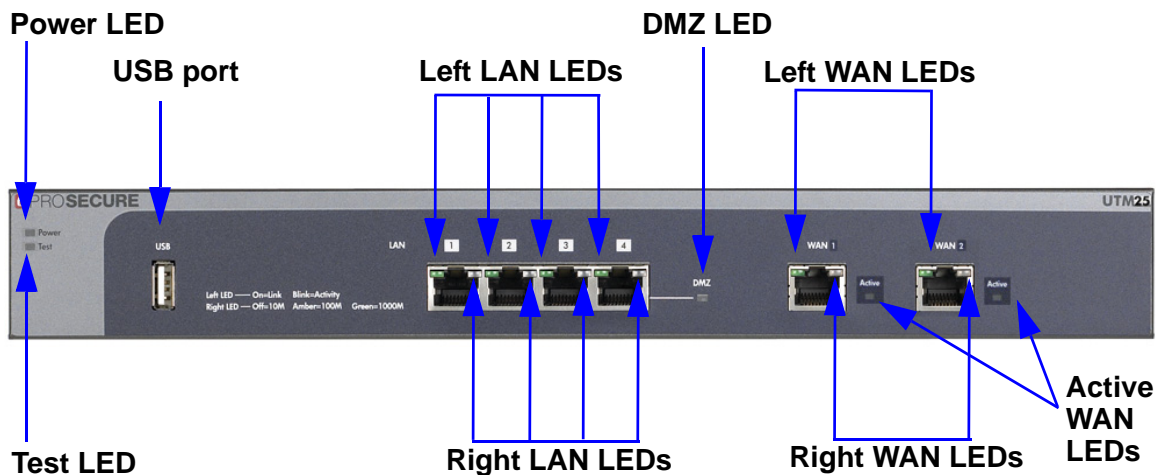
Figure 3. Front panel UTM25

Front Panel UTM50

Viewed from left to right, the UTM front panel contains the following ports (see the following figure, which shows a multiple WAN port model, the UTM25):

- One nonfunctioning USB port. This port is included for future management enhancements. The port is currently not operable on the UTM.

- LAN Ethernet ports. Six switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.

- WAN Ethernet ports. Two independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.

The front panel also contains three groups of status indicator LEDs, including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are explained in detail in *Table 2* on page 27. In addition, the front panel provides some LED explanation to the right of the WAN ports.
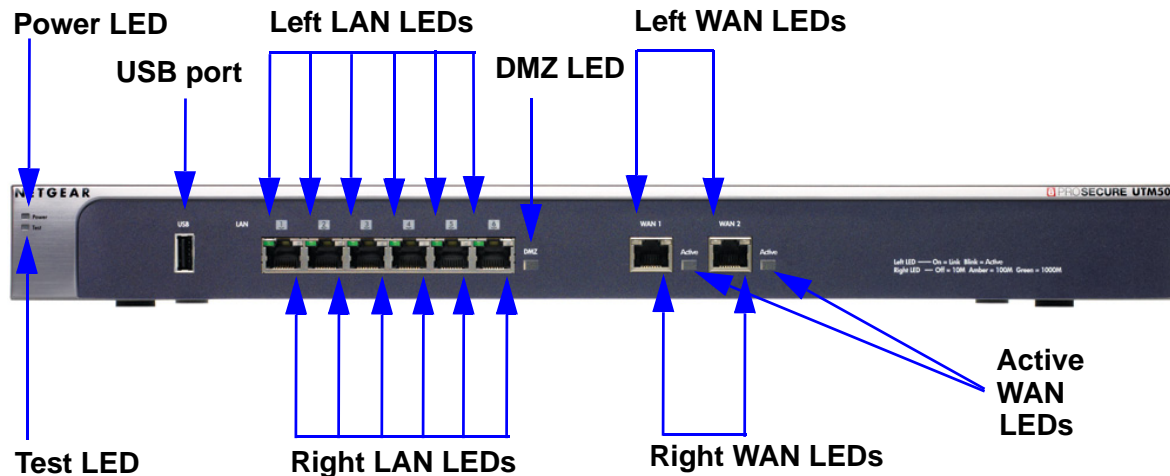
Figure 4. Front panel UTM50

Front Panel UTM150

Viewed from left to right, the UTM150 front panel contains the following ports:

- One nonfunctioning USB port. This port is included for future management enhancements. The port is currently not operable on the UTM.

- LAN Ethernet ports. Four switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.

- WAN Ethernet ports. Four independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.

The front panel also contains three groups of status indicator LEDs, including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are explained in detail in *Table 2* on page 27. In addition, the front panel provides some LED explanation to the right of the WAN ports.
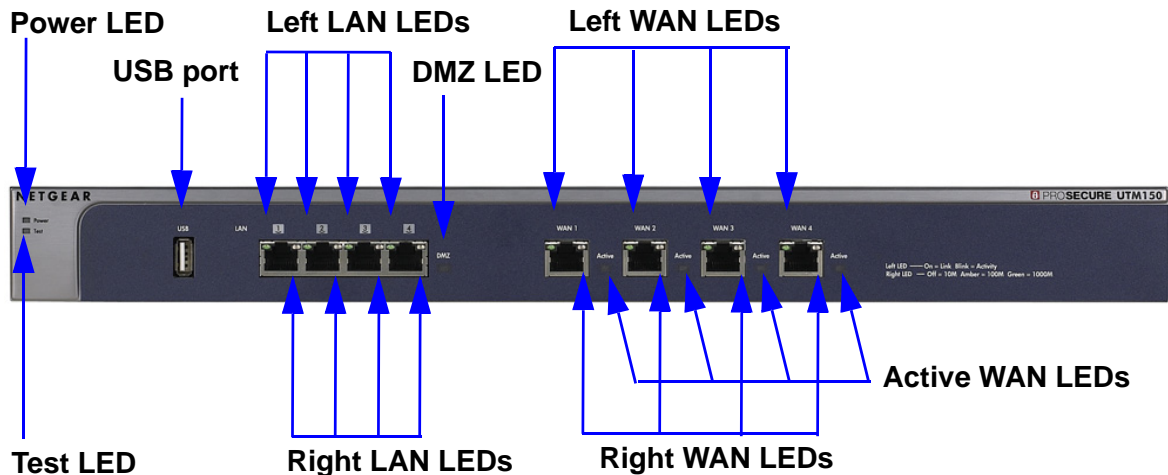
Figure 5. Front panel UTM150

Front Panel UTM9S and Modules

Viewed from left to right, the UTM9S front panel contains the following ports and slots:

- One nonfunctioning USB port. This port is included for future management enhancements. The port is currently not operable on the UTM9S.
- LAN Ethernet ports. Four switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.
- WAN Ethernet ports. Two independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.

The front panel also contains three groups of status indicator LEDs, including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are explained in detail in *Table 3* on page 28. Some LED explanation is provided on the front panel below the LAN and WAN ports.
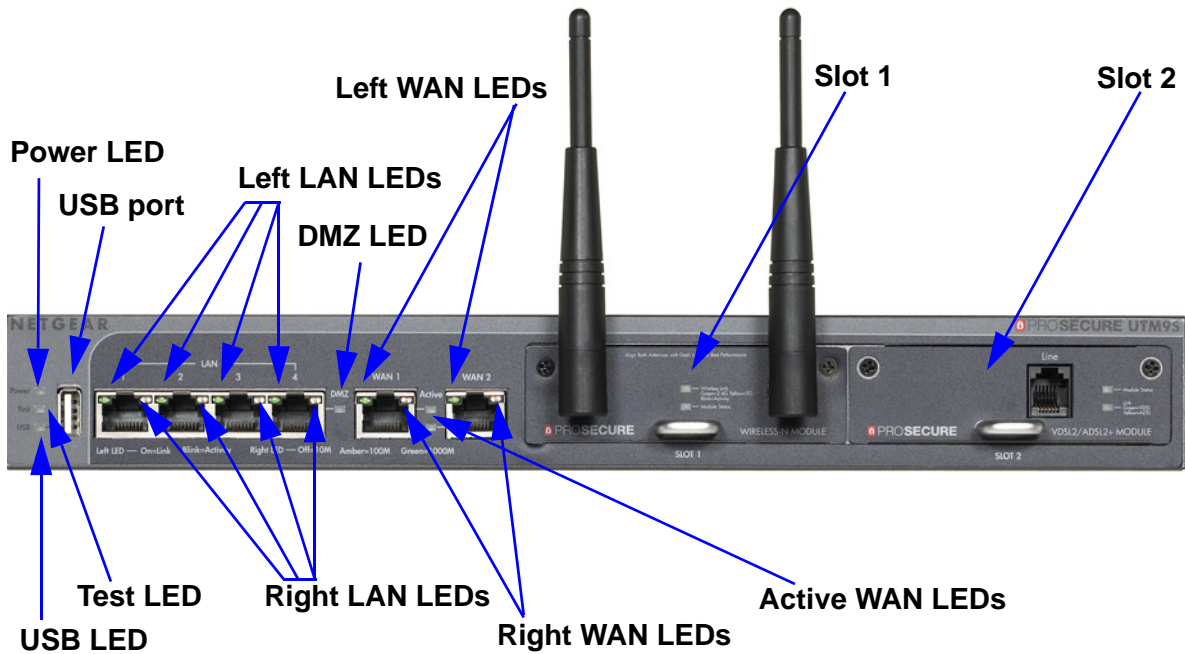
Figure 6. Front panel UTM9S

UTM9SDSL xDSL Module

The following xDSL modules are available for insertion in one of the UTM9S slots:

- UTM9SDSLA. VDSL/ADSL2+ module, Annex A.
- UTM9SDSLB. VDSL/ADSL2+ module, Annex B.

The xDLS module provides one RJ-11 port for connection to a telephone line. The two LEDs are explained in *Table 3* on page 28.
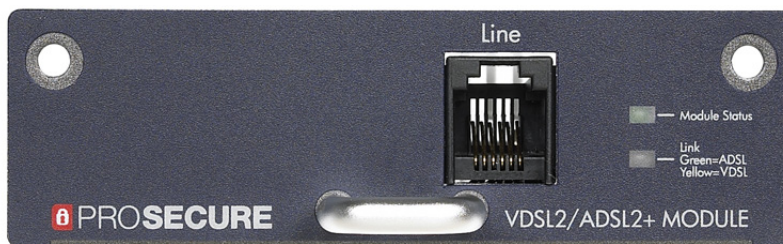
Figure 7. UTM9SDSL xDSL module

UTM9SWLSN Wireless Module

The wireless module (UTM9SWLSN) can be inserted in one of the UTM9S slots. The wireless module does not provide any ports. The antennas are detachable. The two LEDs are explained in *Table 3* on page 28.

Figure 8. UTM9SWLSN wireless module

LED Descriptions, UTM5, UTM10, UTM25, UTM50, and UTM150

The following table describes the function of each LED.

Table 2. LED descriptions UTM5, UTM10, UTM25, UTM50, and UTM150

LED	Activity	Description
Power LED	On (green)	Power is supplied to the UTM.
	Off	Power is not supplied to the UTM.
Test LED	On (amber) during startup	Test mode. The UTM is initializing. After approximately 2 minutes, when the UTM has completed its initialization, the Test LED goes off.
	On (amber) during any other time	The initialization has failed, or a hardware failure has occurred.
	Blinking (amber)	The UTM is writing to flash memory (during upgrading or resetting to defaults).
	Off	The UTM has booted successfully.

Table 2. LED descriptions UTM5, UTM10, UTM25, UTM50, and UTM150 (continued)

LED	Activity	Description
LAN ports		
Left LED	Off	The LAN port has no link.
	On (green)	The LAN port has detected a link with a connected Ethernet device.
	Blinking (green)	Data is being transmitted or received by the LAN port.
Right LED	Off	The LAN port is operating at 10 Mbps.
	On (amber)	The LAN port is operating at 100 Mbps.
	On (green)	The LAN port is operating at 1000 Mbps.
DMZ LED	Off	Port 4 (UTM5, UTM9S, UTM10, UTM25, and UTM150) or port 6 (UTM50) is operating as a normal LAN port.
	On (green)	Port 4 (UTM5, UTM9S, UTM10, UTM25, and UTM150) or port 6 (UTM50) is operating as a dedicated hardware DMZ port.
WAN ports		
Left LED	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the UTM.
	On (green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blinking (green)	Data is being transmitted or received by the WAN port.
Right LED	Off	The WAN port is operating at 10 Mbps.
	On (amber)	The WAN port is operating at 100 Mbps.
	On (green)	The WAN port is operating at 1000 Mbps.
Active LED (multiple WAN port models only)	Off	The WAN port either is not enabled or has no link to the Internet.
	On (green)	The WAN port has a valid Internet connection.

LED Descriptions, UTM9S and Modules

The following table describes the function of each LED on the UTM9S and the modules.

Table 3. LED descriptions UTM9S

LED	Activity	Description
Power LED	On (green)	Power is supplied to the UTM.
	Off	Power is not supplied to the UTM.

Table 3. LED descriptions UTM9S (continued)

LED	Activity	Description
Test LED	On (amber) during startup	Test mode. The UTM is initializing. After approximately 2 minutes, when the UTM has completed its initialization, the Test LED goes off.
	On (amber) during any other time	The initialization has failed, or a hardware failure has occurred.
	Blinking (amber)	The UTM is writing to flash memory (during upgrading or resetting to defaults).
	Off	The UTM has booted successfully.
USB LED	Nonfunctioning	The USB port is currently not operable on the UTM9S.
LAN ports		
Left LED	Off	The LAN port has no link.
	On (green)	The LAN port has detected a link with a connected Ethernet device.
	Blinking (green)	Data is being transmitted or received by the LAN port.
Right LED	Off	The LAN port is operating at 10 Mbps.
	On (amber)	The LAN port is operating at 100 Mbps.
	On (green)	The LAN port is operating at 1000 Mbps.
DMZ LED	Off	Port 4 is operating as a normal LAN port.
	On (green)	Port 4 is operating as a dedicated hardware DMZ port.
WAN ports		
Left LED	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the UTM.
	On (green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blinking (green)	Data is being transmitted or received by the WAN port.
Right LED	Off	The WAN port is operating at 10 Mbps.
	On (amber)	The WAN port is operating at 100 Mbps.
	On (green)	The WAN port is operating at 1000 Mbps.
Active LED	Off	The WAN port either is not enabled or has no link to the Internet.
	On (green)	The WAN port has a valid Internet connection.
Wireless module		
Module Status LED	Off	The module is not enabled.
	On (green)	The module is enabled.

Table 3. LED descriptions UTM9S (continued)

LED	Activity	Description
Wireless Link LED	Off	The wireless access point is not enabled.
	On (green)	The wireless access point is enabled in 2.4-GHz operating mode.
	Blinking (green)	There is wireless activity in 2.4-GHz operating mode.
	On (yellow)	The wireless access point is enabled in 5-GHz operating mode.
	Blinking (yellow)	There is wireless activity in 5-GHz operating mode.
xDSL module		
Module Status LED	Off	The module is enabled or has a link the the telephone line.
	On (green)	The module either is not enabled or has no link to the telephone line.
Link LED	Off	The xDLS port has no Internet connection.
	On (green)	The xDSL port functions in ADSL mode.
	On (yellow)	The xDSL port functions in VDSL mode.

Rear Panel UTM5, UTM10, and UTM25

The rear panel of the UTM includes a cable lock receptacle, a console port, a factory default Reset button, and an AC power connection.

Figure 9. Rear panel of the UTM5, UTM10, and UTM25

Viewed from left to right, the rear panel of the UTM5, UTM10, and UTM25 contains the following components:

1. Cable security lock receptacle.
2. Console port. Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd.
3. Factory default Reset button. Using a sharp object, press and hold this button for about 8 seconds until the front panel Test LED flashes to reset the UTM to factory default settings. Configuration changes are lost, and the default password is restored.
4. AC power receptacle. Universal AC input (100–240 VAC, 50–60 Hz).

Rear Panel UTM50 and UTM150

The rear panel of the UTM includes a cable lock receptacle, a console port, a factory default Reset button, and an AC power connection.
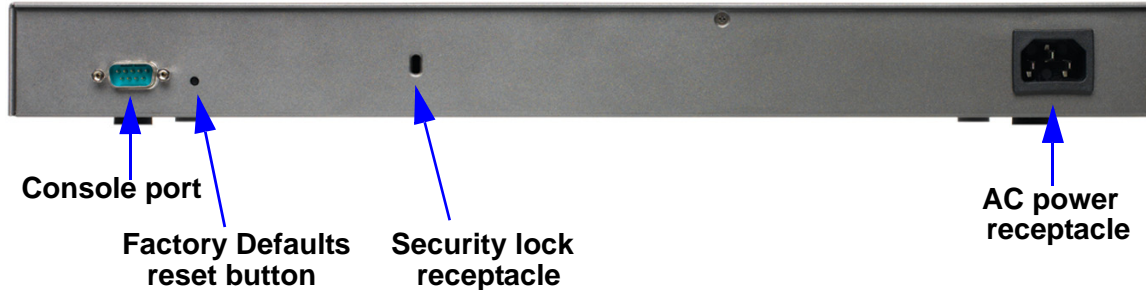
Figure 10. Rear panel of the UTM50 and UTM150

Viewed from left to right, the rear panel of the UTM50 and UTM150 contains the following components:

1. Console port. Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd.

2. Factory default Reset button. Using a sharp object, press and hold this button for about 8 seconds until the front panel Test LED flashes to reset the UTM to factory default settings. Configuration changes are lost, and the default password is restored.

3. Cable security lock receptacle.

4. AC power receptacle. Universal AC input (100–240 VAC, 50–60 Hz).

Rear Panel UTM9S

Figure 11. Rear panel of the UTM9S

Viewed from left to right, the rear panel of the UTM9S contains the following components:

1. Cable security lock receptacle.

2. Factory default Reset button. Using a sharp object, press and hold this button for about 8 seconds until the front panel Test LED flashes to reset the UTM to factory default settings. Configuration changes are lost, and the default password is restored.

3. Console switch to select the console connection: Main Board (left position), Slot 1 (middle position), or Slot 2 (right position).

4. Console port (9600,N,8,1). Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd.

5. AC power receptacle. Universal AC input (100–240 VAC, 50–60 Hz).

6. Power On/Off switch.

Bottom Panels with Product Labels

The product label on the bottom of the UTM's enclosure displays factory defaults settings, regulatory compliance, and other information.

The following figure shows the product label for the UTM5:

Figure 12.

The following figure shows the product label for the UTM10:

Figure 13.

The following figure shows the product label for the UTM25:

Figure 14.

The following figure shows the product label for the UTM50:

Figure 15.

The following figure shows the product label for the UTM150:
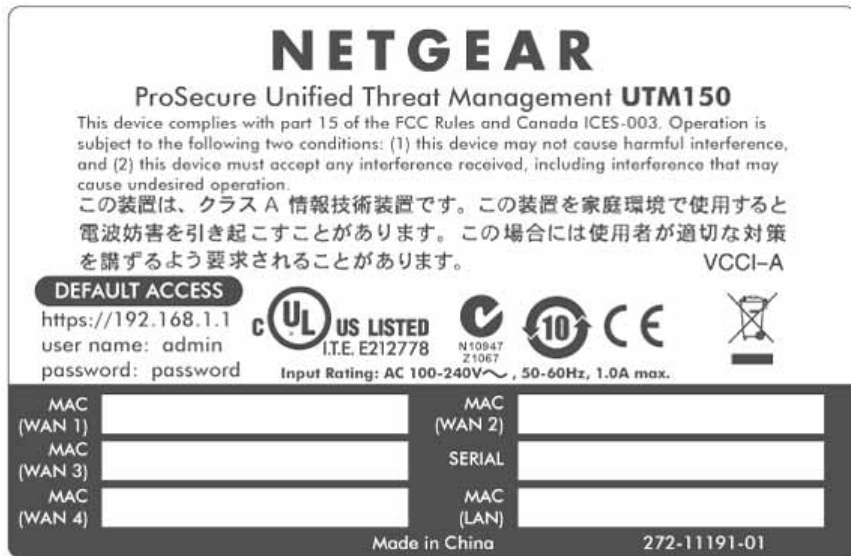
Figure 16.

The following figure shows the product label for the UTM9S:
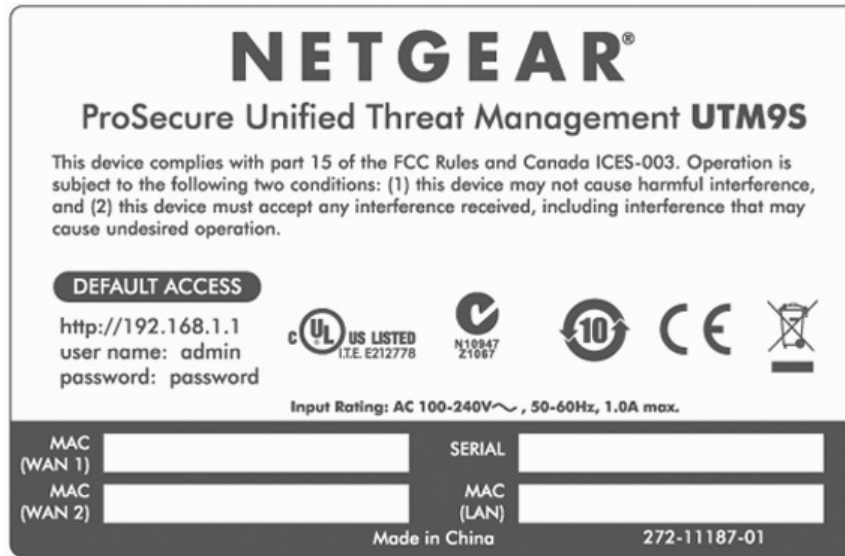
Figure 17.

Choose a Location for the UTM

The UTM is suitable for use in an office environment where it can be freestanding (on its runner feet) or mounted into a standard 19-inch equipment rack. Alternatively, you can rack-mount the UTM in a wiring closet or equipment room. A rack-mounting kit, containing two mounting brackets and four screws, is provided in the package for the multiple WAN port models.

Consider the following when deciding where to position the UTM:

* The unit is accessible, and cables can be connected easily.

* Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air-conditioning units.

* Water or moisture cannot enter the case of the unit.

* Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or 1 inch clearance.

* The air is as free of dust as possible.

* Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information about the recommended operating temperatures for the UTM, see *Appendix G, Default Settings and Technical Specifications*.

> **Note:** For the UTM9S, see also *Wireless Equipment Placement and Range Guidelines* on page 530.

Use the Rack-Mounting Kit

Use the mounting kit for the UTM to install the appliance in a rack. (A mounting kit is provided in the package for the multiple WAN port models.) Attach the mounting brackets using the hardware that is supplied with the mounting kit.
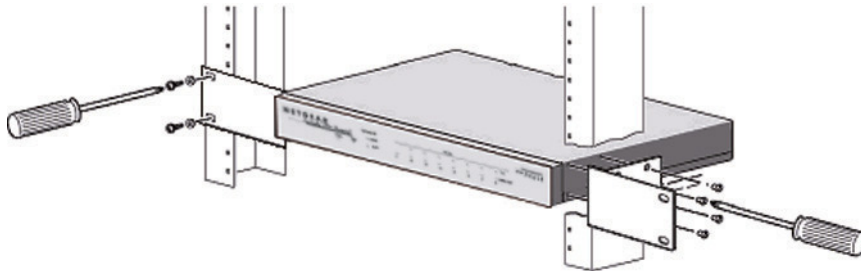
Figure 18.

Before mounting the UTM in a rack, verify that:

- You have the correct screws (supplied with the installation kit).
- The rack onto which you will mount the UTM is suitably located.

Using the Setup Wizard to Provision the UTM in Your Network

2

This chapter explains how to log in to the UTM and use the web management interface, how to use the Setup Wizard to provision the UTM in your network, and how to register the UTM with NETGEAR. The chapter contains the following sections:

- *Steps for Initial Connection*
- *Log In to the UTM*
- *Use the Setup Wizard to Perform the Initial Configuration*
- *Verify Correct Installation*
- *Register the UTM with NETGEAR*
- *What to Do Next*

Steps for Initial Connection

Typically, the UTM is installed as a network gateway to function as a combined LAN switch, firewall, and content scan engine to protect the network from all incoming and outgoing malware threats.

Generally, five steps are required to complete the basic and security configuration of your UTM:

1. **Connect the UTM physically to your network**. Connect the cables and restart your network according to the instructions in the *Installation Guide*. See the *ProSecure Unified Threat Management UTM Installation Guide* for complete steps. A PDF of the *Installation Guide* is on the NETGEAR website at *http://www.prosecure.netgear.com/resources/document-library.php*.

2. **Log in to the UTM**. After logging in, you are ready to set up and configure your UTM. See *Log In to the UTM* on page 38.

3. **Use the Setup Wizard to configure basic connections and security**. During this phase, you connect the UTM to one or more ISPs (more than one ISP applies to multiple WAN port models only). See *Use the Setup Wizard to Perform the Initial Configuration* on page 42.

4. **Verify the installation**. See *Verify Correct Installation* on page 61.

5. **Register the UTM**. See *Register the UTM with NETGEAR* on page 62.

Each of these tasks is described separately in this chapter. The configuration of the WAN mode (required for multiple WAN port models), Dynamic DNS, and other WAN options is described in *Chapter 3, Manually Configuring Internet and WAN Settings*.

The configuration of LAN, firewall, scanning, VPN, management, and monitoring features is described in later chapters.

Qualified Web Browsers

To configure the UTM, you need to use a web browser such as Microsoft Internet Explorer 6 or later, Mozilla Firefox 3 or later, or Apple Safari 3 or later with JavaScript, cookies, and SSL enabled.

Although these web browsers are qualified for use with the UTM's web management interface, SSL VPN users should choose a browser that supports JavaScript, Java, cookies, SSL, and ActiveX to take advantage of the full suite of applications. Note that Java is required only for the SSL VPN portal, not for the web management interface.

Requirements for Entering IP Addresses

The fourth octet of an IP address needs to be between 1 and 254 (both inclusive). This requirement applies to any IP address that you enter on a screen of the web management interface.

Log In to the UTM

To connect to the UTM, your computer needs to be configured to obtain an IP address automatically from the UTM through DHCP.

➢ **To connect and log in to the UTM:**

1. Start any of the qualified web browsers, as explained in the previous section, *Qualified Web Browsers*.

2. In the address field, enter **https://192.168.1.1**. The NETGEAR Configuration Manager Login screen displays in the browser. (The following figure shows the screen for the UTM50.) This screen also provides the User Portal Login Link. For general information about the User Portal Login Link, see *Access the New SSL Portal Login Screen* on page 320; for platform-specific information, see *Login Portals* on page 345.

> **Note:** The UTM factory default IP address is 192.168.1.1. If you change the IP address, you need to use the IP address that you assigned to the UTM to log in to the UTM.
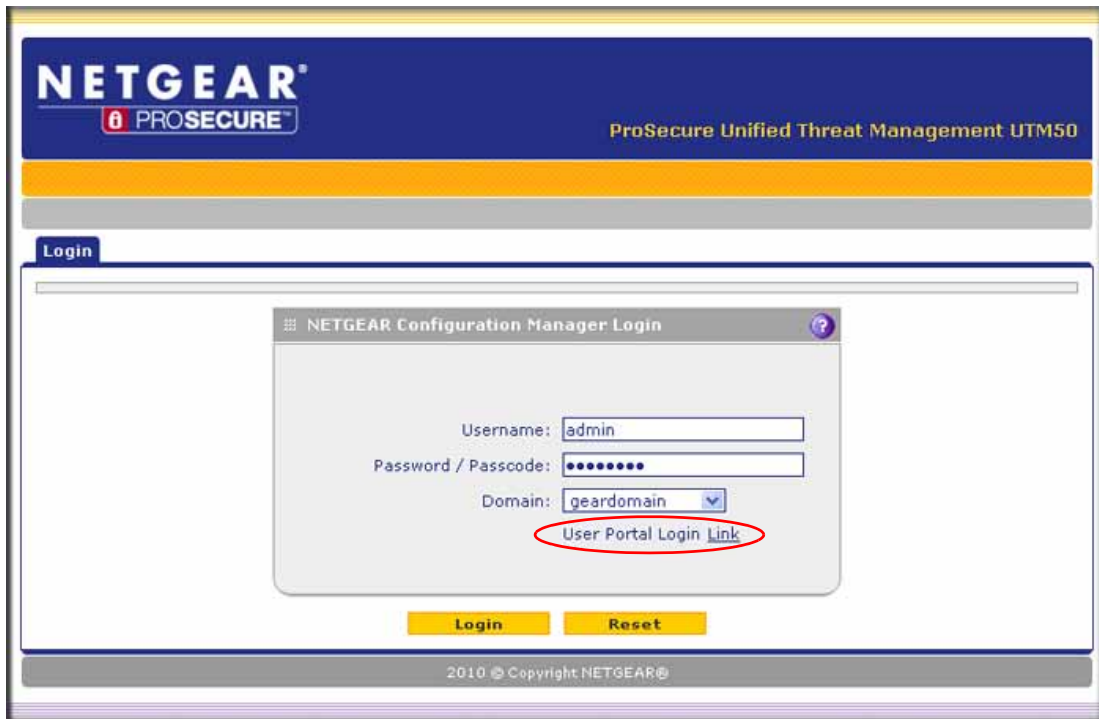
Figure 19.

3. In the User Name field, type **admin**. Use lowercase letters.

4. In the Password / Passcode field, type **password**. Here, too, use lowercase letters.

> **Note:** The UTM user name and password are not the same as any user name or password you might use to log in to your Internet connection.

5. Click **Login**. The web management interface displays, showing the System Status screen. The following figure shows the top part of the UTM50 System Status screen. For more information, see *View the System Status* on page 439.

> **Note:** After 5 minutes of inactivity (the default login time-out), you are automatically logged out.
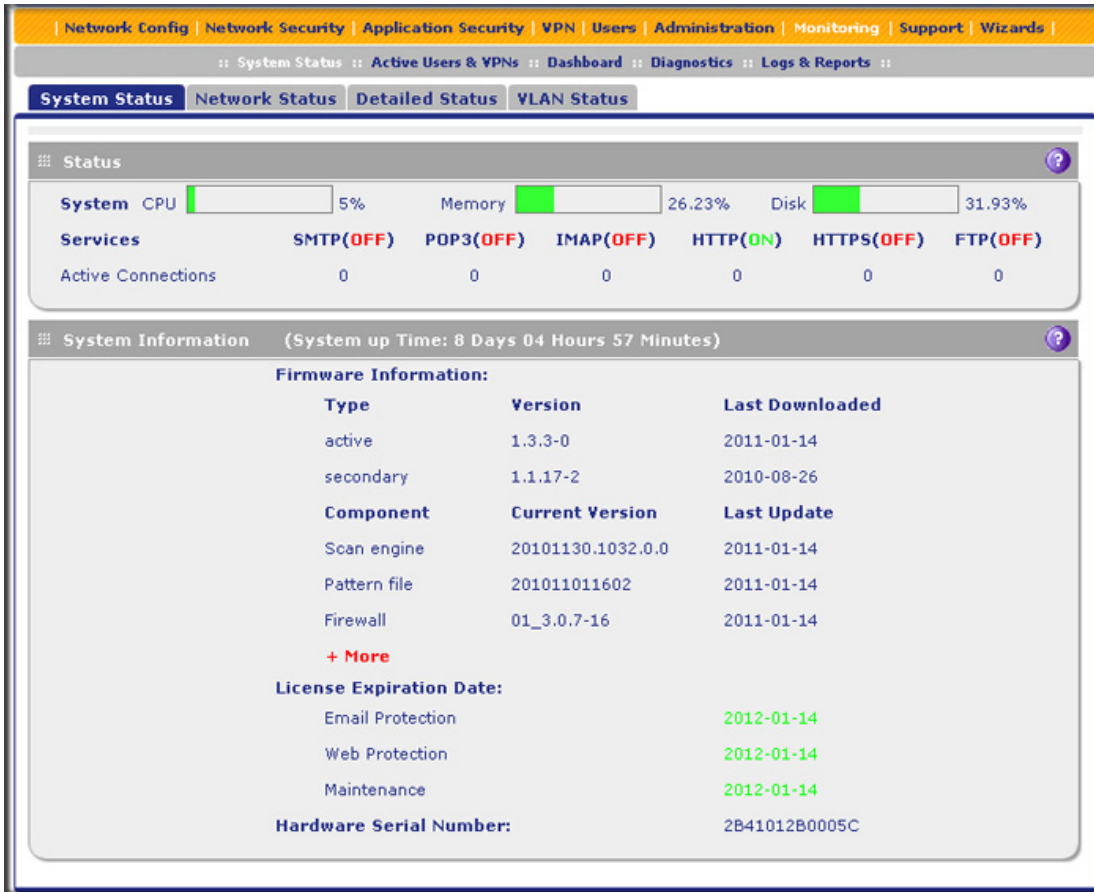
Figure 20.

Web Management Interface Menu Layout

The following figure shows the menu at the top the UTM50 web management interface as an example.

Figure 21.

The web management interface menu consists of the following components:

- **1st level: Main navigation menu links**. The main navigation menu in the orange bar across the top of the web management interface provides access to all the configuration functions of the UTM, and remains constant. When you select a main navigation menu link, the letters are displayed in white against an orange background.

- **2nd level: Configuration menu links**. The configuration menu links in the gray bar (immediately below the main navigation menu bar) change according to the main navigation menu link that you select. When you select a configuration menu link, the letters are displayed in white against a gray background.

- **3rd level: Submenu tabs**. Each configuration menu item has one or more submenu tabs that are listed below the gray menu bar. When you select a submenu tab, the text is displayed in white against a blue background.

- **Option arrows**. If there are additional screens for the submenu item, links to the screens display on the right side in blue letters against a white background, preceded by a white arrow in a blue circle.

The bottom of each screen provides action buttons. The nature of the screen determines which action buttons are shown. The following figure shows an example:

Figure 22.

Any of the following action buttons might display on screen (this list might not be complete):

- **Apply**. Save and apply the configuration.
- **Reset**. Cancel the changes and reset the configuration to the current values.
- **Test**. Test the configuration before you decide whether or not to save and apply the configuration.
- **Auto Detect**. Enable the UTM to detect the configuration automatically and suggest values for the configuration.
- **Next**. Go to the next screen (for wizards).
- **Back**. Go to the previous screen (for wizards).
- **Search**. Perform a search operation.
- **Cancel**. Cancel the operation.
- **Send Now**. Send a file or report.

When a screen includes a table, table buttons display to let you configure the table entries. The nature of the screen determines which table buttons are shown. The following figure shows an example:
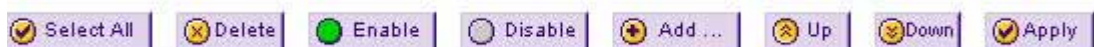
Figure 23.

Any of the following table buttons might display on screen:

- **Select All**. Select all entries in the table.
- **Delete**. Delete the selected entry or entries from the table.
- **Enable**. Enable the selected entry or entries in the table.
- **Disable**. Disable the selected entry or entries in the table.
- **Add**. Add an entry to the table.
- **Edit**. Edit the selected entry.
- **Up**. Move the selected entry up in the table.
- **Down**. Move the selected entry down in the table.
- **Apply**. Apply the selected entry.

Almost all screens and sections of screens have an accompanying help screen. To open the help screen, click the (question mark) icon.

Use the Setup Wizard to Perform the Initial Configuration

The Setup Wizard facilitates the initial configuration of the UTM by taking you through 10 screens, the last of which allows you to save the configuration. If you prefer to perform the initial WAN setup manually, see *Chapter 3, Manually Configuring Internet and WAN Settings*.

➢ **To start the Setup Wizard:**

1. Select **Wizards** from the main navigation menu. The Welcome to the Netgear Configuration Wizard screen displays:
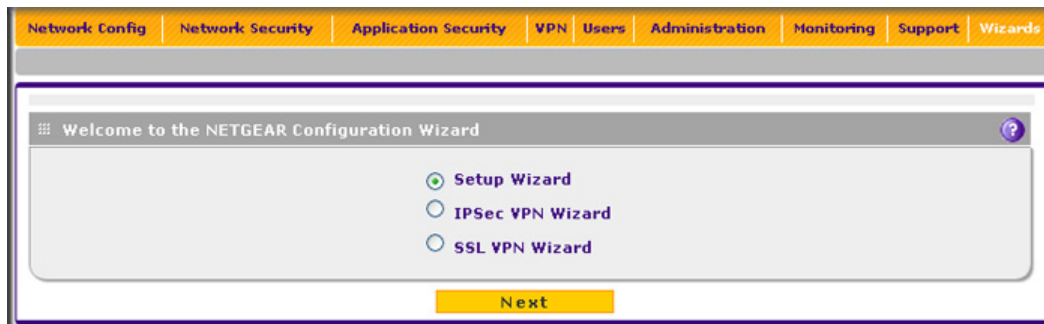
Figure 24.

2. Select the **Setup Wizard** radio button.
3. Click **Next**. The first Setup Wizard screen displays.

The following sections explain the 9 configuration screens of the Setup Wizard. On the 10th screen, you can save your configuration.

The tables in the following sections explain the buttons and fields of the Setup Wizard screens. Additional information about the settings in the Setup Wizard screens is provided in other chapters that explain manual configuration; each of the following sections provides a specific link to a section in another chapter.

Setup Wizard Step 1 of 10: LAN Settings

Figure 25.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

> **Note:** In this first step, you are actually configuring the LAN settings for the UTM's default VLAN. For more information about VLANs, see *Manage Virtual LANs and DHCP Options* on page 93.

Table 4. Setup Wizard Step 1: LAN Settings screen settings

Setting	Description	
LAN TCP/IP Setup		
IP Address	Enter the IP address of the UTM's default VLAN (the factory default address is 192.168.1.1). **Note:** Always make sure that the LAN port IP address and DMZ port IP address are in different subnets. **Note:** If you change the LAN IP address of the UTM's default VLAN while being connected through the browser, you are disconnected. You then need to open a new connection to the new IP address and log in again. For example, if you change the default IP address from 192.168.1.1 to 10.0.0.1, you now need to enter **https://10.0.0.1** in your browser to reconnect to the web management interface.	
Subnet Mask	Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. The UTM automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the UTM).	
DHCP		
Disable DHCP Server	If another device on your network is the DHCP server for the default VLAN, or if you will manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. By default, this radio button is not selected, and the DHCP server is enabled.	
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the UTM to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the default VLAN. Enter the following settings.	
	Domain Name	This setting is optional. Enter the domain name of the UTM.
	Starting IP Address	Enter the starting IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the ending IP address. The IP address 192.168.1.2 is the default starting address.
	Ending IP Address	Enter the ending IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address. **Note:** The starting and ending DHCP IP addresses should be in the same *network* as the LAN TCP/IP address of the UTM (that is, the IP address in the LAN TCP/IP Setup section as described earlier in this table).

Table 4. Setup Wizard Step 1: LAN Settings screen settings (continued)

Setting	Description	
Enable DHCP Server (continued)	Primary DNS Server	This setting is optional. If an IP address is specified, the UTM provides this address as the primary DNS server IP address. If no address is specified, the UTM provides its own LAN IP address as the primary DNS server IP address.
	Secondary DNS Server	This setting is optional. If an IP address is specified, the UTM provides this address as the secondary DNS server IP address.
	WINS Server	This setting is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.
DHCP Relay	Select the **DHCP Relay** radio button to use the UTM as a DHCP relay agent for a DHCP server somewhere else on your network. Enter the following setting:	
	Relay Gateway	The IP address of the DHCP server for which the UTM serves as a relay.
Enable LDAP information	Select the **Enable LDAP information** check box to enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information. Enter the following settings. **Note:** The LDAP settings that you specify as part of the VLAN profile are used only for SSL VPN and UTM authentication, but not for web and email security.	
	LDAP Server	The IP address or name of the LDAP server.
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begins. You can specify multiple search objects, separated by commas. The search objects include: • CN (for common name) • OU (for organizational unit) • O (for organization) • C (for country) • DC (for domain) For example, to search the Netgear.net domain for all last names of Johnson, you would enter: cn=Johnson,dc=Netgear,dc=net
	Port	The port number for the LDAP server. The default setting is 0 (zero).
DNS Proxy		
Enable DNS Proxy	This setting is optional. Select the **Enable DNS Proxy** radio button to enable the UTM to provide a LAN IP address for DNS address name resolution. This radio button is selected by default. **Note:** When the DNS Proxy option is disabled, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address.	

Table 4. Setup Wizard Step 1: LAN Settings screen settings (continued)

Setting	Description
Inter VLAN Routing	
Enable Inter VLAN Routing	This setting is optional. To ensure that traffic is routed only to VLANs for which inter-VLAN routing is enabled, select the **Enable Inter VLAN Routing** check box. This setting is disabled by default. When the Enable Inter VLAN Routing check box is not selected, traffic from this VLAN is not routed to other VLANs, and traffic from other VLANs is not routed to this VLAN. **Note:** For information about inter-VLAN firewall rules, see *VLAN Rules* on page 144.

After you have completed the steps in the Setup Wizard, you can make changes to the LAN settings by selecting **Network Config > LAN Settings > Edit LAN Profile**. For more information about these LAN settings, see *VLAN DHCP Options* on page 96.

Setup Wizard Step 2 of 10: WAN Settings

Figure 26.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

> **Note:** Instead of manually entering the settings, you can also click the **Auto Detect** action button at the bottom of the screen. The autodetect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support.

Table 5. Setup Wizard Step 2: WAN Settings screen settings

Setting	Description	
ISP Login		
Does your Internet connection require a login?	If you need to enter login information every time you connect to the Internet through your ISP, select the **Yes** radio button. Otherwise, select the **No** radio button, which is the default setting, and skip the ISP Type section. If you select the **Yes** radio button, enter the following settings.	
	Login	The login name that your ISP has assigned to you.
	Password	The password that your ISP has assigned to you.
ISP Type		
What type of ISP connection do you use?	If your connection is PPPoE or PPTP, then you need to log in. Select the **Yes** radio button. Based on the connection that you select, the text fields that require data entry are highlighted. If your ISP has not assigned any login information, then select the **No** radio button and skip this section. If you select the **Yes** radio button, enter the following settings.	
Austria (PPTP)	If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this radio button and enter the following settings:	
	Account Name	The account name is also known as the host name or system name. Enter the valid account name for the PPTP connection (usually your email ID assigned by your ISP). Some ISPs require you to enter your full email address here.
	Domain Name	Your domain name or workgroup name assigned by your ISP, or your ISP's domain name. You can leave this field blank.
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Timeout** radio button and, in the time-out field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in.
	My IP Address	The IP address assigned by the ISP to make the connection with the ISP server.
	Server IP Address	The IP address of the PPTP server.

Table 5. Setup Wizard Step 2: WAN Settings screen settings (continued)

Setting	Description	
Other (PPPoE)	If you have installed login software such as WinPoET or Enternet, then your connection type is PPPoE. Select this radio button and enter the following settings:	
	Account Name	The valid account name for the PPPoE connection.
	Domain Name	The name of your ISP's domain or your domain name if your ISP has assigned one. You can leave this field blank.
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Timeout** radio button and, in the time-out field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in. **Note:** When you use a PPPoE connection and select the Idle Timeout radio button, you cannot configure load balancing (see *Configure Load Balancing (Multiple WAN Port Models)* on page 81). To use load balancing on a PPPoE connection, select the **Keep Connected** radio button.
	Connection Reset	Select the **Connection Reset** check box to specify a time when the PPPoE WAN connection is reset, that is, the connection is disconnected momentarily and then reestablished. Then, specify the disconnect time and delay.
	Disconnect Time	Specify the hour and minutes when the connection should be disconnected.
	Delay	Specify the period in seconds after which the connection should be reestablished.
Internet (IP) Address Click the **Current IP Address** link to see the currently assigned IP address.		
Get Dynamically from ISP	If your ISP has not assigned you a static IP address, select the **Get dynamically from ISP** radio button. The ISP automatically assigns an IP address to the UTM using DHCP network protocol.	
	Client Identifier	Select the **Client Identifier** check box if your ISP requires the client identifier information to assign an IP address using DHCP.
	Vendor Class Identifier	Select the **Vendor Class Identifier** check box if your ISP requires the vendor class identifier information to assign an IP address using DHCP.

Table 5. Setup Wizard Step 2: WAN Settings screen settings (continued)

Setting	Description	
Use Static IP Address	If your ISP has assigned you a fixed (static or permanent) IP address, select the **Use Static IP Address** radio button and enter the following settings.	
	IP Address	The static IP address assigned to you. This address identifies the UTM to your ISP.
	Subnet Mask	The subnet mask, which is usually provided by your ISP.
	Gateway IP Address	The IP address of the ISP's gateway, which is usually provided by your ISP.
Domain Name Server (DNS) Servers		
Get Automatically from ISP	If your ISP has not assigned any Domain Name Servers (DNS) addresses, select the **Get Automatically from ISP** radio button.	
Use These DNS Servers	If your ISP has assigned DNS addresses to you, select the **Use these DNS Servers** radio button. Make sure that you fill in valid DNS server IP addresses in the fields. Incorrect DNS entries might cause connectivity issues.	
	Primary DNS Server	The IP address of the primary DNS server.
	Secondary DNS Serve	The IP address of the secondary DNS server.

After you have completed the steps in the Setup Wizard, you can make changes to the WAN settings by selecting **Network Config > WAN Settings**. Then click the **Edit** button in the Action column of the WAN interface for which you want to change the settings.

For more information about these WAN settings, see *Manually Configure the Internet Connection* on page 71.

Setup Wizard Step 3 of 10: System Date and Time

Figure 27.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Table 6. Setup Wizard Step 3: System Date and Time screen settings

Setting	Description
Set Time, Date, and NTP Servers	
Date/Time	From the drop-down list, select the local time zone in which the UTM operates. The correct time zone is required in order for scheduling to work correctly. The UTM includes a real-time clock (RTC), which it uses for scheduling.
Automatically Adjust for Daylight Savings Time	If daylight savings time is supported in your region, select the **Automatically Adjust for Daylight Savings Time** check box.
NTP Server (default or custom)	From the drop-down list, select an NTP server: • **Use Default NTP Servers**. The UTM's RTC is updated regularly by contacting a default NETGEAR NTP server on the Internet. • **Use Custom NTP Servers**. The UTM's RTC is updated regularly by contacting one of the two NTP servers (primary and backup), both of which you need to specify in the fields that become available with this selection. **Note:** If you select this option but leave either the Server 1 or Server 2 field blank, both fields are set to the default NETGEAR NTP servers. **Note:** A list of public NTP servers is available at *http://support.ntp.org/bin/view/Servers/WebHome*.
	Server 1 Name / IP Address	Enter the IP address or host name of the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name of the backup NTP server.

After you have completed the steps in the Setup Wizard, you can make changes to the date and time by selecting **Administration > System Date & Time**. For more information about these settings, see *Configure Date and Time Service* on page 412.

Setup Wizard Step 4 of 10: Services

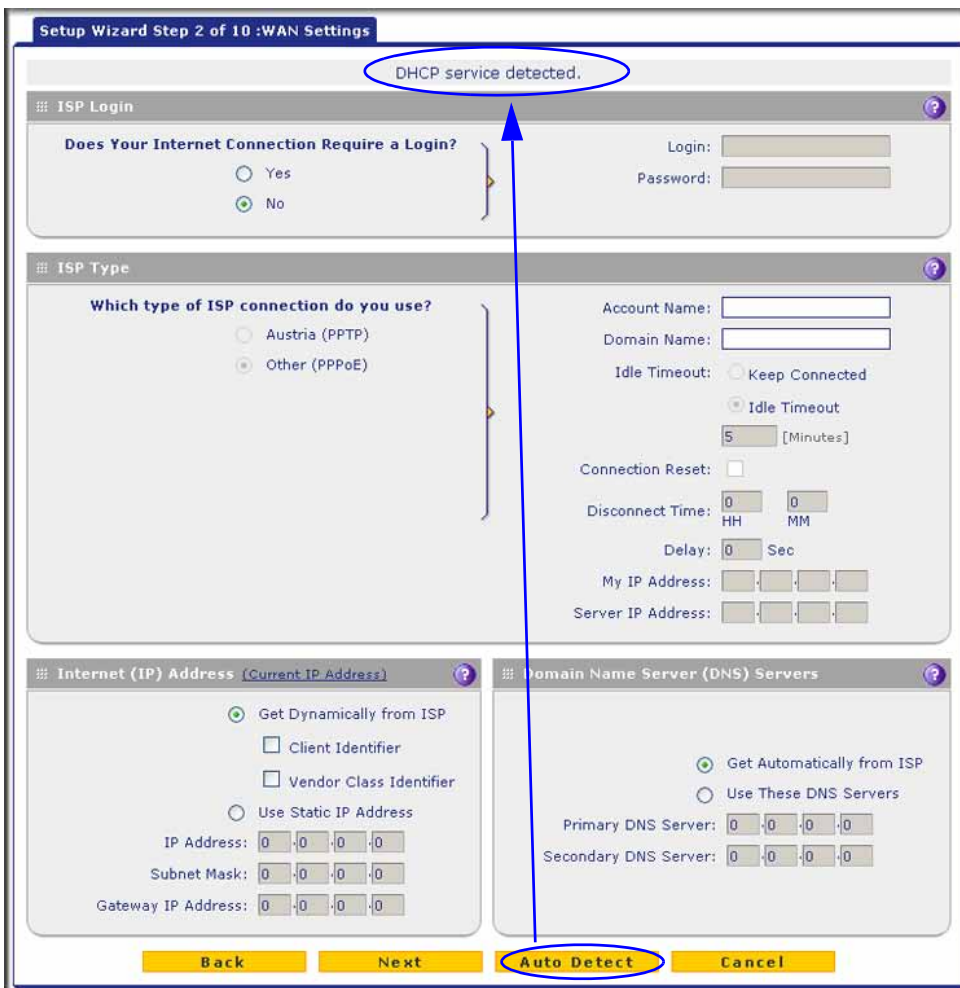**Figure 28.**

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Table 7. Setup Wizard Step 4: Services screen settings

Setting	Description	
Email		
SMTP	SMTP scanning is enabled by default on standard service port 25.	To disable any of these services, clear the corresponding check box. You can change the standard service port or add another port in the corresponding Ports to Scan field.
POP3	POP3 scanning is enabled by default on standard service port 110.	
IMAP	IMAP scanning is enabled by default on standard service port 143.	

Table 7. Setup Wizard Step 4: Services screen settings (continued)

Setting	Description	
Web		
HTTP	HTTP scanning is enabled by default on standard service port 80.	To disable HTTP scanning, clear the corresponding check box. You can change the standard service port or add another port in the corresponding Ports to Scan field.
HTTPS	HTTPS scanning is disabled by default.	To enable HTTPS scanning, select the corresponding check box. You can change the standard service port (443) or add another port in the corresponding Ports to Scan field.
FTP	FTP scanning is enabled by default on standard service port 21.	To disable FTP scanning, clear the corresponding check box. You cannot change the standard service port in the corresponding Ports to Scan field.
Instant Messaging		
Google Talk	Scanning of these instant messaging services is disabled by default. To enable any of these services, select the corresponding check box. **Note:** For instant messaging services, the following services can be blocked: logging in, sharing files, sharing video, sharing audio, and text messaging.	
ICQ		
mIRC		
MSN Messenger		
QQ		
Yahoo Messenger		
Peer-to-Peer (P2P)		
BitTorrent	Scanning of these file-sharing applications is disabled by default. To enable any of these services, select the corresponding check box.	
eDonkey		
Gnutella		
Media Applications		
iTunes (Music Store, update)	Scanning of these media applications is disabled by default. To enable any of these applications, select the corresponding check box.	
QuickTime (Update)		
Real Player (Guide)		
Rhapsody (Guide, Music Store)		
Winamp (Internet Radio/TV)		

Table 7. Setup Wizard Step 4: Services screen settings (continued)

Setting	Description
SSL Handshaking to Websites **Note:** SSL handshaking is supported only on the UTM9S.	
Facebook	Scanning of Facebook is disabled by default. To enable it, select the corresponding check box. (This option is not shown in the previous figure, but it is shown in *Figure 110* on page 195.)
Tools	
Alexa Toolbar	Scanning of these tools is disabled by default. To enable any of these tools, select the corresponding check box.
GoToMyPC	
Weatherbug	
Yahoo Toolbar	

After you have completed the steps in the Setup Wizard, you can make changes to the security services by selecting **Application Security > Services**. For more information about these settings, see *Customize Email Protocol Scan Settings* on page 178 and *Customize Web Protocol Scan Settings and Services (Web Applications)* on page 194.

Setup Wizard Step 5 of 10: Email Security

Figure 29.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Table 8. Setup Wizard Step 5: Email Security screen settings

Setting	Description
Action	
SMTP	From the SMTP drop-down list, select one of the following actions to be taken when an infected email is detected: • **Block infected email**. This is the default setting. The email is blocked, and a log entry is created. • **Delete attachment**. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The email is not blocked, and the attachment is not deleted. • **Quarantine attachment** (UTM9S only). The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176). • **Quarantine infected email** (UTM9S only). The email is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176).
POP3	From the POP3 drop-down list, select one of the following actions to be taken when an infected email is detected: • **Delete attachment**. This is the default setting. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The email is not blocked, and the attachment is not deleted. • **Quarantine attachment** (UTM9S only). The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176).
IMAP	From the IMAP drop-down list, select one of the following actions to be taken when an infected email is detected: • **Delete attachment**. This is the default setting. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The email is not blocked, and the attachment is not deleted. • **Quarantine attachment** (UTM9S only). The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176).
Scan Exceptions	
The default maximum size of the file or message that is scanned is 2048 KB, but you can define a maximum size of up to 10240 KB. However, setting the maximum size to a high value might affect the UTM's performance (see *Performance Management* on page 389). From the drop-down list, select one of the following actions to be taken when the file or message exceeds the maximum size: • **Skip**. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • **Block.** The file is blocked and does not reach the end user.	

After you have completed the steps in the Setup Wizard, you can make changes to the email security settings by selecting **Application Security > Email Anti-Virus**. The Email Anti-Virus screen also lets you specify notification settings and email alert settings. For more information about these settings, see *Customize Email Antivirus and Notification Settings* on page 179.

Setup Wizard Step 6 of 10: Web Security

Figure 30.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Table 9. Setup Wizard Step 6: Web Security screen settings

Setting	Description
Action	
HTTP	From the HTTP drop-down list, select one of the following actions to be taken when an infected web file or object is detected: • **Delete file**. This is the default setting. The web file or object is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The web file or object is not deleted. • **Quarantine file** (UTM9S only). The web file or object is quarantined, and a log entry is created (see the Note on page 176). Select the **Streaming** check box to enable streaming of partially downloaded and scanned HTTP file parts to the user. This method allows the user to experience more transparent web downloading. Streaming is enabled by default.

Table 9. Setup Wizard Step 6: Web Security screen settings (continued)

Setting	Description
HTTPS	From the HTTPS drop-down list, select one of the following actions to be taken when an infected web file or object is detected: • **Delete file**. This is the default setting. The web file or object is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The web file or object is not deleted. • **Quarantine file** (UTM9S only). The web file or object is quarantined, and a log entry is created (see the Note on page 176). Select the **Streaming** check box to enable streaming of partially downloaded and scanned HTTPS file parts to the user. This method allows the user to experience more transparent web downloading. Streaming is enabled by default.
FTP	From the FTP drop-down list, select one of the following actions to be taken when an infected web file or object is detected: • **Delete file**. This is the default setting. The FTP file or object is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The FTP file or object is not deleted. • **Quarantine file** (UTM9S only). The FTP file or object is quarantined, and a log entry is created (see the Note on page 176).
Scan Exceptions	
The default maximum size of the file or object that is scanned is 2048 KB, but you can define a maximum size of up to 10240 KB. However, setting the maximum size to a high value might affect the UTM's performance (see *Performance Management* on page 389). From the drop-down list, select one of the following actions to be taken when the file or message exceeds the maximum size: • **Skip**. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • **Block.** The file is blocked and does reach the end user.	

After you have completed the steps in the Setup Wizard, you can make changes to the web security settings by selecting **Application Security > HTTP/HTTPS > Malware Scan**. The Malware Scan screen also lets you specify HTML scanning and notification settings. For more information about these settings, see *Configure Web Malware Scans* on page 197.

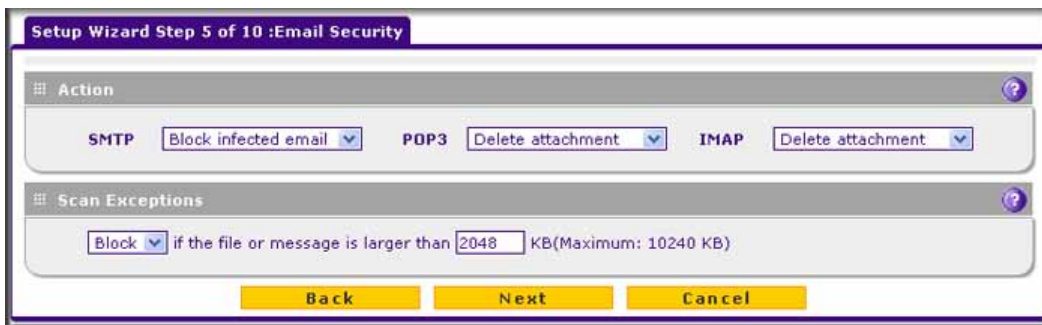## Setup Wizard Step 7 of 10: Web Categories to Be Blocked

Figure 31.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Table 10. Setup Wizard Step 7: Web Categories to be blocked screen settings

Setting	Description
Blocked Web Categories	
Select the **Enable Blocking** check box to enable blocking of web categories. (By default, this check box is selected.) Select the check boxes of any web categories that you want to block. Use the action buttons at the top of the section in the following way: • **Allow All**. All web categories are allowed. • **Block All**. All web categories are blocked. • **Set to Defaults**. Blocking and allowing of web categories are returned to their default settings. See *Table 38* on page 176 for information about the web categories that are blocked by default. Categories that are preceded by a green square are allowed by default; categories that are preceded by a pink square are blocked by default.	
Blocked Categories Scheduled Days	
Make one of the following selections: • Select the **All Days** radio button to enable content filtering to be active all days of the week. • Select the **Specific Days** radio button to enable content filtering to be active on the days that are specified by the check boxes.	
Blocked Categories Time of Day	
Make one of the following selections: • Select the **All Day** radio button to enable content filtering to be active all 24 hours of each selected day. • Select the **Specific Times** radio button to enable content filtering to be active during the time that is specified by the Start Time and End Time fields for each day that content filtering is active.	

After you have completed the steps in the Setup Wizard, you can make changes to the content-filtering settings by selecting **Application Security > HTTP/HTTPS > Content Filtering**. The Content Filtering screen lets you specify additional filtering tasks and notification settings. For more information about these settings, see *Configure Web Content Filtering* on page 199.

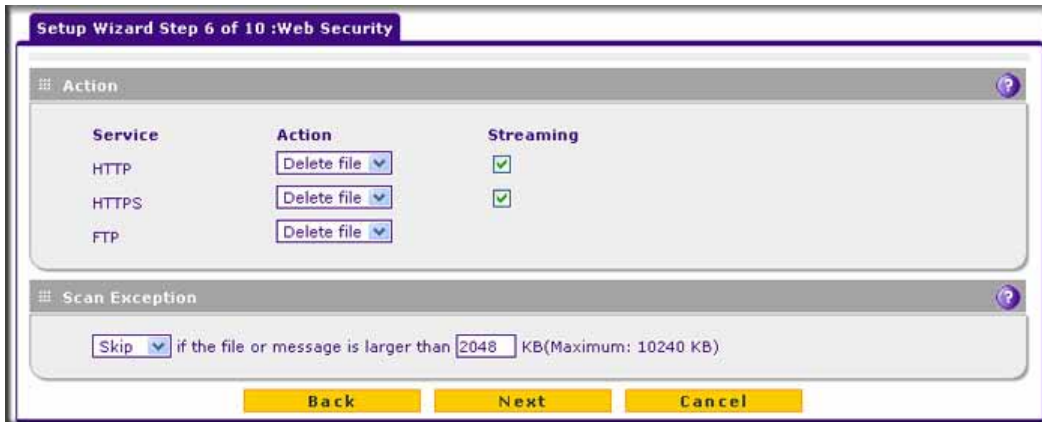# Setup Wizard Step 8 of 10: Email Notification

Figure 32.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Table 11. Setup Wizard Step 8: Email Notification screen settings

Setting	Description
Administrator Email Notification Settings	
Show as mail sender	A descriptive name of the sender for email identification purposes. For example, enter UTM_Notifications@netgear.com.
SMTP server	The IP address and port number or Internet name and port number of your ISP's outgoing email SMTP server. The default port number is 25. **Note:** If you leave this field blank, the UTM cannot send email notifications.
This server requires authentication	If the SMTP server requires authentication, select the **This server requires authentication** check box, and enter the user name and password.
	User name	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.
Send notifications to	The email address to which the notifications should be sent. Typically, this is the email address of the administrator.

After you have completed the steps in the Setup Wizard, you can make changes to the administrator email notification settings by selecting **Network Config > Email Notification**. For more information about these settings, see *Configure the Email Notification Server* on page 422.

Setup Wizard Step 9 of 10: Signatures & Engine

Figure 33.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Table 12. Setup Wizard Step 9: Signatures & Engine screen settings

Setting	Description
Update Settings	
Update	From the drop-down list, select one of the following options: • **Never**. The pattern and firmware files are never automatically updated. • **Scan engine and Signatures**. The pattern and firmware files are automatically updated according to the settings in the Update Frequency section on the screen (see explanations later in this table).
Update From	Set the update source server by selecting one of the following radio buttons: • **Default update server**. Files are updated from the default NETGEAR update server. • **Server address**. Files are updated from the server that you specify. Enter the IP address or host name of the update server in the Server address field.

Table 12. Setup Wizard Step 9: Signatures & Engine screen settings (continued)

Setting	Description	
Update Frequency		
Specify the frequency with which the UTM checks for file updates: • **Weekly**. From the drop-down lists, select the weekday, hour, and minutes that the updates occur. • **Daily**. From the drop-down lists, select the hour and minutes that the updates occur. • **Every**. From the drop-down list, select the frequency with which the updates occur. The range is from 15 minutes to 12 hours.		
HTTPS Proxy Settings		
Enable	If computers on the network connect to the Internet through a proxy server, select the **Enable** check box to specify and enable a proxy server. Enter the following settings.	
	Proxy server	The IP address and port number of the proxy server.
	User name	The user name for proxy server authentication.
	Password	The password for proxy server authentication.

After you have completed the steps in the Setup Wizard, you can make changes to the signatures and engine settings by selecting **Administration > System Update > Signatures & Engine**. For more information about these settings, see *Update the Scan Signatures and Scan Engine Firmware* on page 410.

Setup Wizard Step 10 of 10: Saving the Configuration

Figure 34.

Click **Apply** to save your settings and automatically restart the system.

Verify Correct Installation

Test the UTM before deploying it in a live production environment. The following instructions walk you through a couple of quick tests that are designed to ensure that your UTM is functioning correctly.

Test Connectivity

➢ **Verify that network traffic can pass through the UTM:**

1. Ping an Internet URL.
2. Ping the IP address of a device on either side of the UTM.

Test HTTP Scanning

If client computers have direct access to the Internet through your LAN, try to download the eicar.com test file from *http://www.eicar.org/download/eicar.com*.

The eicar.com test file is a *legitimate* denial of service (DoS) attack and is safe to use because it is not a malware threat and does not include any fragments of malware code. The test file is provided by EICAR, an organization that unites efforts against computer crime, fraud, and misuse of computers or networks.

➢ **Verify that the UTM scans HTTP traffic correctly:**

1. Log in to the UTM web management interface, and then verify that HTTP scanning is enabled. For information about how to enable HTTP scanning, see *Customize Web Protocol Scan Settings and Services (Web Applications)* on page 194 and *Configure Web Malware Scans* on page 197.
2. Check the downloaded eicar.com test file, and note the attached malware information file.

Register the UTM with NETGEAR

To receive threat management component updates and technical support, you need to register your UTM with NETGEAR. The UTM is bundled with three 30-day trial licenses:

• Web scanning
• Email scanning
• Support and maintenance

The service license keys are provided with the product package (see *Service Registration Card with License Keys* on page 20). For electronic licensing, you do not need the service license keys (see *Electronic Licensing* on page 64).

Note: Activating the service licenses initiates their terms of use. Activate the licenses only when you are ready to start using this unit. If your unit has never been registered before, you can use the 30-day trial period for all three types of licenses to perform the initial testing and configuration. To use the trial period, do *not* click Register in *step 4* of the following procedure, but click **Trial** instead.

> **If your UTM is connected to the Internet, you can activate the service licenses:**

1. Select **Support > Registration**. The Registration screen displays:

Figure 35.

2. Enter the license key in the Registration Key field.
3. Fill out the customer and value-added reseller (VAR) fields.
4. Click **Register**.

⚠ **WARNING!**

To activate the 30-day trial period for a license, do *not* click Register but click Trial instead.

5. Repeat *step 2* and *step 4* for additional license keys.

The UTM activates the licenses and registers the unit with the NETGEAR registration server.

> **Note:** The 30-day trial licenses are revoked once you activate the purchased service license keys. The purchased service license keys offer 1 year or 3 years of service.

> **Note:** When you reset the UTM to the original factory default settings after you have entered the license keys to activate the UTM (see *Register the UTM with NETGEAR* on page 62), the license keys are erased. The license keys and the different types of licenses that are available for the UTM are no longer displayed on the Registration screen. However, after you have reconfigured the UTM to connect to the Internet and to the NETGEAR registration server, the UTM retrieves and restores all registration information based on its MAC address and hardware serial number. You do not need to reenter the license keys and reactivate the UTM.

Electronic Licensing

If you have purchased the UTM bundled together with a 1- or 3-year license bundle, you can use the electronic licensing option. When the UTM is connected to the Internet, you need to enter only your customer information and optional value-added reseller (VAR) information on the Register screen but do not need to enter the license numbers. When you click Register, the UTM automatically downloads and activates the license keys because the serial number of the UTM is linked to the license bundle.

If you have purchased licenses from a VAR (either directly or over the web) *after* purchase of the UTM, the VAR should email you the license keys or provide them to you in another way. To register and activate the license keys, follow the regular registration procedure that is explained in the previous section.

What to Do Next

You have completed setting up the UTM to the network. The UTM is now ready to scan the protocols and services that you specified and perform automatic updates based on the update source and frequency that you specified.

If you need to change the settings, or to view reports or logs, log in to the UTM web management interface, using the default IP address or the IP address that you assigned to the UTM in *Setup Wizard Step 1 of 10: LAN Settings* on page 43.

The UTM is ready for use. However, the following sections describe important tasks that you might want to address before you deploy the UTM in your network:

- *Configure the WAN Mode* (required for the multiple WAN port models).
- *Configure Authentication Domains, Groups, and Users*
- *Manage Digital Certificates for VPN Connections*
- *Use the IPSec VPN Wizard for Client and Gateway Configurations*
- *Use the SSL VPN Wizard for Client Configurations*

Manually Configuring Internet and WAN Settings

3

This chapter contains the following sections:

- *Internet and WAN Configuration Tasks*
- *Automatically Detecting and Connecting the Internet Connections*
- *Manually Configure the Internet Connection*
- *Configure the WAN Mode*
- *Configure Secondary WAN Addresses*
- *Configure Dynamic DNS*
- *Configure Advanced WAN Options*

> **Note:** The initial Internet configuration of the UTM is described in *Chapter 2, Using the Setup Wizard to Provision the UTM in Your Network*. If you used the Setup Wizard to configure your Internet settings, you need this chapter only to configure WAN features such as multiple WAN connections (not applicable to the single WAN port models) and dynamic DNS, and to configure secondary WAN addresses and advanced WAN options.

> **Note:** The Wireless Settings configuration menu is shown on the UTM9S only, accessible under the Network Config main navigation menu.

> **Note:** On the UTM9S, the Email Notification configuration menu is accessible under the Monitoring main navigation menu instead of the Network Config main navigation menu.

Internet and WAN Configuration Tasks

> **Note:** For information about configuring the DSL interface of the UTM9S, see *Appendix A, xDSL Module for the UTM9S*. The information in this chapter does also apply to the WAN interfaces of the UTM9S.

Generally, five steps are required to complete the WAN Internet connection of your UTM.

➢ **Complete these steps:**

1. **Configure the Internet connections to your ISPs**. During this phase, you connect to your ISPs. See *Automatically Detecting and Connecting the Internet Connections* on page 67 or *Manually Configure the Internet Connection* on page 71.

2. **Configure the WAN mode (required for multiple WAN port models)**. For all models, select either NAT or classical routing. For the multiple WAN port models, select dedicated (single WAN) mode, auto-rollover mode, or load balancing mode. For load balancing, you can also select any necessary protocol bindings. See *Configure the WAN Mode* on page 75.

3. **Configure secondary WAN addresses on the WAN ports (optional)**. Configure aliases for each WAN port. See *Configure Secondary WAN Addresses* on page 85.

4. **Configure Dynamic DNS on the WAN ports (optional)**. Configure your fully qualified domain names during this phase (if required). See *Configure Dynamic DNS* on page 87.

5. **Configure the WAN options (optional)**. Optionally, you can enable each WAN port to respond to a ping, and you can change the factory default MTU size and port speed. However, these are advanced features, and changing them is not usually required. See *Configure Advanced WAN Options* on page 90.

Each of these tasks is detailed separately in this chapter.

> **Note:** For information about how to configure the WAN meters, see *Enable the WAN Traffic Meter* on page 419.

Automatically Detecting and Connecting the Internet Connections

To set up your UTM for secure Internet connections, the web management interface provides the option to automatically detect the network connections and configure the WAN port or ports. You can also manually configure the Internet connections and ports (see *Manually Configure the Internet Connection* on page 71).

➢ **To automatically configure the WAN ports for connection to the Internet:**

1. Select **Network Config > WAN Settings**. The WAN screen displays. (The following figure shows the UTM50.)
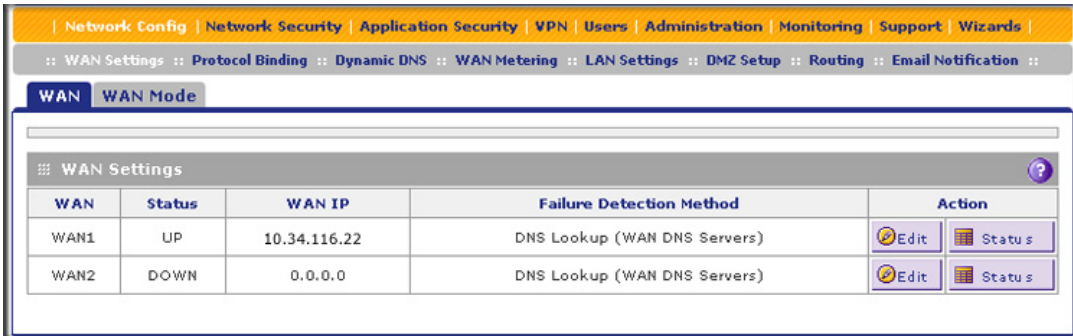
Figure 36.

The UTM5 and UTM10 screens show one WAN interface; the UTM25 and UTM50 screens show two WAN interfaces; the UTM150 screen shows four WAN interfaces; the UTM9S screen shows two WAN interfaces and a slot (SLOT-1 or SLOT-2), in which the xDSL module is installed.

The WAN Settings table displays the following fields:

- **WAN**. The WAN interface.
- **Status**. The status of the WAN interface (UP or DOWN).
- **WAN IP**. The IP address of the WAN interface.
- **Failure Detection Method**. The failure detection method that is active for the WAN interface. The following methods can be displayed:
    - None
    - DNS Lookup (WAN DNS Servers)
    - DNS Lookup (the configured IP address is displayed)
    - PING (the configured IP address is displayed)

    You can set the failure detection method for each WAN interface on its corresponding WAN Advanced Options screen (see *Configure Auto-Rollover Mode and the Failure Detection Method (Multiple WAN Port Models)* on page 78).

- **Action**. The Edit button provides access to the WAN ISP Settings screen (see *step 2*) for the corresponding WAN interface; the Status button provides access to the Connection Status screen (see *step 4*) for the corresponding WAN interface.

2. Click the **Edit** button in the Action column of the WAN interface or slot for which you want to automatically configure the connection to the Internet. The WAN ISP Settings screen displays.

   The following figure shows the WAN1 ISP Settings screen of the UTM50 as an example
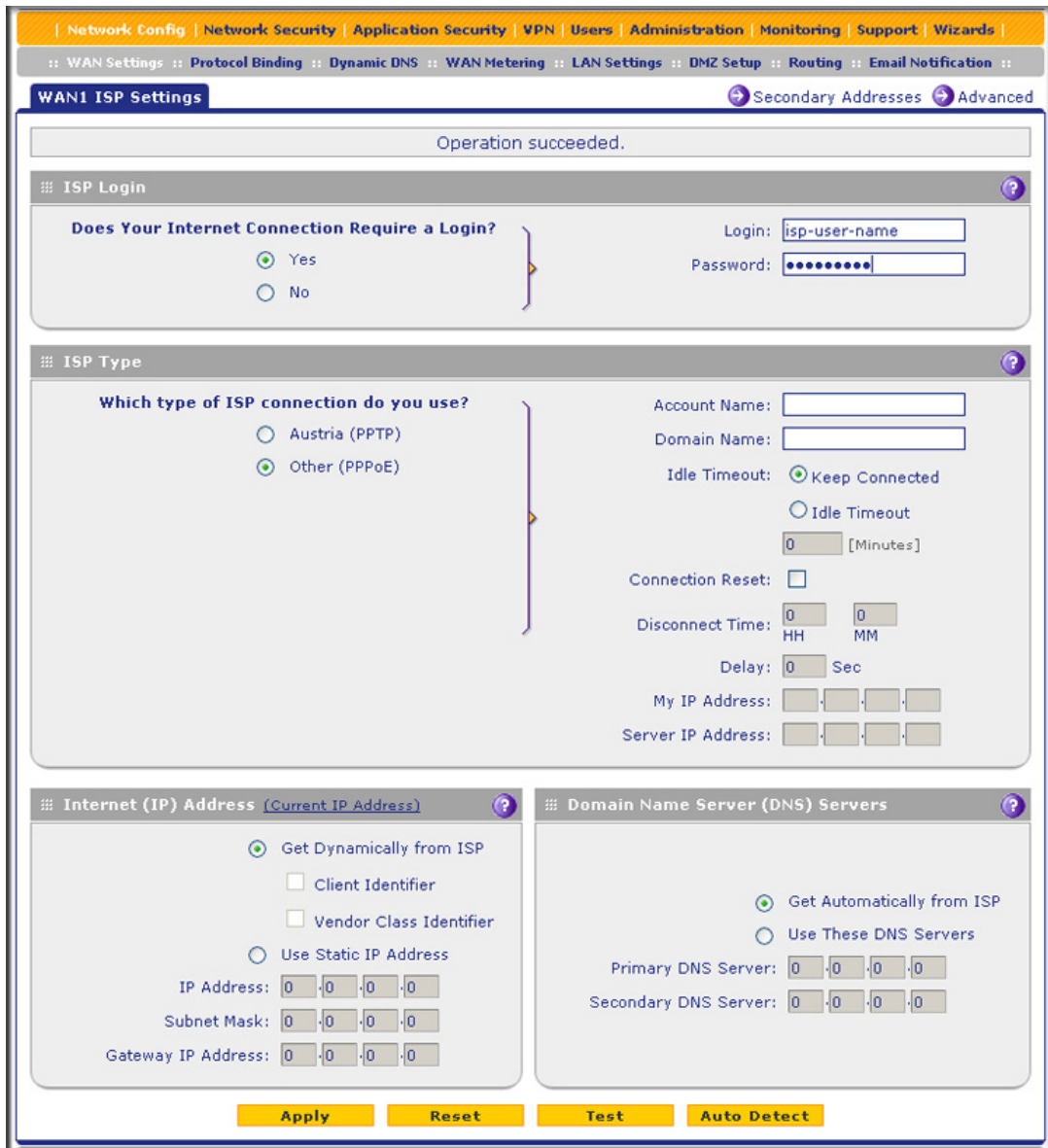
Figure 37.

3. Click the **Auto Detect** button at the bottom of the screen. The autodetect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support.

The autodetect process returns one of the following results:

- If the autodetect process is successful, a status bar at the top of the screen displays the results (for example, *DHCP service detected*).

- If the autodetect process senses a connection method that requires input from you, it prompts you for the information. All methods with their required settings are explained in the following table:

Table 13. Internet connection methods

Connection method	Manual data input required
DHCP (Dynamic IP)	No data is required.
PPPoE	Login, password, account name, and domain name.
PPTP	Login, password, account name, your IP address, and the server IP address.
Fixed (Static) IP	IP address, subnet mask, and gateway IP address, and related data supplied by your ISP.

- If the autodetect process does not find a connection, you are prompted either to check the physical connection between your UTM and the cable, DSL line, satellite dish, or wireless ISP radio antenna to check your UTM's MAC address. For more information, see *Configure Advanced WAN Options* on page 90 and *Troubleshoot the ISP Connection* on page 494.

4. To verify the connection:

   a. Return to the WAN screen by selecting **Network Config > WAN Settings**.

   b. Click the **Status** button in the Action column for the WAN interface that you just configured to display the Connection Status pop-up screen.
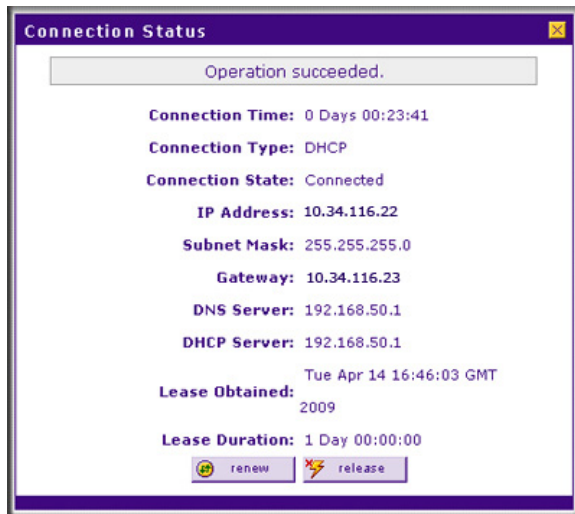
Figure 38.

The Connection Status screen should show a valid IP address and gateway. If the configuration was not successful, skip ahead to *Manually Configure the Internet Connection* on page 71, or see *Troubleshoot the ISP Connection* on page 494.

Note: If the configuration process was successful, you are connected to the Internet through the WAN that you just configured. For the multiple WAN port models, continue with the configuration process for the other WAN interfaces.

Note: For more information about the WAN Connection Status screen, see *View the WAN Ports Status* on page 456.

---

5. For the multiple WAN port models, repeat *step 2*, *step 3*, and *step 4* for any other WAN interface that you want to configure.

If the automatic WAN ISP configuration is successful, you can skip ahead to *Configure the WAN Mode* on page 75.

If the automatic WAN ISP configuration fails, you can attempt a manual configuration as described in *Manually Configure the Internet Connection* on this page, or see *Troubleshoot the ISP Connection* on page 494.

Set the UTM's MAC Address

Each computer or router on your network has a unique 48-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. The default is set to Use Default Address on the WAN Advanced Options screens. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then you need to enter that address on the WAN Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options* on page 90).

Manually Configure the Internet Connection

Unless your ISP automatically assigns your configuration through DHCP, you need to obtain configuration parameters from your ISP to manually establish an Internet connection. The necessary parameters for various connection types are listed in *Table 13* on page 70.

➢ **To manually configure the WAN ISP settings for an interface:**

1. Select **Network Config > WAN Settings**. The WAN screen displays (see *Figure 36* on page 68, which shows the UTM50).

2. Click the **Edit** button in the Action column of the WAN interface for which you want to configure the connection to the Internet. The WAN ISP Settings screen displays (see *Figure 37* on page 69, which shows the WAN1 ISP Settings screen as an example).

3. Locate the ISP Login section on the screen:

Figure 39.

In the ISP Login section, select one of the following options:

- If your ISP requires an initial login to establish an Internet connection, select **Yes**. (The default is No.)

- If a login is not required, select **No**, and ignore the Login and Password fields.

4. If you selected Yes, enter the login name in the Login field and the password in the Password field. This information is provided by your ISP.

5. In the ISP Type section of the screen, select the type of ISP connection that you use from the two listed options. By default, Other (PPPoE) is selected, as shown in the following figure:

Figure 40.

6. If your connection is PPTP or PPPoE, your ISP requires an initial login. Enter the settings as explained in the following table:

Table 14. PPTP and PPPoE settings

Setting	Description	
Austria (PPTP)	If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this radio button, and enter the following settings:	
	Account Name	The account name is also known as the host name or system name. Enter the account name for the PPTP connection (usually your email ID assigned by your ISP). Some ISPs require you to enter your full email address here.
	Domain Name	Your domain name or workgroup name assigned by your ISP, or your ISP's domain name. You can leave this field blank.
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Timeout** radio button and, in the time-out field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in.
	My IP Address	The IP address assigned by the ISP to make the connection with the ISP server.
	Server IP Address	The IP address of the PPTP server.
Other (PPPoE)	If you have installed login software, then your connection type is PPPoE. Select this radio button, and enter the following settings:	
	Account Name	The account name for the PPPoE connection.
	Domain Name	The name of your ISP's domain or your domain name if your ISP has you assigned one. You can leave this field blank.
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Timeout** radio button and, in the time-out field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in. **Note:** When you use a PPPoE connection and select the Idle Timeout radio button, you cannot configure load balancing (see *Configure Load Balancing (Multiple WAN Port Models)* on page 81). To use load balancing on a PPPoE connection, select the **Keep Connected** radio button. When you have configured load balancing, the Idle Timeout radio button and time-out field are masked out.

Table 14. PPTP and PPPoE settings (continued)

Setting	Description		
Other (PPPoE) (continued)	Connection Reset	Select the **Connection Reset** check box to specify a time when the PPPoE WAN connection is reset, that is, the connection is disconnected momentarily and then reestablished. Then, specify the disconnect time and delay.	
		Disconnect Time	Specify the hour and minutes when the connection should be disconnected.
		Delay	Specify the period in seconds after which the connection should be reestablished.

7. In the Internet (IP) Address section of the screen (see the following figure), configure the IP address settings as explained in the following table. Click the **Current IP Address** link to see the currently assigned IP address.
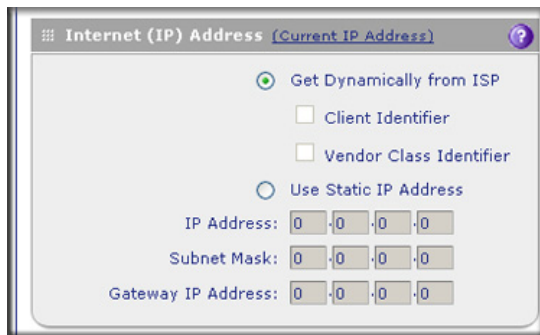
Figure 41.

Table 15. Internet IP address settings

Setting	Description	
Get Dynamically from ISP	If your ISP has not assigned you a static IP address, select the **Get Dynamically from ISP** radio button. The ISP automatically assigns an IP address to the UTM using DHCP network protocol.	
	Client Identifier	If your ISP requires the client identifier information to assign an IP address using DHCP, select the **Client Identifier** check box.
	Vendor Class Identifier	If your ISP requires the vendor class identifier information to assign an IP address using DHCP, select the **Vendor Class Identifier** check box.
Use Static IP Address	If your ISP has assigned you a fixed (static or permanent) IP address, select the **Use Static IP Address** radio button, and enter the following settings:	
	IP Address	Static IP address assigned to you. This address identifies the UTM to your ISP.
	Subnet Mask	The subnet mask is usually provided by your ISP.
	Gateway IP Address	The IP address of the ISP's gateway is usually provided by your ISP.

8. In the Domain Name Server (DNS) Servers section of the screen (see the following figure), specify the DNS settings as explained in the following table.

Figure 42.

Table 16. DNS server settings

Setting	Description	
Get Automatically from ISP	If your ISP has not assigned any Domain Name Server (DNS) addresses, select the **Get Automatically from ISP** radio button.	
Use These DNS Servers	If your ISP has assigned DNS addresses, select the **Use These DNS Servers** radio button. Make sure that you fill in valid DNS server IP addresses in the fields. Incorrect DNS entries might cause connectivity issues.	
	Primary DNS Server	The IP address of the primary DNS server.
	Secondary DNS Server	The IP address of the secondary DNS server.

9. Click **Test** to evaluate your entries. The UTM attempts to make a connection according to the settings that you entered.

10. Click **Apply** to save any changes to the WAN ISP settings. (Or click **Reset** to discard any changes and revert to the previous settings.)

For the multiple WAN port models, if you want to manually configure an additional WAN interface, select another WAN interface and repeat these steps. You can configure up to four WAN interfaces.

When you are finished, click the **Logout** link in the upper right of the web management interface, or proceed to additional setup and management tasks.

Configure the WAN Mode

For the multiple WAN port models, the UTM can be configured on a mutually exclusive basis for either auto-rollover (for increased system reliability) or load balancing (for maximum bandwidth efficiency). If you do not select load balancing, you need to specify one WAN interface as the primary interface.

> **Note:** For the UTM9S only, you can also use a DSL interface for any of the following modes (see *Appendix A, xDSL Module for the UTM9S*).

- **Load balancing mode**. The UTM distributes the outbound traffic equally among the WAN interfaces that are functional. Depending on the UTM model, you can configure up to four WAN interfaces. The UTM supports weighted load balancing and round-robin load balancing (see *Configure Load Balancing and Optional Protocol Binding* on page 81).

> **Note:** Scenarios could arise when load balancing needs to be bypassed for certain traffic or applications. If certain traffic needs to travel on a specific WAN interface, configure protocol binding rules for that WAN interface. The rule should match the desired traffic.

- **Primary WAN mode**. The selected WAN interface is made the primary interface. The other interfaces are disabled.

- **Auto-rollover mode**. The selected WAN interface is defined as the primary link, and another interface needs to be defined as the rollover link. If the UTM model has more than two WAN interfaces, the remaining interfaces are disabled. As long as the primary link is up, all traffic is sent over the primary link. When the primary link goes down, the rollover link is brought up to send the traffic. When the primary link comes back up, traffic automatically rolls back to the original primary link.

  If you want to use a redundant ISP link for backup purposes, select the WAN interface that needs to function as the primary link for this mode. Ensure that the backup WAN interface has also been configured and that you configure the WAN failure detection method on the WAN Advanced Options screen to support auto-rollover (see *Configure Auto-Rollover Mode and the Failure Detection Method (Multiple WAN Port Models)* on page 78).

Whichever WAN mode you select for the multiple WAN port models, you also need to select either NAT or classical routing, as explained in the following sections.

> **Note:** NAT and classical routing also apply to the single WAN port models.

⚠ **WARNING!**

When you change the WAN mode, the UTM restarts. If you change from primary WAN mode to load balancing mode, or the other way around, the interface through which you can access the UTM might change. Take note of the IP addresses of the interfaces before you change the WAN mode.

Configure Network Address Translation (All Models)

Network Address Translation (NAT) allows all PCs on your LAN to share a single public Internet IP address. From the Internet, there is only a single device (the UTM) and a single IP address. PCs on your LAN can use any private IP address range, and these IP addresses are not visible from the Internet.

Note the following about NAT:

- The UTM uses NAT to select the correct PC (on your LAN) to receive any incoming data.
- If you have only a single public Internet IP address, you need to use NAT (the default setting).
- If your ISP has provided you with multiple public IP addresses, you can use one address as the primary shared address for Internet access by your PCs, and you can map incoming traffic on the other public IP addresses to specific PCs on your LAN. This one-to-one inbound mapping is configured using an inbound firewall rule.

⚠ **WARNING!**

Changing the WAN mode from classical routing to NAT causes all LAN WAN and DMZ WAN inbound rules to revert to default settings.

➢ **To configure NAT:**

1. Select **Network Config > WAN Settings > WAN Mode**. The WAN Mode screen displays (see *Figure 43* on page 79).
2. In the NAT (Network Address Translation) section of the screen, select the **NAT** radio button.
3. Click **Apply** to save your settings.

Configure Classical Routing (All Models)

In classical routing mode, the UTM performs routing, but without NAT. To gain Internet access, each PC on your LAN needs to have a valid static Internet IP address.

If your ISP has allocated a number of static IP addresses to you, and you have assigned one of these addresses to each PC, you can choose classical routing. Or, you can use classical routing for routing private IP addresses within a campus environment.

To view the status of the WAN ports, you can view the Router Status screen (see *View the System Status* on page 439).

⚠ **WARNING!**

Changing the WAN mode from NAT to classical routing causes all LAN WAN and DMZ WAN inbound rules to revert to default settings.

➢ **To configure classical routing:**

1. Select **Network Config > WAN Settings > WAN Mode**. The WAN Mode screen displays (see *Figure 43* on page 79).

2. In the NAT (Network Address Translation) section of the screen, select the **Classical Routing** radio button.

3. Click **Apply** to save your settings.

Configure Auto-Rollover Mode and the Failure Detection Method (Multiple WAN Port Models)

To use a redundant ISP link for backup purposes, ensure that the backup WAN interface has already been configured. Then select the WAN interface that should function as the primary link for this mode, and configure the WAN failure detection method on the WAN Mode screen to support auto-rollover.

When the UTM is configured in auto-rollover mode, it uses the selected WAN failure detection method to detect the status of the primary link connection at regular intervals. Link failure is detected in one of the following ways:

• DNS queries sent to a DNS server

• Ping request sent to an IP address

• None (no failure detection is performed)

From the primary WAN interface, DNS queries or ping requests are sent to the specified IP address. If replies are not received after a specified number of retries, the primary WAN interface is considered down, and a rollover to the backup WAN interface occurs. When the primary WAN interface comes back up, another rollover occurs from the backup WAN interface back to the primary WAN interface. The WAN failure detection method that you select applies only to the primary WAN interface, that is, it monitors the primary link only.

Configure Auto-Rollover Mode

➢ **To configure auto-rollover mode:**

1. Select **Network Config > WAN Settings > WAN Mode**. The WAN Mode screen displays:
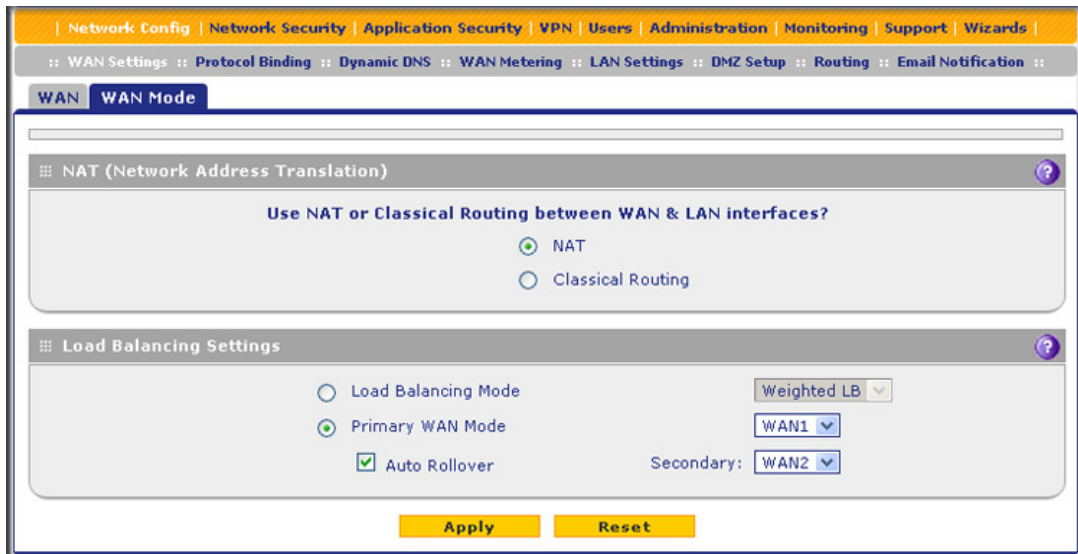
Figure 43.

2. In the Load Balancing Settings section of the screen, configure the following settings:

   a. Select the **Primary WAN Mode** radio button.

   b. From the corresponding drop-down list on the right, select a WAN interface to function as the primary WAN interface. The other WAN interface or interfaces become disabled.

   c. Select the **Auto Rollover** check box.

   d. From the corresponding drop-down list on the right, select a WAN interface to function as the backup WAN interface.

Note: Ensure that the backup WAN interface is configured before enabling auto-rollover mode.

---

3. Click **Apply** to save your settings.

Configure the Failure Detection Method

➢ **To configure the failure detection method:**

1. Select **Network Config > WAN Settings**. The WAN screen displays (see *Figure 36* on page 68).

2. Click the **Edit** button in the Action column of the WAN interface that you selected as the primary WAN interface. The WAN ISP Settings screen displays (see *Figure 37* on page 69, which shows the WAN1 ISP Settings screen as an example).

3. Click the **Advanced** option arrow at the upper right of the screen. The WAN Advanced Options screen displays for the WAN interface that you selected. (For an image of the entire screen, see *Figure 51* on page 90.)

4. Locate the Failure Detection Method section on the screen (see the following figure). Enter the settings as explained in the following table.
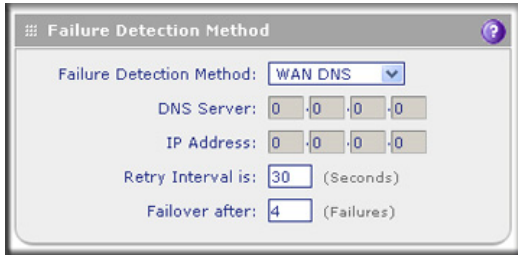
Figure 44.

Table 17. Failure detection method settings

Setting	Description	
WAN Failure Detection Method		
Select a failure detection method from the drop-down list. DNS queries or pings are sent through the WAN interface that is being monitored. The retry interval and number of failover attempts determine how quickly the UTM switches from the primary link to the backup link in case the primary link fails, or when the primary link comes back up, switches back from the backup link to the primary link.		
WAN DNS	DNS queries are sent to the DNS server that is configured in the Domain Name Server (DNS) Servers section of the WAN ISP screen (see *Manually Configure the Internet Connection* on page 71).	
Custom DNS	DNS queries are sent to the specified DNS server.	
	DNS Server	The IP address of the DNS server.
Ping	Pings are sent to a server with a public IP address. This server should not reject the ping request and should not consider ping traffic to be abusive.	
	IP Address	The IP address of the ping server.
Retry Interval is	The retry interval in seconds. The DNS query or ping is sent periodically after every test period. The default test period is 30 seconds.	
Failover after	The number of failover attempts. The primary WAN interface is considered down after the specified number of queries have failed to elicit a reply. The backup interface is brought up after this situation has occurred. The failover default is 4 failures.	

Note: The default time to roll over after the primary WAN interface fails is 2 minutes. The minimum test period is 30 seconds, and the minimum number of tests is 4.

5. Click **Apply** to save your settings.

Note: You can configure the UTM to generate a WAN status log and email this log to a specified address (see *Configure Logging, Alerts, and Event Notifications* on page 422).

Configure Load Balancing and Optional Protocol Binding

To use multiple ISP links simultaneously, configure load balancing. In load balancing mode, any WAN port carries any outbound protocol unless protocol binding is configured.

When a protocol is bound to a particular WAN port, all outgoing traffic of that protocol is directed to the bound WAN port. For example, if the HTTPS protocol is bound to the WAN1 port and the FTP protocol is bound to the WAN2 port, then the UTM automatically routes all outbound HTTPS traffic from the computers on the LAN through the WAN1 port. All outbound FTP traffic is routed through the WAN2 port.

Protocol binding addresses two issues:

- Segregation of traffic between links that are not of the same speed.
  High-volume traffic can be routed through the WAN port connected to a high-speed link, and low-volume traffic can be routed through the WAN port connected to the low-speed link.

- Continuity of source IP address for secure connections.
  Some services, particularly HTTPS, cease to respond when a client's source IP address changes shortly after a session has been established.

Configure Load Balancing (Multiple WAN Port Models)

➢ **To configure load balancing:**

1. Select **Network Config > WAN Settings > WAN Mode**. The WAN Mode screen displays:
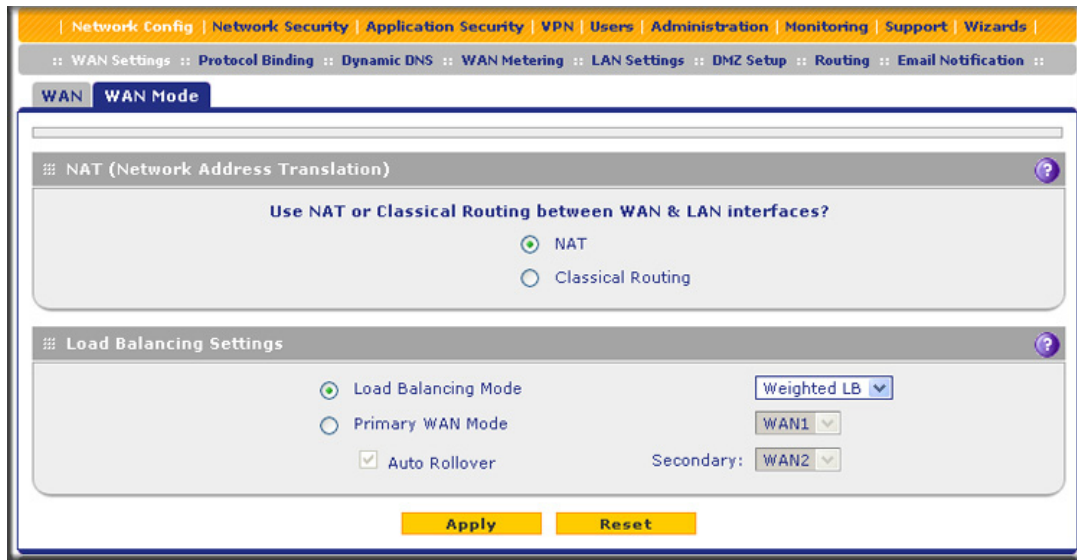
Figure 45.

> **Note:** You cannot configure load balancing when you use a PPPoE
> connection and have selected the Idle Timeout radio button on the
> WAN ISP Settings screen (single WAN port models) or on one of the
> WAN ISP Settings screens (multiple WAN port models); to use load
> balancing on a PPPoE connection, select the **Keep Connected**
> radio button. For more information, see *Figure 40* on page 72 and
> the accompanying PPPoE information in *Table 14* on page 73.

2. In the Load Balancing Settings section of the screen, configure the following settings:
   a. Select the **Load Balancing Mode** radio button.
   b. From the corresponding drop-down list on the right, select one of the following load balancing methods:
      • **Weighted LB**. With weighted load balancing, balance weights are calculated based on WAN link speed and available WAN bandwidth. This is the default setting and the most efficient load-balancing algorithm.
      • **Round-robin**. With round-robin load balancing, new traffic connections are sent over a WAN link in a serial method irrespective of bandwidth or link speed. For example on a UTM150, if the WAN1, WAN2, and WAN3 interfaces are active in round-robin load balancing mode, an HTTP request could first be sent over the WAN1 interface, then a new FTP session could start on the WAN2 interface, and then any new connection to the Internet could be made on the WAN3 interface. This load-balancing method ensures that a single WAN interface does not carry a disproportionate distribution of sessions.
3. Click **Apply** to save your settings.

Configure Protocol Binding (Optional)

➢ **To configure protocol binding and add protocol binding rules:**

1. Select **Network Config > Protocol Binding**. The Protocol Bindings screen displays. (The following figure shows two examples in the Protocol Bindings table.)
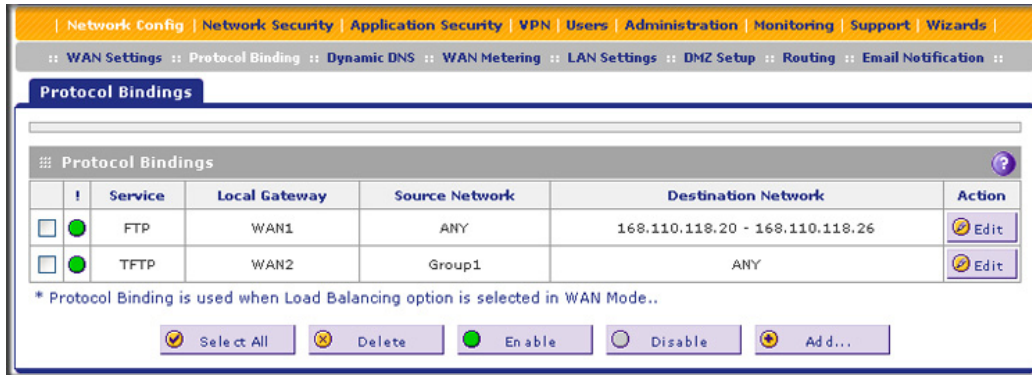
Figure 46.

The Protocol Bindings table displays the following fields:

- **Check box**. Allows you to select the protocol binding rule in the table.
- **Status icon**. Indicates the status of the protocol binding rule:
  - **Green circle**. The protocol binding rule is enabled.
  - **Gray circle**. The protocol binding rule is disabled.
- **Service**. The service or protocol for which the protocol binding rule is set up.
- **Local Gateway**. The WAN interface to which the service or protocol is bound.
- **Source Network**. The computers on your network that are affected by the protocol binding rule.
- **Destination Network**. The Internet locations (based on their IP address) that are covered by the protocol binding rule.
- **Action**. The Edit button provides access to the Edit Protocol Binding screen for the corresponding service.

2. Click the **Add** table button below the Protocol Bindings table. The Add Protocol Binding screen displays:

Figure 47.

3. Configure the protocol binding settings as explained in the following table:

Table 18. Add Protocol Binding screen settings

Setting	Description	
Service	From the drop-down list, select a service or application to be covered by this rule. If the service or application does not appear in the list, you need to define it using the Services screen (see *Service-Based Rules* on page 123).	
Local Gateway	From the drop-down list, select one of the WAN interfaces.	
Source Network	The source network settings determine which computers on your network are affected by this rule. Select one of the following options from the drop-down list:	
	Any	All devices on your LAN.
	Single address	In the Start IP field, enter the IP address to which the rule is applied.
	Address Range	In the Start IP field and End IP field, enter the IP addresses for the range to which the rule is applied.
	Group 1–Group 8	If this option is selected, the rule is applied to the devices that are assigned to the selected group. **Note:** You can also assign a customized name to a group (see *Change Group Names in the Network Database* on page 110).
Destination Network	The destination network settings determine which Internet locations (based on their IP address) are covered by the rule. Select one of the following options from the drop-down list:	
	Any	All Internet IP address.
	Single address	In the Start IP field, enter the IP address to which the rule is applied.
	Address range	In the Start IP field and End IP field, enter the IP addresses for the range to which the rule is applied.

4. Click **Apply** to save your settings. The protocol binding rule is added to the Protocol Bindings table. The rule is automatically enabled, which is indicated by the ! status icon, a green circle.

➢ **To edit a protocol binding:**

1. On the Protocol Bindings screen (see *Figure 46* on page 83), in the Protocol Bindings table, click the **Edit** table button to the right of the binding that you want to edit. The Edit Protocol Binding screen displays. This screen shows the same fields as the Add Protocol Binding screen (see the previous figure).

2. Modify the settings as explained in the previous table.

3. Click **Apply** to save your settings.

➢ **To enable, disable, or delete one or more protocol bindings:**

1. On the Protocol Bindings screen (see *Figure 46* on page 83), select the check box to the left of each protocol binding that you want to enable, disable, or delete, or click the **Select All** table button to select all bindings.

2. Click one of the following table buttons:
   - **Enable**. Enables the binding or bindings. The ! status icon changes from a gray circle to a green circle, indicating that the selected binding or bindings are enabled. (By default, when a binding is added to the table, it is automatically enabled.)
   - **Disable**. Disables the binding or bindings. The ! status icon changes from a green circle to a gray circle, indicating that the selected binding or bindings are disabled.
   - **Delete**. Deletes the binding or bindings.

Configure Secondary WAN Addresses

You can set up a single WAN port to be accessed through multiple IP addresses by adding aliases to the port. An alias is a secondary WAN address. One advantage is, for example, that you can assign different virtual IP addresses to a web server and an FTP server, even though both servers use the same physical IP address. You can add several secondary IP addresses to a single WAN port.

After you have configured secondary WAN addresses, these addresses are displayed on the following firewall rule screens:

- In the WAN Destination IP Address drop-down lists of the following inbound firewall rule screens:
  - Add LAN WAN Inbound Service screen
  - Add DMZ WAN Inbound Service screen

- In the NAT IP drop-down lists of the following outbound firewall rule screens:
  - Add LAN WAN Outbound Service screen
  - Add DMZ WAN Outbound Service screen

For more information about firewall rules, see *Use Rules to Block or Allow Specific Kinds of Traffic* on page 122).

It is important that you ensure that any secondary WAN addresses are different from the primary WAN, LAN, and DMZ IP addresses that are already configured on the UTM. However, primary and secondary WAN addresses can be in the same subnet. The following is an example of correctly configured IP addresses on a multiple WAN port model:

- Primary WAN1 IP address. 10.121.0.1 with subnet 255.255.255.0
- Secondary WAN1 IP address. 10.121.26.1 with subnet 255.255.255.0
- Primary WAN2 IP address. 10.216.75.1 with subnet 255.255.255.0
- Secondary WAN2 IP address. 10.216.82.1 with subnet 255.255.255.0
- DMZ IP address. 192.168.10.1 with subnet 255.255.255.0
- Primary LAN IP address. 192.168.1.1 with subnet 255.255.255.0
- Secondary LAN IP address. 192.168.2.1 with subnet 255.255.255.0

➢ **To add a secondary WAN address to a WAN interface:**

1. Select **Network Config > WAN Settings**. The WAN screen displays (see *Figure 36* on page 68).

2. Click the **Edit** button in the Action column of the WAN interface for which you want to add a secondary address. The WAN ISP Settings screen displays (see *Figure 36* on page 68, which shows the WAN1 ISP Settings screen as an example).

3. Click the **Secondary Addresses** option arrow at the upper right of the screen. The WAN Secondary Addresses screen displays for the WAN interface that you selected (see the following figure, which shows the WAN1 Secondary Addresses screen as an example, and which includes one entry in the List of Secondary WAN addresses table).
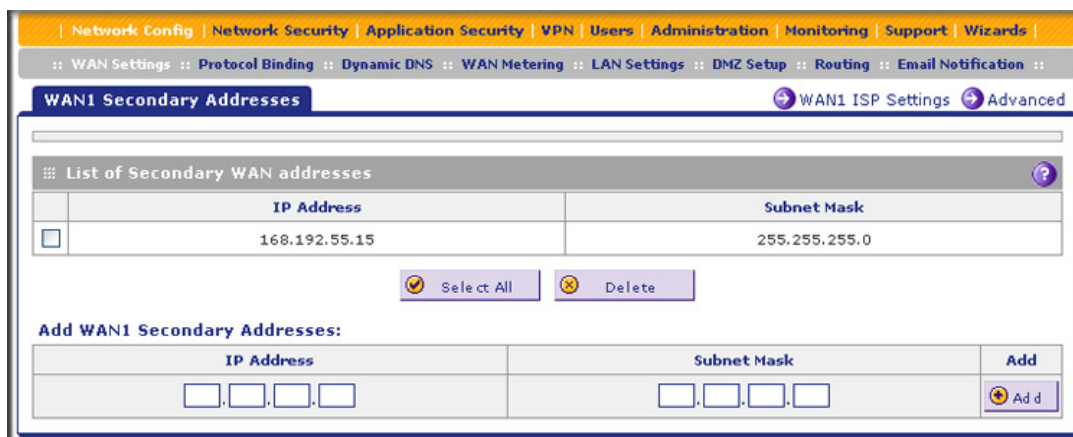
Figure 48.

The List of Secondary WAN addresses table displays the secondary LAN IP addresses added for the selected WAN interface.

4. In the Add WAN Secondary Addresses section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the WAN interface.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.

5. Click the **Add** table button in the rightmost column to add the secondary IP address to the List of Secondary WAN addresses table.

   Repeat *step 4* and *step 5* for each secondary IP address that you want to add to the List of Secondary WAN addresses table.

➢ **To delete one or more secondary addresses:**

1. In the List of Secondary WAN addresses table, select the check box to the left of each address that you want to delete, or click the **Select All** table button to select all addresses.

2. Click the **Delete** table button.

Configure Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows devices with varying public IP addresses to be located using Internet domain names. To use DDNS, you need to set up an account with a DDNS provider such as DynDNS.org, TZO.com, Oray.net, or 3322.org. (Links to DynDNS, TZO, Oray, and 3322 are provided for your convenience as option arrows on the DDNS configuration screens.) The UTM firmware includes software that notifies DDNS servers of changes in the WAN IP address, so that the services running on this network can be accessed by others on the Internet.

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently—hence, the need for a commercial DDNS service, which allows you to register an extension to its domain, and restores DNS requests for the resulting fully qualified domain name (FQDN) to your frequently changing IP address.

After you have configured your account information on the UTM, when your ISP-assigned IP address changes, your UTM automatically contacts your DDNS service provider, logs in to your account, and registers your new IP address.

Consider the following:

• For auto-rollover mode, you need an FQDN to implement features such as exposed hosts and virtual private networks regardless of whether you have a fixed or dynamic IP address.

• For load balancing mode, you might still need an FQDN either for convenience or if you have a dynamic IP address.

Note: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the DDNS service does not work because private addresses are not routed on the Internet.

➢ **To configure DDNS:**

1. Select **Network Config > Dynamic DNS**. The Dynamic DNS screen displays (see the following figure).

   The WAN Mode section on the screen reports the currently configured WAN mode (for example, Single Port WAN1, Load Balancing, or Auto Rollover). Only those options that match the configured WAN mode are accessible on the screen.

2. Click the submenu tab for your DDNS service provider:

   • **Dynamic DNS** for DynDNS.org (which is shown in the following figure)

   • **DNS TZO** for TZO.com

   • **DNS Oray** for Oray.net

   • **3322 DDNS** for 3322.org

Figure 49.

3. Click the **Information** option arrow in the upper right of a DNS screen for registration information.

Figure 50.

4. Access the website of the DDNS service provider, and register for an account (for example, for DynDNS.org, go to *http://www.dyndns.com/*).

5. Configure the DDNS service settings as explained in the following table:

Table 19. DNS service settings

Setting	Description	
WAN (Dynamic DNS Status: ...) **or** **WAN1 (Dynamic DNS Status: ...)**		
Change DNS to (DynDNS, TZO, Oray, or 3322)	Select the **Yes** radio button to enable the DDNS service. The fields that display on the screen depend on the DDNS service provider that you have selected. Enter the following settings:	
	Host and Domain Name	The host and domain name for the DDNS service.
	Username or User Email Address	The user name or email address for DDNS server authentication.
	Password or User Key	The password that is used for DDNS server authentication.
	Use wildcards	If your DDNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
	Update every 30 days	If your WAN IP address does not change often, you might need to force a periodic update to the DDNS service to prevent your account from expiring. If the **Update every 30 days** check box displays, select it to enable a periodic update.
WAN2 (Dynamic DNS Status: ...) or **WAN3 (Dynamic DNS Status: ...)** or **WAN4 (Dynamic DNS Status: ...)**		
See the information for WAN or WAN1 about how to enter the settings. You can select different DDNS services for different WAN interfaces.		

6. Click **Apply** to save your configuration.

Configure Advanced WAN Options

The advanced options include configuring the maximum transmission unit (MTU) size, the port speed, and the UTM's MAC address, and setting a rate limit on the traffic that is being forwarded by the UTM.

Note: You can also configure the failure detection method for the auto-rollover mode on the Advanced screen. This procedure is discussed in *Configure the Failure Detection Method* on page 79.

> **To configure advanced WAN options:**

1. Select **Network Config > WAN Settings**.
2. Click the **Edit** button in the Action column of the WAN interface for which you want to configure the advanced options. The WAN ISP Settings screen displays (see *Figure 37* on page 69, which shows the WAN1 ISP Settings screen of the UTM50 as an example).
3. Click the **Advanced** option arrow in the upper right of the screen. The WAN Advanced Options screen displays for the WAN interface that you selected. (The following figure shows the WAN1 Advanced Options screen of the UTM50 as an example.)

Figure 51.

4. Enter the settings as explained in the following table:

Table 20. Advanced WAN settings

Setting	Description
MTU Size Make one of the following selections:	
Default	Select the **Default** radio button for the normal maximum transmit unit (MTU) value. For most Ethernet networks this value is 1500 bytes, or 1492 bytes for PPPoE connections.
Custom	Select the **Custom** radio button, and enter an MTU value in the Bytes field. For some ISPs, you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
Speed	
In most cases, the UTM can automatically determine the connection speed of the WAN port of the device (modem or router) that provides the WAN connection. If you cannot establish an Internet connection, you might need to manually select the port speed. If you know the Ethernet port speed of the modem or router, select it from the drop-down list. Use the half-duplex settings only if the full-duplex settings do not function correctly. Select one of the following speeds from the drop-down list: • **AutoSense**. Speed autosensing. This is the default setting, This is the default setting, which can sense all Ethernet speeds and duplex modes, including 1000BASE-T speed at full duplex. • **10BaseT Half_Duplex**. Ethernet speed at half duplex. • **10BaseT Full_Duplex**. Ethernet speed at full duplex. • **100BaseT Half_Duplex**. Fast Ethernet speed at half duplex. • **100BaseT Full_Duplex**. Fast Ethernet speed at full duplex. • **1000BaseT Full_Duplex**. Gigabit Ethernet.	
Router's MAC Address Make one of the following selections:	
Use Default Address	Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. To use the UTM's own MAC address, select the **Use Default Address** radio button.
Use this computer's MAC Address	Select the **Use this computer's MAC Address** radio button to allow the UTM to use the MAC address of the computer you are now using to access the web management interface. This setting is useful if your ISP requires MAC authentication.
Use this MAC Address	Select the **Use this MAC Address** radio button, and manually enter the MAC address in the field next to the radio button. You would typically enter the MAC address that your ISP is requiring for MAC authentication. **Note:** The format for the MAC address is 01:23:45:67:89:AB (numbers 0–9 and either uppercase or lowercase letters A–F). If you enter a MAC address, the existing entry is overwritten.
Failure Detection Method See *Configure the Failure Detection Method* on page 79, including *Table 17* on page 80.	

Table 20. Advanced WAN settings (continued)

Setting	Description
Upload/Download Settings These settings rate-limit the traffic that is being forwarded by the UTM.	
WAN Connection Type	From the drop-down list, select the type of connection that the UTM uses to connect to the Internet: **DSL**, **ADLS**, **Cable Modem**, **T1**, **T3**, or **Other**.
WAN Connection Speed Upload	From the drop-down list, select the maximum upload speed that is provided by your ISP. You can select from **56 Kbps** to **1 Gbps**, or you can select **Custom** and enter the speed in Kbps in the field below the drop-down list.
WAN Connection Speed Download	From the drop-down list, select the maximum download speed that is provided by your ISP. You can select from **56 Kbps** to **1 Gbps**, or you can select **Custom** and enter the speed in Kbps in the field below the drop-down list.

5. Click **Apply** to save your changes.

> ⚠️ **WARNING!**
>
> **Depending on the changes that you made, when you click Apply, the UTM restarts, or services such as HTTP and SMTP might restart.**

If you want to configure the advanced settings for an additional WAN interface, select another WAN interface and repeat these steps.

Additional WAN-Related Configuration Tasks

- If you want the ability to manage the UTM remotely, enable remote management (see *Configure Remote Management Access* on page 399). If you enable remote management, NETGEAR strongly recommend that you change your password (see *Change Passwords and Administrator and Guest Settings* on page 397).

- You can set up the traffic meter for each WAN, if you wish. See *Enable the WAN Traffic Meter* on page 419.

LAN Configuration

4

This chapter describes how to configure the advanced LAN features of your UTM. This chapter contains the following sections:

- *Manage Virtual LANs and DHCP Options*
- *Configure Multihome LAN IPs on the Default VLAN*
- *Manage Groups and Hosts (LAN Groups)*
- *Configure and Enable the DMZ Port*
- *Manage Routing*

Note: The initial LAN configuration of the UTM's default VLAN 1 is described in *Chapter 2, Using the Setup Wizard to Provision the UTM in Your Network*.

Note: The Wireless Settings configuration menu is shown on the UTM9S only, accessible under the Network Config main navigation menu.

Note: On the UTM9S, the Email Notification configuration menu is accessible under the Monitoring main navigation menu instead of the Network Config main navigation menu.

Manage Virtual LANs and DHCP Options

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. Endpoints can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic needs to go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of PCs, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

VLANs have a number of advantages:

- It is easy to set up network segmentation. Users who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.

- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.

- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.

- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Port-Based VLANs

The UTM supports port-based VLANs. Port-based VLANs help to confine broadcast traffic to the LAN ports. Even though a LAN port can be a member of more than one VLAN, the port can have only one VLAN ID as its port VLAN identifier (PVID). By default, all four LAN ports of the UTM are assigned to the default VLAN, or VLAN 1. Therefore, by default, all four LAN ports have the default PVID 1. However, you can assign another PVID to a LAN port by selecting a VLAN profile from the drop-down list on the LAN Setup screen.

After you have created a VLAN profile and assigned one or more ports to the profile, you need to enable the profile to activate it.

The UTM's default VLAN cannot be deleted. All untagged traffic is routed through the default VLAN (VLAN1), which you need to assign to at least one LAN port.

Note the following about VLANs and PVIDs:

- One physical port is assigned to at least one VLAN.
- One physical port can be assigned to multiple VLANs.
- When one port is assigned to multiple VLANs, the port is used as a trunk port to connect to another switch or router.

- When a port receives an untagged packet, this packet is forwarded to a VLAN based on the PVID.
- When a port receives a tagged packet, this packet is forwarded to a VLAN based on the ID that is extracted from the tagged packet.

When you create a VLAN profile, assign LAN ports to the VLAN, and enable the VLAN, the LAN ports that are members of the VLAN can send and receive both tagged and untagged packets. Untagged packets that enter these LAN ports are assigned to the default PVID 1; packets that leave these LAN ports with the same default PVID 1 are untagged. All other packets are tagged according to the VLAN ID that you assigned to the VLAN when you created the VLAN profile.

This is a typical scenario for a configuration with an IP phone that has two Ethernet ports, one of which is connected to the UTM, the other one to another device:

Packets coming from the IP phone to the UTM LAN port are tagged. Packets passing through the IP phone from the connected device to the UTM LAN port are untagged. When you assign the UTM LAN port to a VLAN, packets entering and leaving the port are tagged with the VLAN ID. However, untagged packets entering the UTM LAN port are forwarded to the default VLAN with PVID 1; packets that leave the LAN port with the same default PVID 1 are untagged.

Note: The configuration of the DHCP options for the default VLAN are explained in *Chapter 2, Using the Setup Wizard to Provision the UTM in Your Network*. For information about how to add and edit a VLAN profile, including its DHCP options, see *Configure a VLAN Profile* on page 98.

Assign and Manage VLAN Profiles

➢ **To assign VLAN profiles to the LAN ports and manage VLAN profiles:**

1. Select **Network Config > LAN Settings**. The LAN submenu tabs display, with the LAN Setup screen in view. The following figure shows the LAN Setup screen for the UTM50 with six LAN ports, and the default VLAN profile and another VLAN profile as examples. Note that the screens for all other UTM models (not shown in this manual) have four LAN ports in the Default VLAN section.
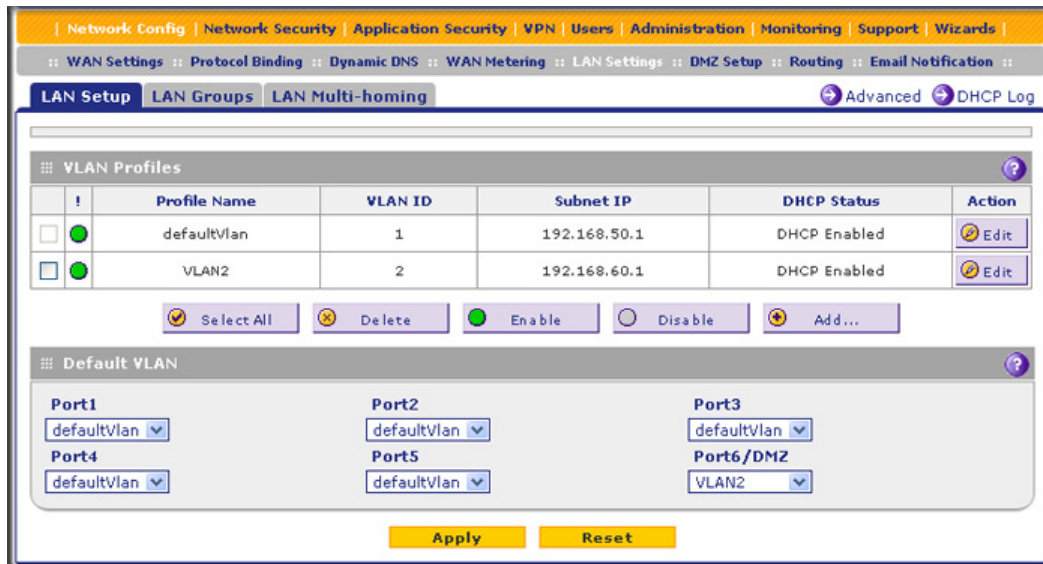
Figure 52.

For each VLAN profile, the following fields display in the VLAN Profiles table:

- **Check box**. Allows you to select the VLAN profile in the table.
- **Status icon**. Indicates the status of the VLAN profile:
    - **Green circle**. The VLAN profile is enabled.
    - **Gray circle**. The VLAN profile is disabled.
- **Profile Name**. The unique name assigned to the VLAN profile.
- **VLAN ID**. The unique ID (or tag) assigned to the VLAN profile.
- **Subnet IP**. The subnet IP address for the VLAN profile.
- **DHCP Status**. The DHCP server status for the VLAN profile, which can be either DHCP Enabled or DHCP Disabled.
- **Action**. The Edit table button, which provides access to the Edit VLAN Profile screen.

2. Assign a VLAN profile to a LAN port (For the UTM5, UTM10, UTM25, and UTM150: Port 1, Port 2, Port 3, or Port 4/DMZ; for the UTM50: Port 1, Port 2, Port 3, Port 4, Port 5, or Port 6/DMZ) by selecting a VLAN profile from the drop-down list. Both enabled and disabled VLAN profiles are displayed in the drop-down lists.

3. Click **Apply** to save your settings.

VLAN DHCP Options

For each VLAN, you need to specify the Dynamic Host Configuration Protocol (DHCP) options (see *Configure a VLAN Profile* on page 98). The configuration of the DHCP options for the UTM's default VLAN, or VLAN 1, is explained in *Chapter 3, Manually Configuring Internet and WAN Settings*. This section provides further information about the DHCP options.

DHCP Server

The default VLAN (VLAN 1) has the DHCP server option enabled by default, allowing the UTM to assign IP, DNS server, WINS server, and default gateway addresses to all computers connected to the UTM's LAN. The assigned default gateway address is the LAN address of the UTM. IP addresses are assigned to the attached computers from a pool of addresses that you need to specify. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. When you create a new VLAN, the DHCP server option is disabled by default.

For most applications, the default DHCP server and TCP/IP settings of the UTM are satisfactory.

The UTM delivers the following settings to any LAN device that requests DHCP:

- An IP address from the range that you have defined
- Subnet mask
- Gateway IP address (the UTM's LAN IP address)
- Primary DNS server (the UTM's LAN IP address)
- WINS server (if you entered a WINS server address in the DHCP Setup screen)
- Lease time (the date obtained and the duration of the lease).

DHCP Relay

DHCP relay options allow you to make the UTM a DHCP relay agent for a VLAN. The DHCP relay agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP relay agent is therefore the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet. If you do not configure a DHCP relay agent for a VLAN, its clients can obtain IP addresses only from a DHCP server that is on the same subnet. To enable clients to obtain IP addresses from a DHCP server on a remote subnet, you need to configure the DHCP relay agent on the subnet that contains the remote clients, so that the DHCP relay agent can relay DHCP broadcast messages to your DHCP server.

DNS Proxy

When the DNS proxy option is enabled for a VLAN, the UTM acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (as configured on the WAN ISP Settings screens). All DHCP clients receive the primary and secondary DNS IP addresses along with the IP address where the DNS proxy is located (that is, the UTM's LAN IP address). When the DNS proxy option is disabled for a VLAN, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address. A DNS proxy is particularly useful in auto-rollover mode. For example, if the DNS servers for each WAN connection are different servers, then a link failure might render the DNS servers inaccessible. However, when the DNS proxy option is enabled, the DHCP clients can make requests to the UTM, which, in turn, can send those requests to the DNS servers of the active WAN connection. However, disable the DNS proxy if you are using a multiple WAN

configuration in auto-rollover mode with route diversity (that is, with two different ISPs) and you cannot ensure that the DNS server is available after a rollover has occurred.

LDAP Server

A Lightweight Directory Access Protocol (LDAP) server allows a user to query and modify directory services that run over TCP/IP. For example, clients can query email addresses, contact information, and other service information using an LDAP server. For each VLAN, you can specify an LDAP server and a search base that defines the location in the directory (that is, the directory tree) from which the LDAP search begins.

Configure a VLAN Profile

For each VLAN on the UTM, you can configure its profile, port membership, LAN TCP/IP settings, DHCP options, DNS server, and inter-VLAN routing capability.

The preconfigured default VLAN is called defaultVLAN. A UTM9S in which a wireless module is installed also has a default WLAN with the name defaultWLAN.

➢ **To add or edit a VLAN profile:**

1. Select **Network Config > LAN Settings**. The LAN submenu tabs display, with the LAN Setup screen in view. The following figure shows the LAN Setup screen for the UTM50 with six LAN ports, and the default VLAN profile and another VLAN profile as examples. Note that the screens for all other UTM models (not shown in this manual) have four LAN ports in the Default VLAN section.

> **Note:** For information about how to manage VLANs, see *Port-Based VLANs* on page 94. The following information describes how to configure a VLAN profile.
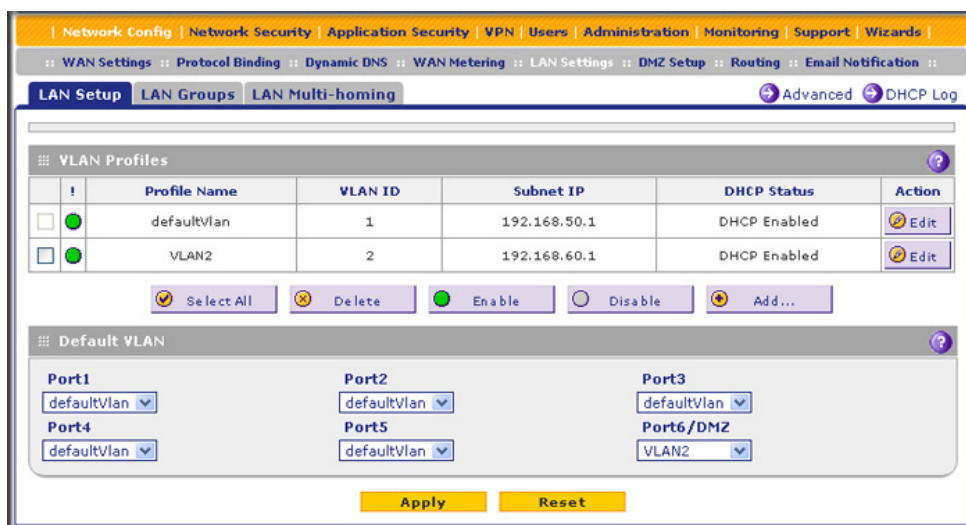
Figure 53.

2. Either select an entry from the VLAN Profiles table and click the corresponding **Edit** table button, or add a new VLAN profile by clicking the **Add** table button under the VLAN Profiles table. The Edit VLAN Profile screen displays. The following figure shows the Edit VLAN Profile screen for the UTM with four ports in the Port Membership section. Note that the Edit VLAN Profile screens for the UTM50 (not shown in this manual) has six ports in the Port Membership section.

Figure 54.

3. Enter the settings as explained in the following table:

Table 21. Edit VLAN Profile screen settings

Setting	Description
VLAN Profile	
Profile Name	Enter a unique name for the VLAN profile. **Note:** You can also change the profile name of the default VLAN.
VLAN ID	Enter a unique ID number for the VLAN profile. No two VLANs can have the same VLAN ID number. **Note:** You can enter VLAN IDs from 2 to 4093. VLAN ID 1 is reserved for the default VLAN; VLAN ID 4094 is reserved for the DMZ interface.
Port Membership	
UTM5, UTM9S, UTM10, UTM25, and UTM150: Port 1, Port 2, Port 3, and Port 4 / DMZ	Select one, several, or all port check boxes to make the ports members of this VLAN.
UTM50: Port 1, Port 2, Port 3, Port 4, Port 5, and Port 6 / DMZ	**Note:** A port that is defined as a member of a VLAN profile can send and receive data frames that are tagged with the VLAN ID.
LAN TCP/IP Setup	
IP Address	Enter the IP address of the UTM (the factory default address is 192.168.1.1). **Note:** Always make sure that the LAN port IP address and DMZ port IP address are in different subnets. **Note:** If you change the LAN IP address of the VLAN while being connected through the browser to the VLAN, you are disconnected. You then need to open a new connection to the new IP address and log in again. For example, if you change the default IP address 192.168.1.1 to 10.0.0.1, you now need to enter **https://10.0.0.1** in your browser to reconnect to the web management interface.
Subnet Mask	Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Based on the IP address that you assign, the UTM automatically calculates the subnet mask. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the UTM).
DHCP	
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you will manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. By default, this radio button is not selected, and the DHCP server is enabled.

Table 21. Edit VLAN Profile screen settings (continued)

Setting	Description		
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the UTM to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the VLAN. Enter the following settings:		
	Domain Name	This setting is optional. Enter the domain name of the UTM.	
	Starting IP Address	Enter the starting IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the ending IP address. The IP address 192.168.1.2 is the default starting address.	
	Ending IP Address	Enter the ending IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address. **Note:** The starting and ending DHCP IP addresses should be in the same *network* as the LAN TCP/IP address of the UTM (that is, the IP address in the LAN TCP/IP Setup section as described earlier in this table).	
	Primary DNS Server	This setting is optional. If an IP address is specified, the UTM provides this address as the primary DNS server IP address. If no address is specified, the UTM uses the VLAN IP address as the primary DNS server IP address.	
	Secondary DNS Server	This setting is optional. If an IP address is specified, the UTM provides this address as the secondary DNS server IP address.	
	WINS Server	This setting is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.	
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.	
DHCP Relay	To use the UTM as a DHCP relay agent for a DHCP server somewhere else in your network, select the **DHCP Relay** radio button. Enter the following setting:		
	Relay Gateway	The IP address of the DHCP server for which the UTM serves as a relay.	

Table 21. Edit VLAN Profile screen settings (continued)

Setting	Description	
Enable LDAP information	To enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information, select the **Enable LDAP information** check box. Enter the following settings. **Note:** The LDAP settings that you specify as part of the VLAN profile are used only for SSL VPN and UTM authentication, but not for web and email security.	
	LDAP Server	The IP address or name of the LDAP server.
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begins. You can specify multiple search objects, separated by commas. The search objects include: • CN (for common name) • OU (for organizational unit) • O (for organization) • C (for country) • DC (for domain) For example, to search the Netgear.net domain for all last names of Johnson, you would enter: cn=Johnson,dc=Netgear,dc=net
	Port	The port number for the LDAP server. The default setting is 0 (zero).
DNS Proxy		
Enable DNS Proxy	This setting is optional. To enable the UTM to provide a LAN IP address for DNS address name resolution, select the **Enable DNS Proxy** check box. This setting is disabled by default. **Note:** When the DNS proxy option is disabled for a VLAN, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address.	
Inter VLAN Routing		
Enable Inter VLAN Routing	This setting is optional. To ensure that traffic is routed only to VLANs for which inter-VLAN routing is enabled, select the **Enable Inter VLAN Routing** check box. This setting is disabled by default. When the Enable Inter VLAN Routing check box is not selected, traffic from this VLAN is not routed to other VLANs, and traffic from other VLANs is not routed to this VLAN. **Note:** For information about inter-VLAN firewall rules, see *VLAN Rules* on page 144.	

4. Click **Apply** to save your settings.

Note: When you have completed the LAN setup, all outbound traffic is
allowed and all inbound traffic is discarded except responses to
requests from the LAN side. For information about how to change
these default traffic rules, see *Chapter 5, Firewall Protection*.

➢ To edit a VLAN profile:

1. On the LAN Setup screen (see *Figure 53* on page 98), click the **Edit** button in the Action
   column for the VLAN profile that you want to modify. The Edit VLAN Profile screen
   displays (see the previous screen).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ To enable, disable, or delete one or more VLAN profiles:

1. On the LAN Setup screen (see *Figure 53* on page 98), select the check box to the left of
   each VLAN profile that you want to enable, disable, or delete, or click the **Select All**
   table button to select all profiles. (You cannot select the default VLAN profile.)
2. Click one of the following table buttons:
   - **Enable**. Enables the VLAN or VLANs. The ! status icon changes from a gray circle to
     a green circle, indicating that the selected VLAN or VLANs are enabled. (By default,
     when a VLAN is added to the table, it is automatically enabled.)
   - **Disable**. Disables the VLAN or VLANs. The ! status icon changes from a green circle
     to a gray circle, indicating that the selected VLAN or VLANs are disabled.
   - **Delete**. Deletes the VLAN or VLANs.

Configure VLAN MAC Addresses and Advanced LAN Settings

By default, all configured VLAN profiles share the same single MAC address as the LAN
ports. (All LAN ports share the same MAC address.) However, you can change the VLAN
MAC settings to allow up to 16 VLANs to each be assigned a unique MAC address.

You can also enable or disable the broadcast of Address Resolution Protocol (ARP) packets
for the default VLAN. If the broadcast of ARP packets is enabled, IP addresses can be
mapped to physical addresses (that is, MAC addresses).

➢ To configure a VLAN to have a unique MAC address:

1. Select **Network Config > LAN Settings**. The LAN submenu tabs display, with the LAN
   Setup screen in view (see *Figure 53* on page 98).
2. Click the **Advanced** option arrow in the upper right of the LAN Setup screen. The LAN
   Advanced screen displays:
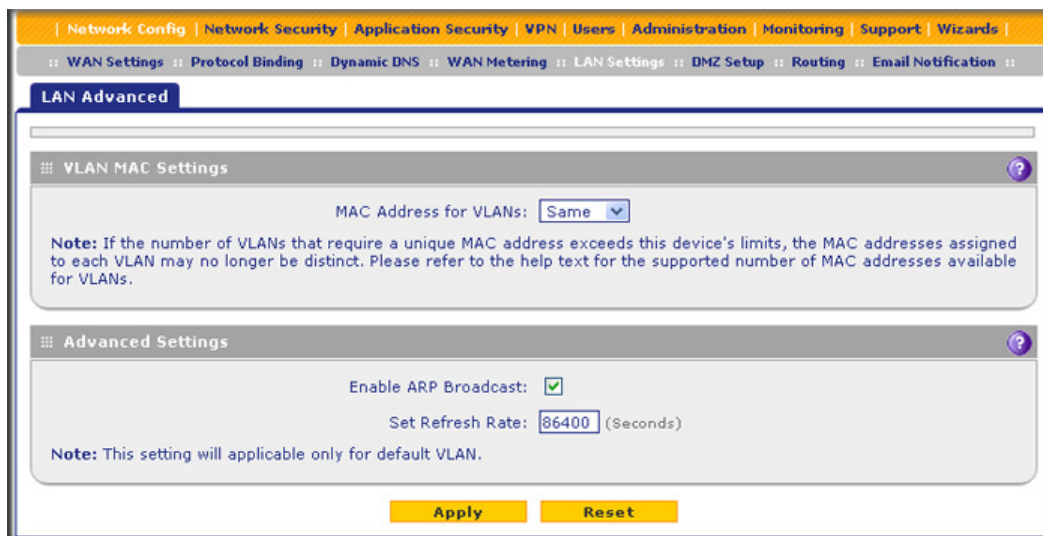
Figure 55.

3. From the MAC Address for VLANs drop-down list, select **Unique**. (The default is Same.)

4. As an option, you can disable the broadcast of ARP packets for the default VLAN by clearing the **Enable ARP Broadcast** check box. (The broadcast of ARP packets is enabled by default for the default VLAN.) If you choose to keep the broadcast of ARP enabled, you can enter an ARP refresh rate in the Set Refresh Rate field. The default setting is 180 seconds. The maximum ARP refresh rate is 86400 seconds (24 hours).

5. Click **Apply** to save your settings.

Note: If you attempt to configure more than 16 VLANs while the MAC address for VLANs is set to Unique on the LAN Advanced screen, the MAC addresses that are assigned to each VLAN might no longer be distinct.

Configure Multihome LAN IPs on the Default VLAN

If you have computers using different IP networks in the LAN, (for example, 172.16.2.0 or 10.0.0.0), you can add aliases to the LAN ports and give computers on those networks access to the Internet, but you can do so only for the default VLAN. The IP address that is assigned as a secondary IP address needs to be unique and cannot be assigned to the VLAN.

It is important that you ensure that any secondary LAN addresses are different from the primary LAN, WAN, and DMZ IP addresses and subnet addresses that are already configured on the UTM.

The following is an example of correctly configured IP addresses on a multiple WAN port model:

- WAN1 IP address. 10.0.0.1 with subnet 255.0.0.0
- WAN2 IP address. 20.0.0.1 with subnet 255.0.0.0
- DMZ IP address. 192.168.10.1 with subnet 255.255.255.0
- Primary LAN IP address. 192.168.1.1 with subnet 255.255.255.0
- Secondary LAN IP address. 192.168.20.1 with subnet 255.255.255.0

➢ **To add a secondary LAN IP address:**

1. Select **Network Config > LAN Settings > LAN Multi-homing**. The LAN Multi-homing screen displays:
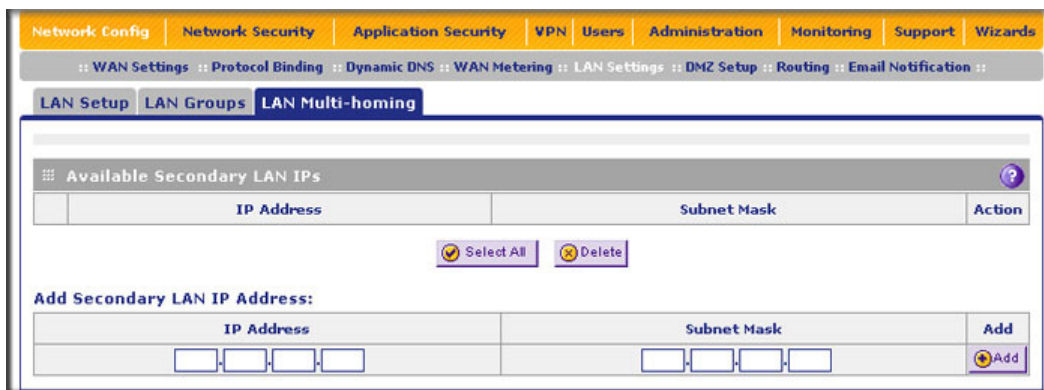
Figure 56.

The Available Secondary LAN IPs table displays the secondary LAN IP addresses added to the UTM.

2. In the Add Secondary LAN IP Address section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the LAN ports.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.

3. Click the **Add** table button in the rightmost column to add the secondary IP address to the Available Secondary LAN IPs table.

   Repeat *step 2* and *step 3* for each secondary IP address that you want to add to the Available Secondary LAN IPs table.

Note: Secondary IP addresses cannot be configured in the DHCP server. The hosts on the secondary subnets need to be manually configured with the IP addresses, gateway IP address, and DNS server IP addresses.

> ➤ **To edit a secondary LAN IP address:**

1. On the LAN Multi-homing screen (see the previous screen), click the **Edit** button in the Action column for the secondary IP address that you want to modify. The Edit Secondary LAN IP address screen displays.

2. Modify the IP address or subnet mask, or both.

3. Click **Apply** to save your settings.

> ➤ **To delete one or more secondary LAN IP addresses:**

1. On the LAN Multi-homing screen (see the previous screen), select the check box to the left of each secondary IP address that you want to delete, or click the **Select All** table button to select secondary IP addresses.

2. Click the **Delete** table button.

Manage Groups and Hosts (LAN Groups)

The Known PCs and Devices table on the LAN Groups screen (see *Figure 57* on page 108) contains a list of all known PCs and network devices that are assigned dynamic IP addresses by the UTM, or have been discovered by other means. Collectively, these entries make up the network database.

The network database is updated by these methods:

- **DHCP client requests**. When the DHCP server is enabled, it accepts and responds to DHCP client requests from PCs and other network devices. These requests also generate an entry in the network database. This is an advantage of enabling the DHCP server feature.

- **Scanning the network**. The local network is scanned using Address Resolution Protocol (ARP) requests. The ARP scan detects active devices that are not DHCP clients.

Note: In large networks, scanning the network might generate unwanted traffic.

Note: When the UTM receives a reply to an ARP request, it might not be able to determine the device name if the software firewall of the device blocks the name.

- **Manual entry**. You can manually enter information about a network device.

These are some advantages of the network database:

- Generally, you do not need to enter an IP address or a MAC address. Instead, you can just select the name of the desired PC or device.

- There is no need to reserve an IP address for a PC in the DHCP server. All IP address assignments made by the DHCP server are maintained until the PC or device is removed from the network database, either by expiration (inactive for a long time) or by you.

- There is no need to use a fixed IP address on a PC. Because the IP address allocated by the DHCP server never changes, you do not need to assign a fixed IP address to a PC to ensure that it always has the same IP address.

- A PC is identified by its MAC address—not its IP address. The network database uses the MAC address to identify each PC or device. Therefore, changing a PC's IP address does not affect any restrictions applied to that PC.

- Control over PCs can be assigned to groups and individuals:
  - You can assign PCs to groups (see *Manage the Network Database* on this page) and apply restrictions (outbound rules and inbound rules) to each group (see *Use Rules to Block or Allow Specific Kinds of Traffic* on page 122).
  - You can select groups that are allowed access to applications, web categories, and URLs that you have blocked for all other users, or the other way around, block access to applications, web categories, and URLs that you have allowed access to for all other users (see *Set Web Access Exception Rules* on page 221).
  - If necessary, you can also create firewall rules to apply to a single PC (see *Enable Source MAC Filtering* on page 164). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.

Manage the Network Database

You can view the network database, manually add or remove database entries, and edit database entries.

To view the network database, select **Network Config > LAN Settings > LAN Groups**. The LAN Groups screen displays. (The following figure shows some examples in the Known PCs and Devices table.)

Figure 57.

The Known PCs and Devices table lists the entries in the network database. For each PC or device, the following fields display:

- **Check box**. Allows you to select the PC or device in the table.
- **Name**. The name of the PC or device. For computers that do not support the NetBIOS protocol, the name is displayed as *Unknown* (you can edit the entry manually to add a meaningful name). If the PC or device was assigned an IP address by the DHCP server, then the name is appended by an asterisk.
- **IP Address**. The current IP address of the PC or device. For DHCP clients of the UTM, this IP address does not change. If a PC or device is assigned a static IP address, you need to update this entry manually after the IP address on the PC or device has changed.
- **MAC Address**. The MAC address of the PC or device's network interface.
- **Group**. Each PC or device can be assigned to a single LAN group. By default, a PC or device is assigned to Group 1. You can select a different LAN group from the Group drop-down list in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen.
- **Profile Name**. The VLAN to which the PC or device is assigned.
- **Action**. The Edit table button, which provides access to the Edit Groups and Hosts screen.

Add PCs or Devices to the Network Database

➢ **To add PCs or devices manually to the network database:**

1. In the Add Known PCs and Devices section of the LAN Groups screen (see the previous figure), enter the settings as explained in the following table:

Table 22. Known PCs and devices settings

Setting	Description
Name	Enter the name of the PC or device.
IP Address Type	From the drop-down list, select how the PC or device receives its IP address: • **Fixed (set on PC)**. The IP address is statically assigned on the PC or device. • **Reserved (DHCP Client)**. Directs the UTM's DHCP server to always assign the specified IP address to this client during the DHCP negotiation (see *Set Up Address Reservation* on page 111). **Note:** When you assign a reserved IP address to a client, the selected IP address needs to be outside the range of addresses allocated to the DHCP server pool.
IP Address	In the IP Address field, enter the IP address that this PC or device is assigned. If the IP address type is Reserved (DHCP Client), the UTM reserves the IP address for the associated MAC address.
MAC Address	Enter the MAC address of the PC's or device's network interface. The MAC address format is six colon-separated pairs of hexadecimal characters (0–9 and A–F), such as 01:23:45:67:89:AB.
Group	From the drop-down list, select the group to which the PC or device is assigned. (Group 1 is the default group.)
Profile Name	From the drop-down list, select the VLAN profile to which the PC or device is assigned. (defaultVlan is the default VLAN group.)

2. Click the **Add** table button to add the PC or device to the Known PCs and Devices table.

3. As an optional step: To enable DHCP address reservation for the entry that you just added to the Known PCs and Devices table, select the check box for the table entry, and click the **Save Binding** button to bind the IP address to the MAC address for DHCP assignment.

Edit PCs or Devices in the Network Database

➢ **To edit PCs or devices manually in the network database:**

1. In the Known PCs and Devices table of the LAN Groups screen (see the previous figure), click the **Edit** table button of a table entry. The Edit Groups and Hosts screen displays (see the following figure, which contains an example).
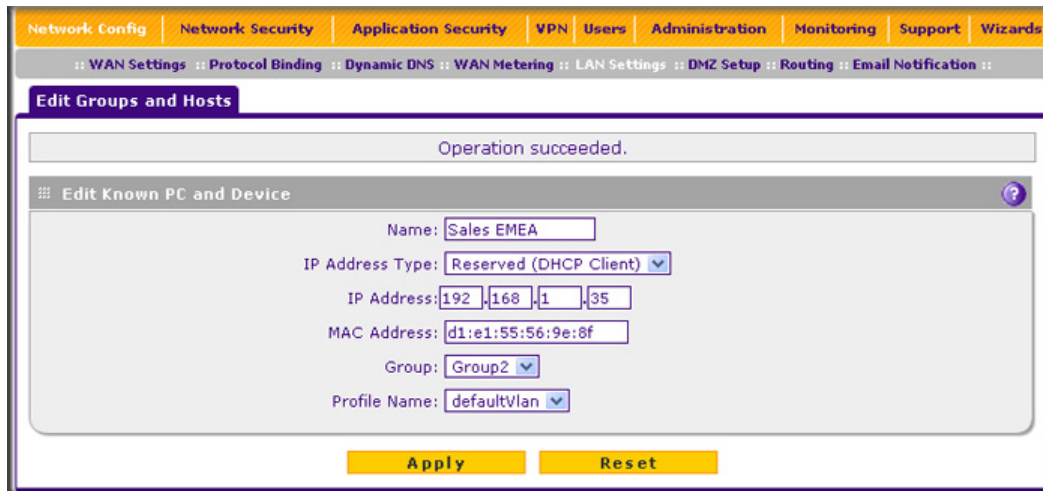
Figure 58.

2. Modify the settings as explained in *Table 22* on page 109.
3. Click **Apply** to save your settings in the Known PCs and Devices table.

Deleting PCs or Devices from the Network Database

➢ **To delete one or more PCs or devices from the network database:**

1. On the LAN Groups screen (see *Figure 57* on page 108), select the check box to the left of each PC or device that you want to delete, or click the **Select All** table button to select all PCs and devices.
2. Click the **Delete** table button.

Change Group Names in the Network Database

By default, the groups are named Group1 through Group8. You can rename these group names to be more descriptive, such as GlobalMarketing and GlobalSales.

➢ **To edit the names of any of the eight available groups:**

1. Select **Network Config > LAN Setting > LAN Groups**. The LAN Groups screen displays (see *Figure 57* on page 108, which shows some examples in the Known PCs and Devices table).
2. Click the **Edit Group Names** option arrow to the right of the LAN submenu tabs. The Network Database Group Names screen displays. (The following figure shows some examples.)
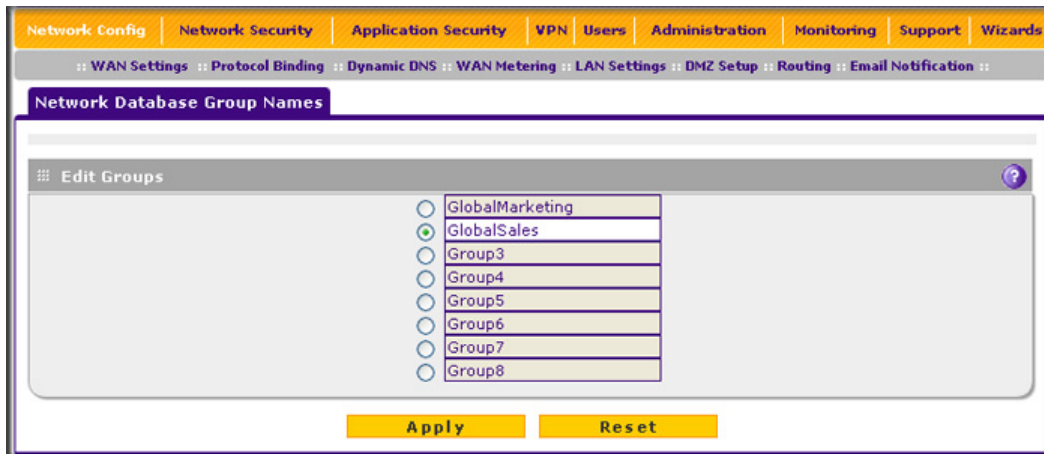
Figure 59.

3. Select the radio button next to the group name that you want to edit.

4. Type a new name in the field. The maximum number of characters is 15; spaces and double quotes (") are not allowed.

5. Repeat *step 3* and *step 4* for any other group names.

6. Click **Apply** to save your settings.

Set Up Address Reservation

When you specify a reserved IP address for a PC or device on the LAN (based on the MAC address of the device), that PC or device always receives the same IP address each time it accesses the UTM's DHCP server. Reserved IP addresses should be assigned to servers or access points that require permanent IP address settings. The reserved IP address that you select needs to be outside of the DHCP server pool.

To reserve an IP address, select **Reserved (DHCP Client)** from the IP Address Type drop-down list on the LAN Groups screen as described in *Add PCs or Devices to the Network Database* on page 109 or on the Edit Groups and Hosts screen as described in *Edit PCs or Devices in the Network Database* on page 109.

> **Note:** The reserved address is not assigned until the next time the PC or device contacts the UTM's DHCP server. Reboot the PC or device, or access its IP configuration and force a DHCP release and renew.

Configure and Enable the DMZ Port

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions than the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. The rightmost LAN port on the UTM can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN. On the UTM5, UTM10, UTM25, and UTM150, this is LAN port 4; on the UTM50, this is LAN port 6.

By default, the DMZ port and both inbound and outbound DMZ traffic are disabled. Enabling the DMZ port and allowing traffic to and from the DMZ increases the traffic through the WAN ports.

Using a DMZ port is also helpful with online games and videoconferencing applications that are incompatible with NAT. The UTM is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, local PCs can run the application correctly if those PCs are used on the DMZ port.

> **Note:** A separate firewall security profile is provided for the DMZ port that is also physically independent of the standard firewall security component that is used for the LAN.

The DMZ Setup screen lets you set up the DMZ port. It permits you to enable or disable the hardware DMZ port (LAN port 4 or LAN port 6; see *Front Panel UTM5 and UTM10* on page 22) and configure an IP address and subnet mask for the DMZ port.

➢ **To enable and configure the DMZ port:**

1. Select **Network Config > DMZ Setup**. The DMZ Setup screen displays:
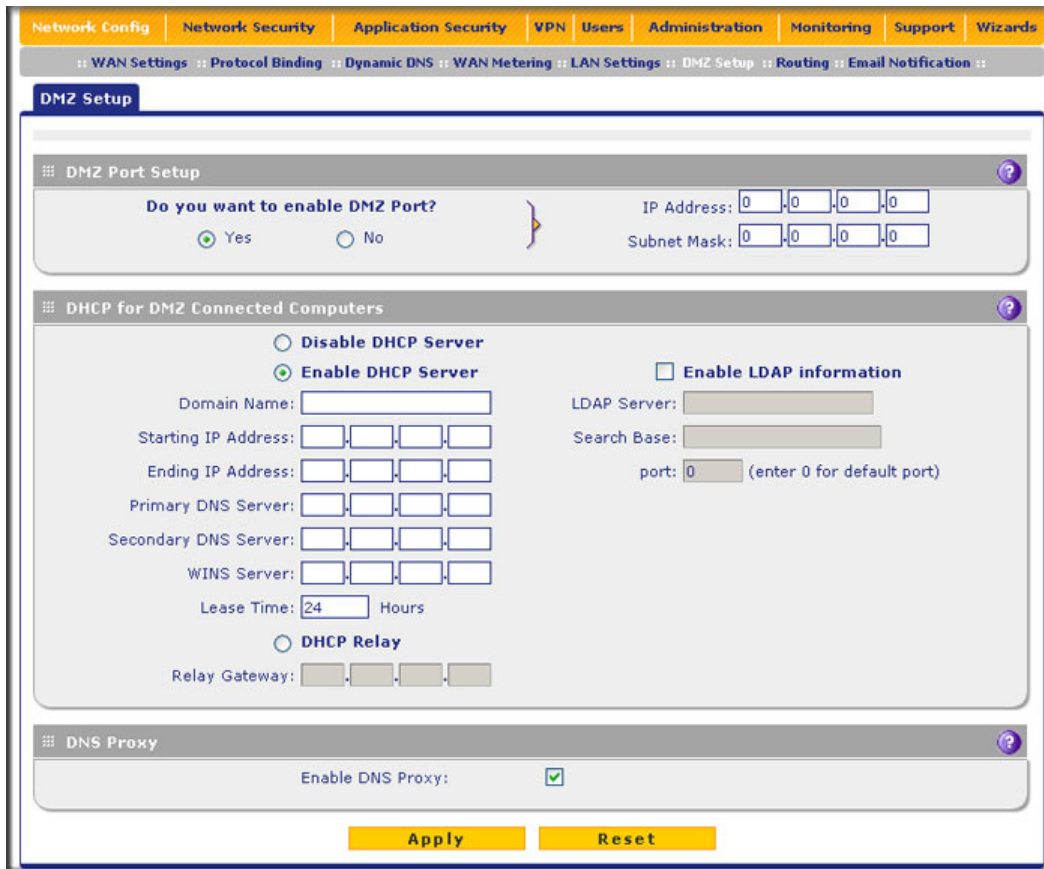
Figure 60.

2. Enter the settings as explained in the following table:

Table 23. DMZ Setup screen settings

Setting	Description		
DMZ Port Setup			
Do you want to enable DMZ Port?	Select one of the following radio buttons: • **Yes**. Enables you to configure the DMZ port settings. Fill in the IP Address and Subnet Mask fields. • **No**. Allows you to disable the DMZ port after you have configured it.		
	IP Address	Enter the IP address of the DMZ port. Make sure that the DMZ port IP address and LAN port IP address are in different subnets (for example, an address outside the LAN address pool, such as 192.168.1.101).	
	Subnet Mask	Enter the IP subnet mask of the DMZ port. The subnet mask specifies the network number portion of an IP address.	

Table 23. DMZ Setup screen settings (continued)

Setting	Description
DHCP	
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you will manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. By default, this radio button is not selected, and the DHCP server is enabled.
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the UTM to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the VLAN. Enter the following settings:
	Domain Name / This setting is optional. Enter the domain name of the UTM.
	Starting IP Address / Enter the starting IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the ending IP address. The IP address 192.168.1.2 is the default start address.
	Ending IP Address / Enter the ending IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address. **Note:** The starting and ending DHCP IP addresses should be in the same network as the LAN TCP/IP address of the UTM (that is, the IP address in the DMZ Port Setup section as described earlier in this table).
	Primary DNS Server / This setting is optional. If an IP address is specified, the UTM provides this address as the primary DNS server IP address. If no address is specified, the UTM provides its own LAN IP address as the primary DNS server IP address.
	Secondary DNS Server / This setting is optional. If an IP address is specified, the UTM provides this address as the secondary DNS server IP address.
	WINS Server / This setting is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.
	Lease Time / Enter a lease time. This specifies the duration for which IP addresses are leased to clients.
DHCP Relay	To use the UTM as a DHCP relay agent for a DHCP server somewhere else in your network, select the **DHCP Relay** radio button. Enter the following setting:
	Relay Gateway / The IP address of the DHCP server for which the UTM serves as a relay.

Table 23. DMZ Setup screen settings (continued)

Setting	Description	
Enable LDAP information	To enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information, select the **Enable LDAP information** check box. Enter the following settings:	
	LDAP Server	The IP address or name of the LDAP server.
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begins. You can specify multiple search objects, separated by commas. The search objects include: • CN (for common name) • OU (for organizational unit) • O (for organization) • C (for country) • DC (for domain) For example, to search the Netgear.net domain for all last names of Johnson, you would enter: cn=Johnson,dc=Netgear,dc=net
	Port	The port number for the LDAP server. The default setting is 0 (zero).
DNS Proxy		
Enable DNS Proxy	This setting is optional. To enable the UTM to provide a LAN IP address for DNS address name resolution, select the **Enable DNS Proxy** check box. This check box is selected by default. **Note:** When the DNS Proxy option is disabled, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address.	

3. Click **Apply** to save your settings.

Note: For all UTM models with the exception of the UTM50, the DMZ LED next to LAN port 4 (see *Hardware Features* on page 22) lights green to indicate that the DMZ port is enabled. For the UTM50, the DMZ LED next to LAN port 6 lights green to indicate that the DMZ port is enabled.

For information about how to define the DMZ WAN rules and LAN DMZ rules, see *Set DMZ WAN Rules* on page 133 and *Set LAN DMZ Rules* on page 136, respectively.

Manage Routing

Static routes provide additional routing information to your UTM. Under normal circumstances, the UTM has adequate routing information after it has been configured for

Internet access, and you do not need to configure additional static routes. You should configure static routes only for unusual cases such as multiple firewalls or multiple IP subnets located on your network.

Note: The UTM automatically sets up routes between VLANs and secondary IP addresses that you have configured on the LAN Multi-homing screen (see *Configure Multihome LAN IPs on the Default VLAN* on page 104). Therefore, you do not need to manually add a static route between a VLAN and a secondary IP address.

Configure Static Routes

➢ **To add a static route to the Static Route table:**

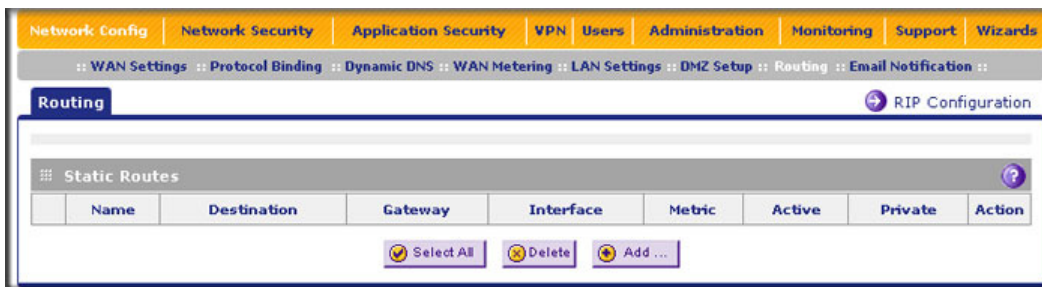1. Select **Network Config > Routing**. The Routing screen displays:

Figure 61.

2. Click the **Add** table button under the Static Routes table. The Add Static Route screen displays:
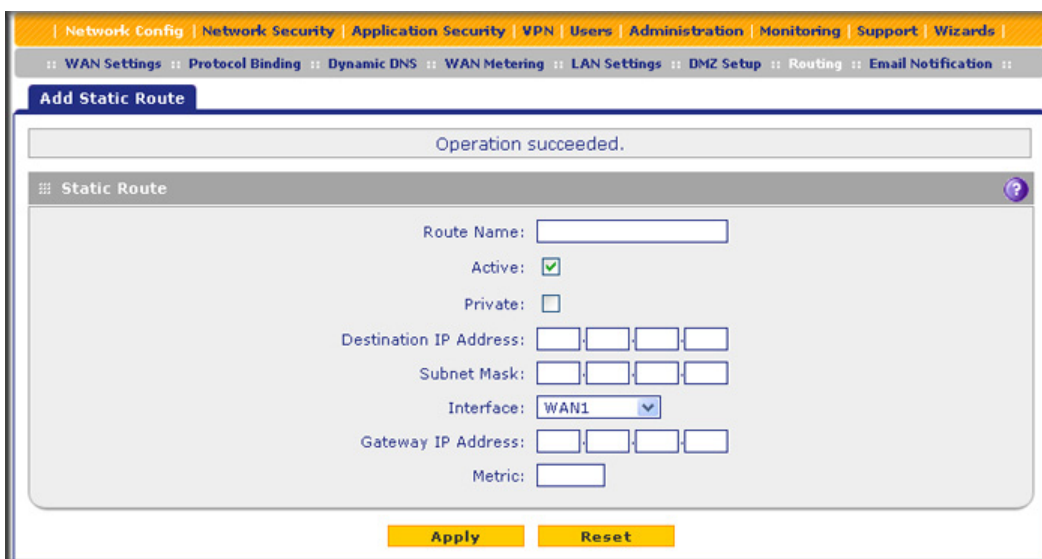

Figure 62.

---

3. Enter the settings as explained in the following table:

Table 24. Add Static Route screen settings

Setting	Description
Route Name	The route name for the static route (for purposes of identification and management).
Active	To make the static route effective, select the **Active** check box. **Note:** A route can be added to the table and made inactive if not needed. This allows you to use routes as needed without deleting and re-adding the entry. An inactive route is not advertised if RIP is enabled.
Private	If you want to limit access to the LAN only, select the **Private** check box. Doing so prevents the static route from being advertised in RIP.
Destination IP Address	The destination IP address of the host or network to which the route leads.
IP Subnet Mask	The IP subnet mask of the host or network to which the route leads. If the destination is a single host, enter **255.255.255.255**.
Interface	From the drop-down list, select the interface that is the physical network interface (a WAN interface, LAN, or DMZ for the multiple WAN port models; WAN, LAN, or DMZ for the single WAN port models) or virtual interface (VLAN profile) through which the route is accessible.
Gateway IP Address	The gateway IP address through which the destination host or network can be reached.
Metric	The priority of the route. Select a value between 2 and 15. If multiple routes to the same destination exist, the route with the lowest metric is used.

4. Click **Apply** to save your settings. The new static route is added to the Static Routes table.

➢ **To edit a static route that is in the Static Routes table:**

1. On the Routing screen (see *Figure 61* on page 116), click the **Edit** button in the Action column for the route that you want to modify. The Edit Static Route screen displays. This screen is identical to the Add Static Route screen (see the previous screen).

2. Modify the settings as explained in the previous table.

3. Click **Apply** to save your settings.

➢ **To delete one or more routes:**

1. On the Routing screen (see *Figure 61* on page 116), select the check box to the left of each route that you want to delete, or click the **Select All** table button to select all routes.

2. Click the **Delete** table button.

Configure Routing Information Protocol

Routing Information Protocol (RIP), RFC 2453, is an Interior Gateway Protocol (IGP) that is commonly used in internal networks (LANs). RIP enables a router to exchange its routing information automatically with other routers, to dynamically adjust its routing tables, and to adapt to changes in the network. RIP is disabled by default.

➤ **To enable and configure RIP:**

1. Select **Network Config > Routing**.

2. Click the **RIP Configuration** option arrow to the right of the Routing submenu tab. The RIP Configuration screen displays:

Figure 63.

3. Enter the settings as explained in the following table:

Table 25. RIP Configuration screen settings

Setting	Description
RIP	
RIP Direction	From the RIP Direction drop-down list, select the direction in which the UTM sends and receives RIP packets: • **None**. The UTM neither advertises its route table, nor accepts any RIP packets from other routers. This effectively disables RIP, and is the default setting. • **In Only**. The UTM accepts RIP information from other routers but does not advertise its routing table. • **Out Only**. The UTM advertises its routing table but does not accept RIP information from other routers. • **Both**. The UTM advertises its routing table and also processes RIP information received from other routers.
RIP Version	By default, the RIP version is set to Disabled. From the RIP Version drop-down list, select the version: • **RIP-1**. Classful routing that does not include subnet information. This is the most commonly supported version. • **RIP-2**. Routing that supports subnet information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format: - **RIP-2B**. Sends the routing data in RIP-2 format and uses subnet broadcasting. - **RIP-2M**. Sends the routing data in RIP-2 format and uses multicasting.
Authentication for RIP-2B/2M	
Authentication for RIP-2B/2M required?	Authentication for RP-2B or RIP-2M is disabled by default, that is, the No radio button is selected. To enable authentication for RP-2B or RIP-2M, select the **Yes** radio button, and enter the settings for the following fields.

First Key Parameters

MD5 Key Id	The identifier for the key that is used for authentication.
MD5 Auth Key	The password that is used for MD5 authentication.
Not Valid Before	The beginning of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. Before this date and time, the MD5 key is not valid.
Not Valid After	The end of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. After this date and time, the MD5 key is no longer valid.

Second Key Parameters

MD5 Key Id	The identifier for the key that is used for authentication.
MD5 Auth Key	The password that is used for MD5 authentication.

Table 25. RIP Configuration screen settings (continued)

Setting	Description	
Authentication for RIP-2B/2M required? (continued)	Not Valid Before	The beginning of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. Before this date and time, the MD5 key is not valid.
	Not Valid After	The end of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. After this date and time, the MD5 key is no longer valid.

4. Click **Apply** to save your settings.

Static Route Example

In this example, we assume the following:

- The UTM's primary Internet access is through a cable modem to an ISP.
- The UTM is on a local LAN with IP address 192.168.1.100.
- The UTM connects to a remote network where you need to access a device.
- The LAN IP address of the remote network is 134.177.0.0.

When you first configured the UTM, two implicit static routes were created:

- A default static route was created with your ISP as the gateway.
- A second static route was created to the local LAN for all 192.168.1.x addresses.

With this configuration, if you attempt to access a device on the 134.177.0.0 remote network, the UTM forwards your request to the ISP. In turn, the ISP forwards your request to the remote network, where the request is likely to be denied by the remote network's firewall.

In this case, you need to define a static route, informing the UTM that the 134.177.0.0 IP address should be accessed through the local LAN IP address (192.168.1.100).

The static route on the UTM needs to be defined as follows:

- The destination IP address and IP subnet mask need to specify that the static route applies to all 134.177.x.x IP addresses.
- The gateway IP address needs to specify that all traffic for the 134.177.x.x IP addresses should be forwarded to the local LAN IP address (192.168.1.100).
- A metric value of 1 should work since the UTM is on the local LAN.
- The static route can be made private only as a precautionary security measure in case RIP is activated.

Firewall Protection

5

This chapter describes how to use the firewall features of the UTM to protect your network. This chapter contains the following sections:

- *About Firewall Protection*
- *Use Rules to Block or Allow Specific Kinds of Traffic*
- *Configure Other Firewall Features*
- *Create Services, QoS Profiles, and Bandwidth Profiles*
- *Set a Schedule to Block or Allow Specific Traffic*
- *Enable Source MAC Filtering*
- *Set Up IP/MAC Bindings*
- *Configure Port Triggering*
- *Configure Universal Plug and Play*
- *Use the Intrusion Prevention System*

> **Note:** The IGMP submenu tab shows on the Firewall configuration menu of the UTM9S only.

About Firewall Protection

A firewall protects one network (the trusted network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. You can further segment keyword blocking to certain known groups. For information about how to set up LAN groups, see *Manage Groups and Hosts (LAN Groups)* on page 106.

A firewall incorporates the functions of a Network Address Translation (NAT) router, protects the trusted network from hacker intrusions or attacks, and controls the types of traffic that can flow between the two networks. Unlike simple NAT routers, a firewall uses a process called Stateful Packet Inspection to protect your network from attacks and intrusions. NAT performs a very limited stateful inspection in that it considers whether the incoming packet is in response to an outgoing request, but true Stateful Packet Inspection goes far beyond NAT.

Administrator Tips

Consider the following operational items:

1. As an option, you can enable remote management if you have to manage distant sites from a central location (see *Configure Authentication Domains, Groups, and Users* on page 345 and *Configure Remote Management Access* on page 399).

2. Although rules are the basic way of managing the traffic through your system (see *Use Rules to Block or Allow Specific Kinds of Traffic* on page 122), you can further refine your control using the following features and capabilities of the UTM:

   - Groups and hosts (see *Manage Groups and Hosts (LAN Groups)* on page 106)
   - Services (see *Service-Based Rules* on page 123)
   - Schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 163)
   - Allow or block sites and applications (see *Set Web Access Exception Rules* on page 221)
   - Source MAC filtering (see *Enable Source MAC Filtering* on page 164)
   - Port triggering (see *Configure Port Triggering* on page 168)

3. Content filtering is a firewall component. The UTM provides such extensive content-filtering options that an entire chapter is dedicated to this subject; see *Chapter 6, Content Filtering and Optimizing Scans*.

4. Some firewall settings might affect the performance of the UTM. For more information, see *Performance Management* on page 389.

5. You can monitor blocked content and malware threats in real time. For more information, see *Monitor Real-Time Traffic, Security, and Statistics* on page 433.

6. The firewall logs can be configured to log and then email denial of access, general attack, and other information to a specified email address. For information about how to configure logging and notifications, see *Configure Logging, Alerts, and Event Notifications* on page 422.

Use Rules to Block or Allow Specific Kinds of Traffic

Firewall rules are used to block or allow specific traffic passing through from one side to the other. You can configure up to 800 rules on the UTM. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the UTM are:

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

The firewall rules for blocking and allowing traffic on the UTM can be applied to LAN WAN traffic, DMZ WAN traffic, and LAN DMZ traffic.

Table 26. Number of supported firewall rule configurations

Traffic rule	Maximum number of outbound rules	Maximum number of inbound rules	Maximum number of supported rules
LAN WAN	300	300	600
DMZ WAN	50	50	100
LAN DMZ	50	50	100
Total Rules	400	400	800

Service-Based Rules

The rules to block traffic are based on the traffic's category of service:

- **Outbound rules (service blocking)**. Outbound traffic is usually allowed unless the firewall is configured to disallow it.
- **Inbound rules (port forwarding)**. Inbound traffic is usually blocked by the firewall unless the traffic is in response to a request from the LAN side. The firewall can be configured to allow this otherwise blocked traffic.
- **Customized services**. Additional services can be added to the list of services in the factory defaults list. These added services can then have rules defined for them to either allow or block that traffic (see *Add Customized Services* on page 152).
- **Quality of Service (QoS) priorities**. Each service has its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change the QoS priority, which changes the traffic mix through the system (see *Create Quality of Service Profiles* on page 158).

Outbound Rules (Service Blocking)

The UTM allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering.

> **Note:** See *Enable Source MAC Filtering* on page 164 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.

⚠ **WARNING!**

Allowing inbound services opens security holes in your UTM. Enable only those ports that are necessary for your network.

The following table describes the fields that define the rules for outbound traffic and that are common to most Outbound Service screens (see *Figure 66* on page 132, *Figure 69* on page 135, and *Figure 72* on page 138).

The steps to configure outbound rules are described in the following sections:

- *Set LAN WAN Rules*
- *Set DMZ WAN Rules*
- *Set LAN DMZ Rules*

Table 27. Outbound rules overview

Setting	Description
Service	The service or application to be covered by this rule. If the service or application does not display in the list, you need to define it using the Services screen (see *Add Customized Services* on page 152).
Action	The action for outgoing connections covered by this rule: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any outbound traffic that is not blocked by rules you create is allowed by the default rule. **Note:** ALLOW rules are useful only if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is currently blocked by another rule.
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This drop-down list is activated only when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action. • Use the Schedule screen to configure the time schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 163).
LAN Users	The settings that determine which computers on your network are affected by this rule. The options are: • **Any**. All PCs and devices on your LAN. • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of devices. • **Group**. Select the LAN group to which the rule applies. Use the LAN Groups screen to assign PCs to groups. See *Manage Groups and Hosts (LAN Groups)* on page 106. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 156.

Table 27. Outbound rules overview (continued)

Setting	Description
WAN Users	The settings that determine which Internet locations are covered by the rule, based on their IP address. The options are: • **Any**. All Internet IP address are covered by this rule. • **Single address**. Enter the required address in the Start field. • **Address range**. Enter the required addresses the Start and End fields. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 156.
DMZ Users	The settings that determine which DMZ computers on the DMZ network are affected by this rule. The options are: • **Any**. All PCs and devices on your DMZ network. • **Single address**. Enter the required address in the Start field to apply the rule to a single PC on the DMZ network. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of DMZ computers.
QoS Profile	The priority assigned to IP packets of this service. The priorities are defined by Type of Service (ToS) in the Internet Protocol Suite standards, RFC 1349. The QoS profile determines the priority of a service, which, in turn, determines the quality of that service for the traffic passing through the firewall. The UTM marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Create Quality of Service Profiles* on page 158. **Note:** There is no default QoS profile on the UTM. After you have created a QoS profile, it can become active only when you apply it to a nonblocking inbound or outbound firewall rule. **Note:** This field is not applicable to LAN DMZ rules.
Bandwidth Profile	Bandwidth limiting determines the way in which the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Create Bandwidth Profiles* on page 160. Bandwidth limiting occurs in the following ways: • For outbound traffic. On the available WAN interface in the primary WAN mode and auto-rollover mode, and on the selected interface in load balancing mode. • For inbound traffic. On the LAN interface for all WAN modes. **Note:** Bandwidth limiting does not apply to the DMZ interface.

Table 27. Outbound rules overview (continued)

Setting	Description
Log	The setting that determines whether packets covered by this rule are logged. The options are: • **Always**. Always log traffic considered by this rule, whether it matches or not. This is useful when you are debugging your rules. • **Never**. Never log traffic considered by this rule, whether it matches or not.
NAT IP	The setting that specifies whether the source address of the outgoing packets on the WAN should be assigned the address of the WAN interface or the address of a different interface. You can specify these settings only for outbound traffic on the WAN interface. The options are: • **WAN Interface Address**. All the outgoing packets on the WAN are assigned to the address of the specified WAN interface. • **Single Address**. All the outgoing packets on the WAN are assigned to the specified IP address, for example, a secondary WAN address that you have configured. **Note:** The NAT IP option is available only when the WAN mode is NAT. The IP address specified should fall under the WAN subnet.

Inbound Rules (Port Forwarding)

If you have enabled Network Address Translation (NAT), your network presents only *one* IP address to the Internet, and outside users cannot directly access any of your local computers (LAN users). (For information about configuring NAT, see *Configure Network Address Translation (All Models)* on page 77.) However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet. The rule informs the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This process is also known as port forwarding.

Whether or not DHCP is enabled, how the PC accesses the server's LAN address impacts the inbound rules. For example:

- If your external IP address is assigned dynamically by your ISP (DHCP enabled), the IP address might change periodically as the DHCP lease expires. Consider using Dyamic DNS so that external users can always find your network (see *Configure Dynamic DNS* on page 87).

- If the IP address of the local server PC is assigned by DHCP, it might change when the PC is rebooted. To avoid this, use the Reserved (DHCP Client) feature in the LAN Groups screen to keep the PC's IP address constant (see *Set Up Address Reservation* on page 111).

- Local PCs need to access the local server using the PCs' local LAN address. Attempts by local PCs to access the server using the external WAN IP address will fail.

Note: See *Configure Port Triggering* on page 168 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Note: The UTM always blocks denial of service (DoS) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you cannot use it (that is, the service becomes unavailable).

Note: When the Block TCP Flood and Block UDP Flood check boxes are selected on the Attack Checks screen (see *Attack Checks, VPN Pass-through, and Multicast Pass-through* on page 146), multiple concurrent connections of the same application from one host or IP address (such as multiple DNS queries from one PC) trigger the UTM's DoS protection.

Note: For more information about protecting the UTM from incoming threats, see *Use the Intrusion Prevention System* on page 172.

The following table describes the fields that define the rules for inbound traffic and that are common to most Inbound Service screens (see *Figure 67* on page 133, *Figure 70* on page 136, and *Figure 73* on page 138).

The steps to configure inbound rules are described in the following sections:

- *Set LAN WAN Rules*
- *Set DMZ WAN Rules*
- *Set LAN DMZ Rules*

Table 28. Inbound rules overview

Setting	Description
Service	The service or application to be covered by this rule. If the service or application does not display in the list, you need to define it using the Services screen (see *Add Customized Services* on page 152).
Action	The action for outgoing connections covered by this rule: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any inbound traffic that is not blocked by rules you create is allowed by the default rule.

Table 28. Inbound rules overview (continued)

Setting	Description
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This drop-down list is activated only when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action. • Use the Schedule screen to configure the time schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 163).
Send to LAN Server	The LAN server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.) The options are: • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of devices.
Send to DMZ Server	The DMZ server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.)
Translate to Port Number	If you want to assign the LAN server or DMZ server to a specific port, you can enable this setting and specify a port number.
WAN Destination IP Address	The setting that determines the destination IP address applicable to incoming traffic. This is the public IP address that maps to the internal LAN server. On the multiple WAN port models, it can be either the address of a WAN interface or another public IP address (when you have a secondary WAN address configured). On the single WAN port models, it can be either the address of the single WAN interface or another public IP address (when you have a secondary WAN address configured). You also have the option to enter an address range. Enter the required addresses in the Start and End fields to apply the rule to a range of devices.
LAN Users	The settings that determine which computers on your network are affected by this rule. The options are: • **Any**. All PCs and devices on your LAN. • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of devices. • **Group**. Select the group to which the rule applies. Use the LAN Groups screen to assign PCs to groups. See *Manage Groups and Hosts (LAN Groups)* on page 106. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 156. **Note:** For LAN WAN inbound rules, this field is not applicable when the WAN mode is NAT because your network presents only *one* IP address to the Internet.
WAN Users	The settings that determine which Internet locations are covered by the rule, based on their IP address. The options are: • **Any**. All Internet IP address are covered by this rule. • **Single address**. Enter the required address in the Start field. • **Address range**. Enter the required addresses in the Start and End fields. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 156.

Table 28. Inbound rules overview (continued)

Setting	Description
DMZ Users	The settings that determine which DMZ computers on the DMZ network are affected by this rule. The options are: • **Any**. All PCs and devices on your DMZ network. • **Single address**. Enter the required address in the Start field to apply the rule to a single PC on the DMZ network. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of DMZ computers. **Note:** For DMZ WAN inbound rules, this field is not applicable when the WAN mode is NAT because your network presents only *one* IP address to the Internet.
QoS Profile	The priority assigned to IP packets of this service. The priorities are defined by Type of Service (ToS) in the Internet Protocol Suite standards, RFC 1349. The QoS profile determines the priority of a service which, in turn, determines the quality of that service for the traffic passing through the firewall. The UTM marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Create Quality of Service Profiles* on page 158. **Note:** There is no default QoS profile on the UTM. After you have created a QoS profile, it can become active only when you apply it to a nonblocking inbound or outbound firewall rule. **Note:** This field is not applicable to LAN DMZ rules.
Log	The setting that determines whether packets covered by this rule are logged. The options are: • **Always**. Always log traffic considered by this rule, whether it matches or not. This is useful when you are debugging your rules. • **Never**. Never log traffic considered by this rule, whether it matches or not.
Bandwidth Profile	Bandwidth limiting determines the way in which the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Create Bandwidth Profiles* on page 160. Bandwidth limiting occurs in the following ways: • For outbound traffic. On the available WAN interface in the primary WAN mode and auto-rollover mode, and on the selected interface in load balancing mode. • For inbound traffic. On the LAN interface for all WAN modes. **Note:** Bandwidth limiting does not apply to the DMZ interface.

Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active servers at your location. If you are unsure, see the acceptable use policy of your ISP.

Order of Precedence for Rules

As you define a new rule, it is added to a table in a Rules screen as the last item in the list, as shown in the LAN WAN Rules screen example in the following figure:

Figure 64.

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules table, beginning at the top and proceeding to the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. For example, you should place the most strict rules at the top (those with the most specific services or addresses). The Up and Down table buttons in the Action column allow you to relocate a defined rule to a new position in the table.

Set LAN WAN Rules

The default outbound policy is to allow all traffic to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the Internet (outbound). This feature is also referred to as service blocking. You can change the default policy of Allow Always to Block Always to block all outbound traffic, which then allows you to enable only specific services to pass through the UTM.

➢ **To change the default outbound policy:**

1. Select **Network Security > Firewall**. The Firewall submenu tabs display, with the LAN WAN Rules screen in view.

2. Next to Default Outbound Policy, select **Block Always** from the drop-down list.

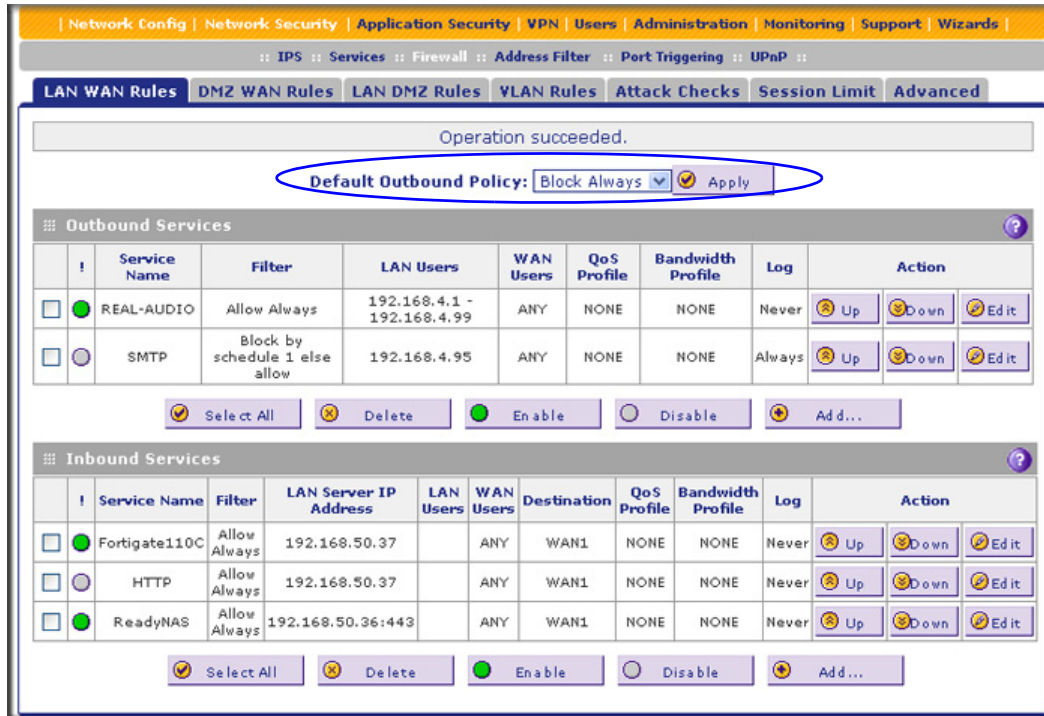**3.** Next to the drop-down list, click the **Apply** table button.

Figure 65.

To make changes to an existing outbound or inbound service rule, in the Action column to the right of to the rule, click one of the following table buttons:

- **Edit**. Allows you to make any changes to the definition of an existing rule. Depending on your selection, either the Edit LAN WAN Outbound Service screen (identical to *Figure 66* on page 132) or Edit LAN WAN Inbound Service screen (identical to *Figure 67* on page 133) displays, containing the data for the selected rule.

- **Up**. Moves the rule up one position in the table rank.

- **Down**. Moves the rule down one position in the table rank.

➢ **To enable, disable, or delete one or more rules:**

1. Select the check box to the left of each rule that you want to enable, disable, or delete, or click the **Select All** table button to select all rules.

2. Click one of the following table buttons:

- **Enable**. Enables the rule or rules. The ! status icon changes from a gray circle to a green circle, indicating that the selected rule or rules are enabled. (By default, when a rule is added to the table, it is automatically enabled.)

- **Disable**. Disables the rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the selected rule or rules are disabled.

- **Delete**. Deletes the selected rule or rules.

LAN WAN Outbound Service Rules

You can define rules that specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule can block or allow traffic between an internal IP LAN address and any external WAN IP address according to the schedule created in the Schedule screen.

You can also tailor these rules to your specific needs (see *Administrator Tips* on page 122).

⚠️ **WARNING!**

> **This feature is for advanced administrators. Incorrect configuration might cause serious problems.**

➢ **To create a new outbound LAN WAN service rule:**

1. In the LAN WAN Rules screen, click the **Add** table button under the Outbound Services table. The Add LAN WAN Outbound Service screen displays:

Figure 66.

2. Enter the settings as explained in *Table 27* on page 124.
3. Click **Apply** to save your changes. The new rule is now added to the Outbound Services table.

LAN WAN Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the Internet to the LAN) is blocked. Remember that allowing inbound services opens potential security holes in your firewall. Enable only those ports that are necessary for your network.

➢ **To create a new inbound LAN WAN service rule:**

1. In the LAN WAN Rules screen, click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays:

Figure 67.

2. Enter the settings as explained in *Table 28* on page 127.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Set DMZ WAN Rules

The firewall rules for traffic between the DMZ and the Internet are configured on the DMZ WAN Rules screen. The default outbound policy is to block all traffic from and to the Internet. You can then apply firewall rules to allow specific types of traffic either going out from the DMZ to the Internet (outbound) or coming in from the Internet to the DMZ (inbound).

There is no drop-down list that lets you set the default outbound policy as there is on the LAN WAN Rules screen. You can change the default outbound policy by enabling all outbound traffic and then blocking only specific services from passing through the UTM. You do so by adding outbound services rules (see *DMZ WAN Outbound Service Rules* on page 134).

To access the DMZ WAN Rules screen, select **Network Security > Firewall > DMZ WAN Rules**. The DMZ WAN Rules screen displays. (The following figure shows a rule in the Outbound Services table as an example.)
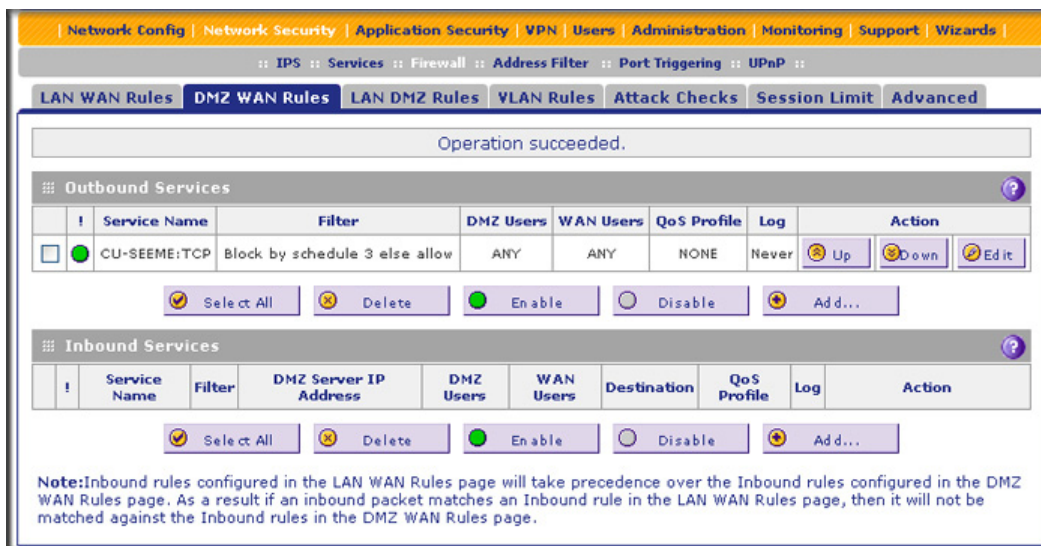

Figure 68.

> **To make changes to an existing outbound or inbound service rule:**

In the Action column to the right of to the rule, click one of the following table buttons:

- **Edit**. Allows you to make any changes to the definition of an existing rule. Depending on your selection, either the Edit DMZ WAN Outbound Service screen (identical to *Figure 69* on page 135) or the Edit DMZ WAN Inbound Service screen (identical to *Figure 70* on page 136) displays, containing the data for the selected rule.
- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.

> **To delete or disable one or more rules:**

1. Select the check box to the left of each rule that you want to delete or disable, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
   - **Disable**. Disables the selected rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the selected rule is or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Delete**. Deletes the selected rule or rules.

DMZ WAN Outbound Service Rules

You can change the default outbound policy or define rules that specify exceptions to the default outbound policy. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule

can block or allow traffic between the DMZ and any external WAN IP address according to the schedule created in the Schedule screen.

➢ **To create a new outbound DMZ WAN service rule:**

1. In the DMZ WAN Rules screen, click the **Add** table button under the Outbound Services table. The Add DMZ WAN Outbound Service screen displays:

Figure 69.

2. Enter the settings as explained in *Table 27* on page 124.
3. Click **Apply.** The new rule is now added to the Outbound Services table. The rule is automatically enabled.

DMZ WAN Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the Internet to the DMZ) is blocked.

Inbound rules that are configured on the LAN WAN Rules screen take precedence over inbound rules that are configured on the DMZ WAN Rules screen. As a result, if an inbound packet matches an inbound rule on the LAN WAN Rules screen, it is not matched against the inbound rules on the DMZ WAN Rules screen.

➢ **To create a new inbound DMZ WAN service rule:**

1. In the DMZ WAN Rules screen, click the **Add** table button under the Inbound Services table. The Add DMZ WAN Inbound Service screen displays:

Figure 70.

2. Enter the settings as explained in *Table 28* on page 127.

3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Set LAN DMZ Rules

The LAN DMZ Rules screen allows you to create rules that define the movement of traffic between the LAN and the DMZ. The default outbound and inbound policies are to block all traffic between the local LAN and DMZ network. You can then apply firewall rules to allow specific types of traffic either going out from the LAN to the DMZ (outbound) or coming in from the DMZ to the LAN (inbound).

There is no drop-down list that lets you set the default outbound policy as there is on the LAN WAN Rules screen. You can change the default outbound policy by allowing all outbound traffic and then blocking specific services from passing through the UTM. You do so by adding outbound service rules (see *LAN DMZ Outbound Service Rules* on page 137).

To access the LAN DMZ Rules screen and to make changes to an existing outbound or inbound service rule, select **Network Security > Firewall > LAN DMZ Rules**. The LAN DMZ Rules screen displays:
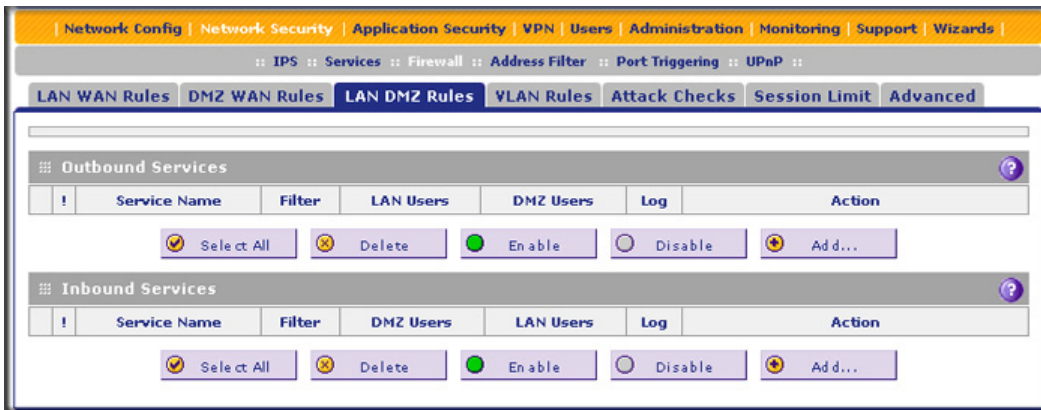
Figure 71.

In the Action column to the right of to the rule, click one of the following table buttons:

- **Edit**. Allows you to make any changes to the rule definition of an existing rule. Depending on your selection, either the Edit LAN DMZ Outbound Service screen (identical to *Figure 72* on page 138) or the Edit LAN DMZ Inbound Service screen (identical to *Figure 73* on page 138) displays, containing the data for the selected rule.
- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.

➢ **To delete or disable one or more rules:**

1. Select the check box to the left of each rule that you want to delete or disable, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
   - **Disable**. Disables the selected rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the selected rule is or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Delete**. Deletes the selected rule or rules.

LAN DMZ Outbound Service Rules

You can change the default outbound policy or define rules that specify exceptions to the default outbound policy. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule can block or allow traffic between the DMZ and any internal LAN IP address according to the schedule created in the Schedule screen.

➢ **To create a new outbound LAN DMZ service rule:**

1. In the LAN DMZ Rules screen, click the **Add** table button under the Outbound Services table. The Add LAN DMZ Outbound Service screen displays:
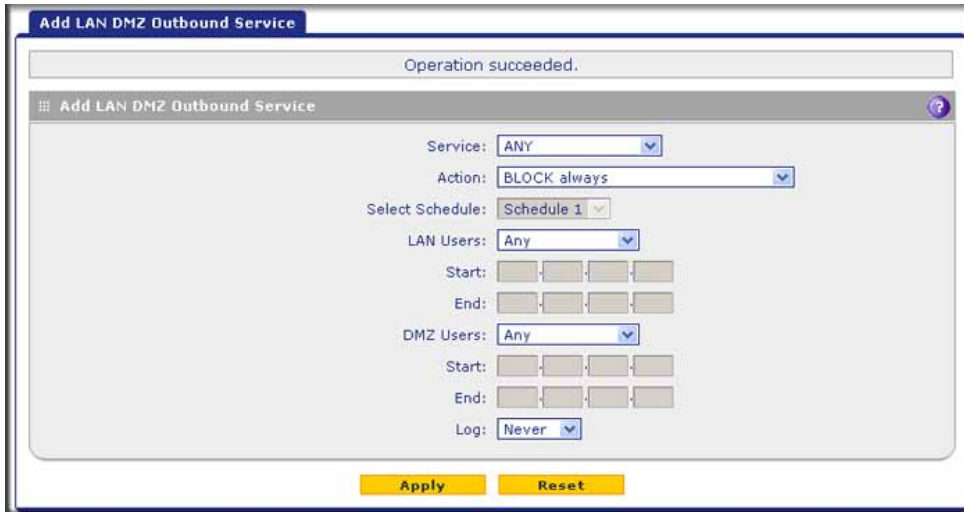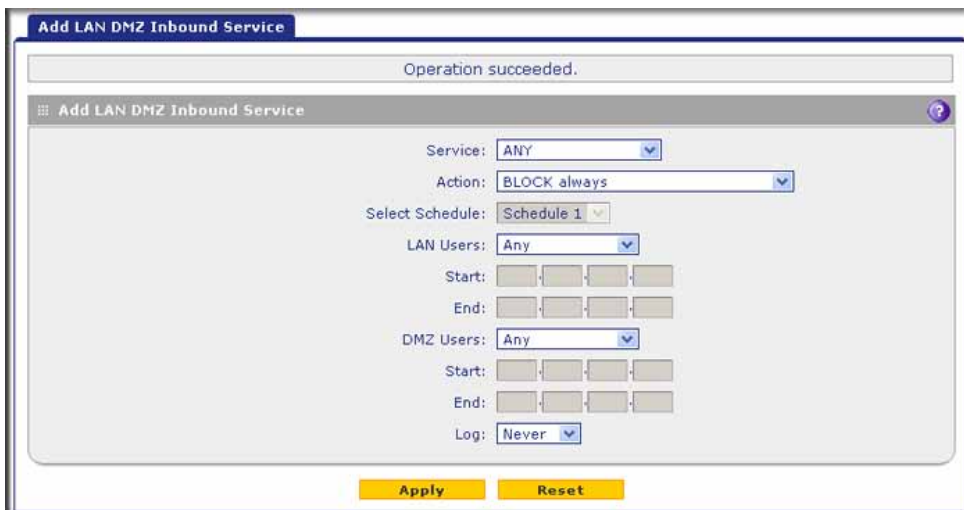
Figure 72.

2. Enter the settings as explained in *Table 27* on page 124.

3. Click **Apply.** The new rule is now added to the Outbound Services table. The rule is automatically enabled.

LAN DMZ Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the LAN to the DMZ) is blocked.

➢ **To create a new inbound LAN DMZ service rule:**

1. In the LAN DMZ Rules screen, click the **Add** table button under the Inbound Services table. The Add LAN DMZ Inbound Service screen displays:

Figure 73.

2. Enter the settings as explained in *Table 28* on page 127.

3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Inbound Rule Examples

LAN WAN Inbound Rule: Host a Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests from any outside IP address to the IP address of your web server at any time of the day.

Figure 74.

LAN WAN Inbound Rule: Allow Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule (see the following figure). In the example, CU-SeeMe connections are allowed only from a specified range of external IP addresses.

Figure 75.

LAN WAN or DMZ WAN Inbound Rule: Set Up One-to-One NAT Mapping

In this example, multi-NAT is configured to support multiple public IP addresses on one WAN interface. An inbound rule configures the UTM to host an additional public IP address and associate this address with a web server on the LAN.

The following addressing scheme is used to illustrate this procedure:

- NETGEAR UTM:
  - WAN IP address. 10.1.0.118
  - LAN IP address subnet. 192.168.1.1 with subnet 255.255.255.0
  - DMZ IP address subnet. 192.168.10.1 with subnet 255.255.255.0
- Web server PC on the UTM's LAN:
  - LAN IP address. 192.168.1.2
  - DMZ IP address. 192.168.10.2
  - Access to web server is (simulated) public IP address. 10.1.0.52

> **Tip:** If you arrange with your ISP to have more than one public IP address for
> your use, you can use the additional public IP addresses to map to
> servers on your LAN or DMZ. One of these public IP addresses is used
> as the primary IP address of the router that provides Internet access to
> your LAN PCs through NAT. The other addresses are available to map to
> your servers.

➢ **To configure the UTM for additional IP addresses:**

1. Select **Network Security > Firewall**. The Firewall submenu tabs display.
2. If your server is to be on your LAN, click the **LAN WAN Rules** submenu tab. (This is the screen used in this example). If your server is to be on your DMZ, click the **DMZ WAN Rules** submenu tab.
3. Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays:
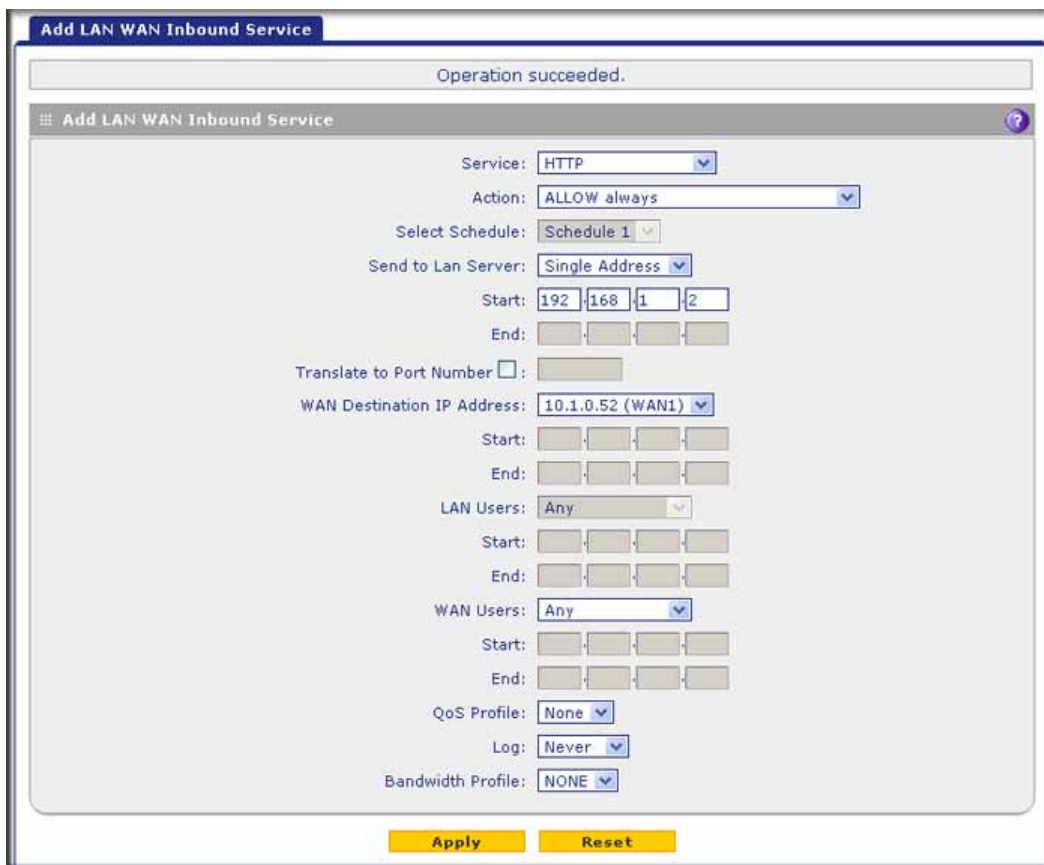

Figure 76.

4. From the Service drop-down list, select **HTTP** for a web server.
5. From the Action drop-down list, select **ALLOW Always**.
6. In the Send to LAN Server field, enter the local IP address of your web server PC (192.168.1.2 in this example).

7. For the multiple WAN port models only: From the WAN Destination IP Address drop-down list, select the web server (the simulated 10.1.0.52 address in this example) that you have defined on a WAN Secondary Addresses screen (see *Configure Secondary WAN Addresses* on page 85).

> **Note:** For the single WAN port models: The WAN Destination IP Address field is a fixed field.

8. Click **Apply** to save your settings. The rule is now added to the Inbound Services table of the LAN WAN Rules screen.

To test the connection from a PC on the Internet, type **http://<IP_address>**, in which *<IP_address>* is the public IP address that you have mapped to your web server. You should see the home page of your web server.

LAN WAN or DMZ WAN Inbound Rule: Specify an Exposed Host

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined.

➢ **To expose one of the PCs on your LAN or DMZ as this host:**

1. Create an inbound rule that allows all protocols.

2. Place the rule below all other inbound rules.

See an example in the following figure.
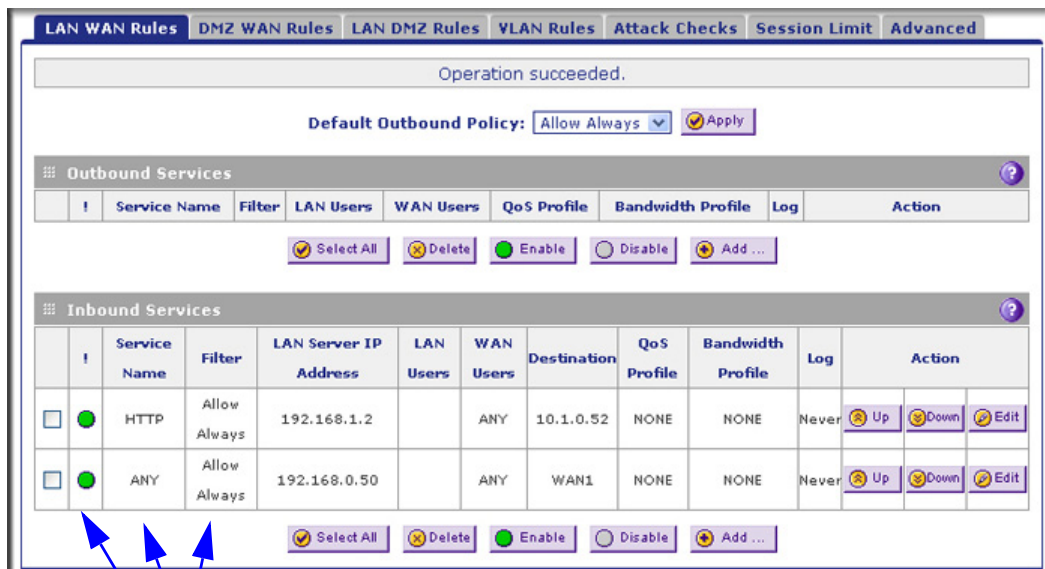
1. Select Any and Allow Always (or Allow by Schedule).
2. Place the rule below all other inbound rules.

Figure 77.

⚠️ **WARNING!**

> **For security, NETGEAR strongly recommends that you avoid creating an exposed host. When a computer is designated as the exposed host, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.**

Outbound Rule Example

Outbound rules let you prevent users from using applications such as Instant Messenger, Real Audio, or other nonessential sites.

LAN WAN Outbound Rule: Block Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block such an application from any internal IP address to any external address according to the schedule that you have created in the Schedule screen. See an example in the following figure.

You can also enable the UTM to log any attempt to use Instant Messenger during the blocked period.

Figure 78.

Configure Other Firewall Features

You can configure global VLAN rules and attack checks, set session limits, and manage the application level gateway (ALG) for SIP sessions.

VLAN Rules

The VLAN Rules screen allows you to specify inter-VLAN firewall rules (that is, firewall rules for VLANs that are created on the UTM) when inter-VLAN routing is not enabled (see *Configure a VLAN Profile* on page 98). For example, you can create one VLAN with IP address 192.168.1.0 and a second VLAN with IP address 192.168.2.0. You can then specify a VLAN firewall rule to allow access from all 192.168.1.* IP addresses to a web server with IP address 192.168.2.10 on the second VLAN and block all other traffic between the two VLANs.

➢ **To create a VLAN rule:**

1. Select **Network Security > Firewall > VLAN Rules**. The VLAN Rules screen displays. (The following figure shows one rule in the VLAN Services table as an example.)
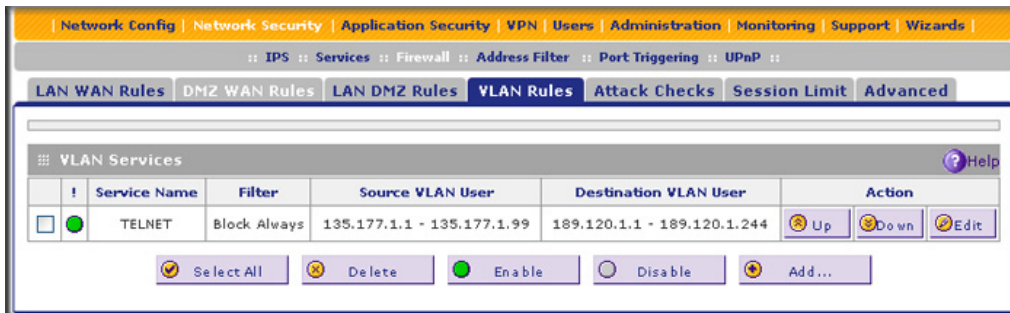

   Figure 79.

2. Under the VLAN Services table, click the **Add** table button. The Add VLAN-VLAN Service screen displays:
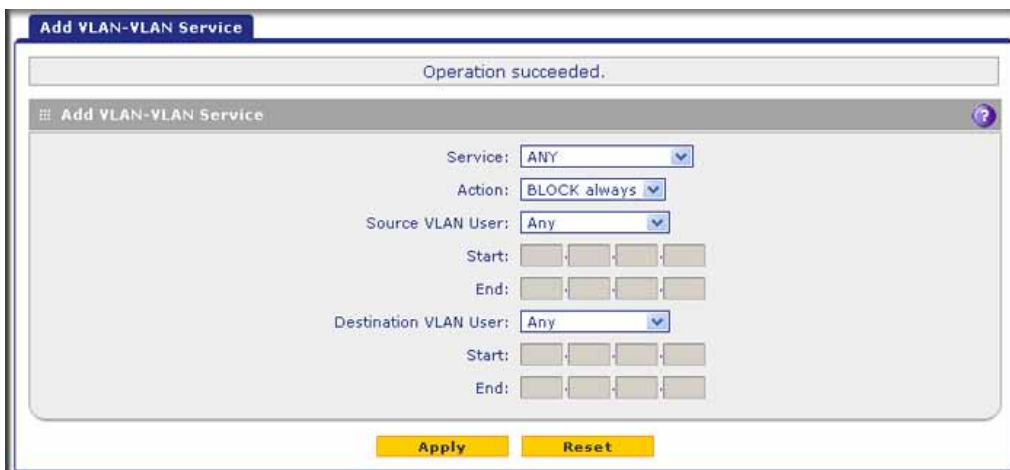

   Figure 80.

3. Enter the settings as explained in the following table.

Table 29. Add VLAN-VLAN Service screen settings

Setting	Description
Service	The service or application to be covered by this rule. If the service or application does not display in the list, you need to define it using the Services screen (see *Add Customized Services* on page 152).
Action	The action for VLAN connections covered by this rule: • **BLOCK always** • **ALLOW always** **Note:** ALLOW rules are useful only if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is currently blocked by another rule.
Source VLAN User	The settings that determine which VLAN users who send traffic are affected by this rule. The options are: • **Any**. All PCs and devices that are part of the VLAN. • **Single address**. Enter the required address in the Start field to apply the rule to a single PC in the VLAN. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of computers in the VLAN.
Destination VLAN User	The settings that determine which VLAN users who receive traffic are affected by this rule. The options are: • **Any**. All PCs and devices that are part of the VLAN. • **Single address**. Enter the required address in the Start field to apply the rule to a single PC in the VLAN. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of computers in the VLAN.

4. Click **Apply** to save your settings. The new VLAN rule is added to the VLAN Services table.

➢ **To change the position of an existing VLAN rule in the VLAN Services table:**

In the Action column to the right of the rule, click one of the following table buttons:

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.

➢ **To edit a VLAN rule:**

1. In the VLAN Services table, click the **Edit** table button to the right of the VLAN rule that you want to edit. The Edit VLAN-VLAN Service screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified VLAN rule is displayed in the VLAN Services table.

➢ **To delete or disable one or more VLAN rules:**

1. Select the check box to the left of each VLAN rule that you want to delete or disable, or click the **Select All** table button to select all VLAN rules.

2. Click one of the following table buttons:

    • **Disable**. Disables the selected VLAN rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the selected VLAN rule is or rules are disabled. (By default, when a VLAN rule is added to the table, it is automatically enabled.)

    • **Delete**. Deletes the selected VLAN rule or rules.

Attack Checks, VPN Pass-through, and Multicast Pass-through

The Attack Checks screen allows you to specify whether or not the UTM should be protected against common attacks in the DMZ, LAN, and WAN networks, and lets you configure VPN pass-through and multicast pass-through. The various types of attack checks are listed on the Attack Checks screen and defined in *Table 30* on page 147. The configuration of multicast pass-through for the UTM9S is different from the other UTM models; see *Configure Multicast Pass-through (UTM9S Only)* on page 148.

➢ **To enable the appropriate attack checks for your network environment:**

1. Select **Network Security > Firewall > Attack Checks**. The Attack Checks screen displays:
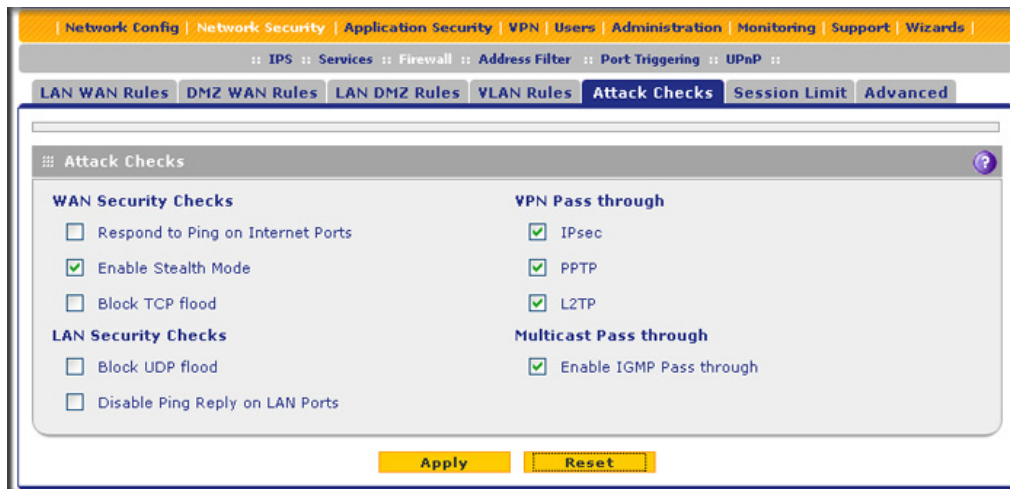

Figure 81.

2. Enter the settings as explained in the following table:

Table 30. Attack Checks screen settings

Setting	Description
WAN Security Checks	
Respond to Ping on Internet Ports	Select the **Respond to Ping on Internet Ports** check box to enable the UTM to respond to a ping from the Internet. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to enable the UTM to respond to a ping from the Internet.
Enable Stealth Mode	Select the **Enable Stealth Mode** check box (which is the default setting) to prevent the UTM from responding to port scans from the WAN, thus making it less susceptible to discovery and attacks.
Block TCP flood	Select the **Block TCP flood** check box to enable the UTM to drop all invalid TCP packets and to protect the UTM from a SYN flood attack. A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN (synchronize) requests to a target system. When the system responds, the attacker does not complete the connections, thus leaving the connection half open and flooding the server with SYN messages. No legitimate connections can then be made. By default, the Block TCP flood check box is cleared.
LAN Security Checks	
Block UDP flood	Select the **Block UDP flood** check box to prevent the UTM from accepting more than 20 simultaneous, active User Datagram Protocol (UDP) connections from a single device on the LAN. By default, the Block UDP flood check box is cleared. A UDP flood is a form of denial of service attack that can be initiated when one device sends a large number of UDP packets to random ports on a remote host. As a result, the distant host does the following: 1. Checks for the application listening at that port. 2. Sees that no application is listening at that port. 3. Replies with an ICMP Destination Unreachable packet. When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker might also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach the attacker, thus making the attacker's network location anonymous.
Disable Ping Reply on LAN Ports	Select the **Disable Ping Reply on LAN Ports** check box to prevent the UTM from responding to a ping on a LAN port. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to prevent the UTM from responding to a ping on a LAN port.

Table 30. Attack Checks screen settings (continued)

Setting	Description
VPN Pass through	
IPSec PPTP L2TP	When the UTM functions in NAT mode, all packets going to the remote VPN gateway are first filtered through NAT and then encrypted according to the VPN policy. For example, if a VPN client or gateway on the LAN side of the UTM wants to connect to another VPN endpoint on the WAN side (placing the UTM between two VPN endpoints), encrypted packets are sent to the UTM. Because the UTM filters the encrypted packets through NAT, the packets become invalid unless you enable the VPN Pass through feature. To enable the VPN tunnel to pass the VPN traffic without any filtering, select any or all of the following check boxes: • **IPSec**. Disables NAT filtering for IPSec tunnels. • **PPTP**. Disables NAT filtering for PPTP tunnels. • **L2TP**. Disables NAT filtering for L2TP tunnels. By default, all three check boxes are selected.
Multicast Pass through **Note:** This section is not displayed on the Attacks screen for the UTM9S. For the UTM9S, see the next section, *Configure Multicast Pass-through (UTM9S Only)*.	
Enable IGMP Pass through	IP multicast pass-through allows multicast packets that originate in the WAN subnet, such as packets from a media streaming or gaming application, to be forwarded to the LAN subnet. Internet Group Management Protocol (IGMP) is used to support multicast between IP hosts and their adjacent neighbors. Select the **Enable IGMP Pass through** check box to enable IP multicast pass-through. By default, IP multicast pass-through is enabled.

3. Click **Apply** to save your settings.

Configure Multicast Pass-through (UTM9S Only)

➢ **To configure multicast pass-through for the UTM9S:**

1. Select **Network Security > Firewall > IGMP**. The IGMP screen displays. (The following figure shows one alternate network as an example.)
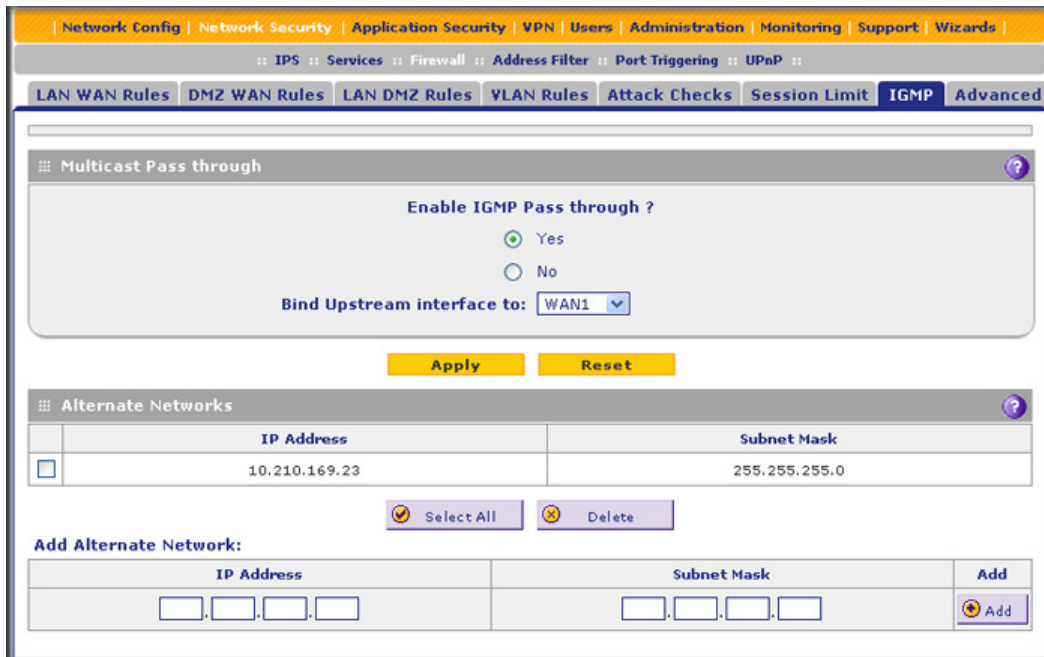
Figure 82.

2. In the Multicast Pass through section of the screen, select the **Yes** radio button to enable multicast pass-through. (By default the Yes radio button is enabled.)

   When you enable multicast pass-through, an Internet Group Management Protocol (IGMP) proxy is enabled for the upstream (WAN) and downstream (LAN) interfaces. This proxy allows the UTM9S to forward relevant multicast traffic from the WAN to the LAN, and to keep track of the IGMP group membership when LAN hosts join or leave the multicast group.

3. If load balancing is configured, select the upstream interface to which multicast traffic is bound because only a single interface can function as the upstream interface. From the Bind Upstream interface to drop-down list, select the interface (WAN1 or WAN2) or the slot in which the xDLS module is installed. The default interface is WAN1.

   When you change the WAN mode to load balancing, multicast traffic is bound by default to the active interface of the previous WAN mode.

   If the interface to which multicast traffic is bound is configured for PPPoE, PPPoA, or PPTP, you need to add the multicast source address to the Alternate Networks table:

   a. In the Alternate Networks section of the screen, below the table, enter the following settings:
      • **IP Address**. Enter the multicast source IP address.
      • **Subnet Mask**. Enter the subnet mask for the multicast source address.

   b. Click the **Add** table button in the rightmost column to add the multicast source address to the Alternate Networks table.

      Repeat *step a* and *step b* for each multicast source address that you need to add to the Alternate Networks table.

Table 31. Session Limit screen settings (continued)

Setting	Description
User Limit	Enter a number to indicate the user limit. If the User Limit Parameter is set to Percentage of Max Sessions, the number specifies the maximum number of sessions that are allowed from a single-source device as a percentage of the total session connection capacity of the UTM. (The session limit is per-device based.) If the User Limit Parameter is set to Number of Sessions, the number specifies an absolute value. **Note:** Some protocols such as FTP and RSTP create two sessions per connection, which should be considered when configuring a session limit.
Total Number of Packets Dropped due to Session Limit	This is a nonconfigurable counter that displays the total number of dropped packets when the session limit is reached.
Session Timeout	
TCP Timeout	For each protocol, specify a time-out in seconds. A session expires if no data for the session is received for the duration of the time-out period. The default time-out periods are 1200 seconds for TCP sessions, 180 seconds for UDP sessions, and 8 seconds for ICMP sessions.
UDP Timeout	
ICMP Timeout	

4. Click **Apply** to save your settings.

Manage the Application Level Gateway for SIP Sessions

The application level gateway (ALG) facilitates multimedia sessions such as voice over IP (VoIP) sessions that use the Session Initiation Protocol (SIP) across the firewall and provides support for multiple SIP clients. ALG support for SIP is disabled by default.

➢ **To enable ALG for SIP:**

1. Select **Network Security > Firewall > Advanced**. The Advanced screen displays (see the following figure).
2. Select the **Enable SIP ALG** check box.
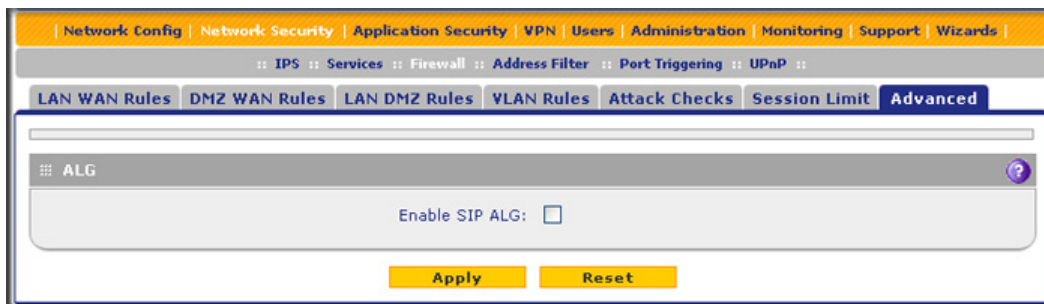3. Click **Apply** to save your settings.

Figure 84.

Create Services, QoS Profiles, and Bandwidth Profiles

When you create inbound and outbound firewall rules, you use firewall objects such as services, service groups, IP groups (LAN and WAN groups), QoS profiles, bandwidth profiles, and schedules to narrow down the firewall rules:

- **Services**. A service narrows down the firewall rule to an application and a port number. You can also narrow down the firewall rule to a group of services. For information about adding services and service groups, see *Add Customized Services* on page 152 and *Create Service Groups* on page 154.

- **IP groups**. An IP group is a LAN group or a WAN group to which you add individual IP addresses. You can narrow down the firewall rule to such an IP group. For information about creating IP groups, see *Create IP Groups* on page 156.

- **QoS profiles**. A Quality of Service (QoS) profile defines the relative priority of an IP packet for traffic that matches the firewall rule. For information about creating QoS profiles, see *Create Quality of Service Profiles* on page 158.

- **Bandwidth profiles**. A bandwidth profile allocates and limits traffic bandwidth for the LAN users to which a firewall rule is applied. For information about creating bandwidth profiles, see *Create Bandwidth Profiles* on page 160.

> **Note:** A schedule narrows down the period during which a firewall rule is applied. For information about specifying schedules, see *Set a Schedule to Block or Allow Specific Traffic* on page 163.

Add Customized Services

Services are functions performed by server computers at the request of client computers. You can configure up to 125 custom services.

For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC 1700, *Assigned Numbers*. Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the UTM already holds a list of many service port numbers, you are not limited to these choices. Use the Services screen to add additional services and applications to the list for use in defining firewall rules. The Services screen shows a list of services that you have defined, as shown in *Figure 85* on page 153.

To define a new service, you need to determine first which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application, user groups, or newsgroups. When you have the port number information, you can enter it on the Services screen.

➢ **To add a customized service:**

1. Select **Network Security > Services**. The Services screen displays. The Custom Services table shows the user-defined services. (The following figure shows some examples.)
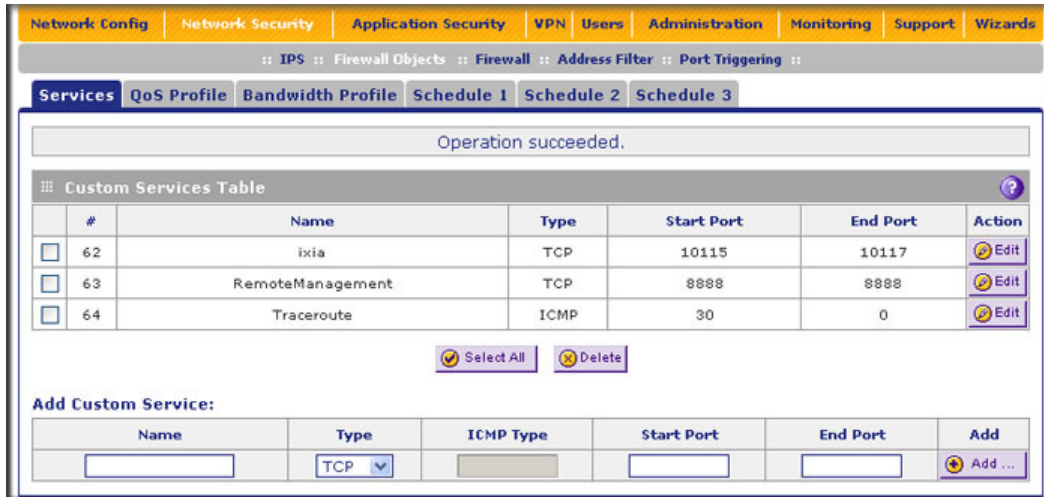
Figure 85.

2. In the Add Customer Service section of the screen, enter the settings as explained in the following table:

Table 32. Services screen settings

Setting	Description
Name	A descriptive name of the service for identification and management purposes.
Type	From the Type drop-down list, select the Layer 3 protocol that the service uses as its transport protocol: • **TCP** • **UDP** • **ICMP**
ICMP Type	A numeric value that can range between 0 and 40. For a list of ICMP types, see *http://www.iana.org/assignments/icmp-parameters*. **Note:** This field is enabled only when you select ICMP from the Type drop-down list.

Table 32. Services screen settings (continued)

Setting	Description
Start Port	The first TCP or UDP port of a range that the service uses. **Note:** This field is enabled only when you select TCP or UDP from the Type drop-down list.
End Port	The last TCP or UDP port of a range that the service uses. If the service uses only a single port number, enter the same number in the Start Port and End Port fields. **Note:** This field is enabled only when you select TCP or UDP from the Type drop-down list.

3. Click **Apply** to save your settings. The new custom service is added to the Custom Services table.

➤ **To edit a service:**

1. In the Custom Services table, click the **Edit** table button to the right of the service that you want to edit. The Edit Service screen displays:

Figure 86.

2. Modify the settings that you wish to change (see the previous table).

3. Click **Apply** to save your changes. The modified service is displayed in the Custom Services table.

➤ **To delete one or more services:**

1. In the Custom Services table, select the check box to the left of each service that you want to disable, or click the **Select All** table button to select all services.

2. Click the **Delete** table button.

Create Service Groups

A service group can contain a collection of predefined and customized services. You use a service group as a firewall object to which you apply a firewall rule.

One advantage of a service group is that you can create a single firewall object with multiple noncontiguous ports (for example ports 3000, 4000, and 5000) and apply the object in a single firewall rule. For example, if there are 10 web servers, each of which requires the same three port-forwarding rules, you can create a service group for the port-forwarding rules, an IP group for the web servers (see *Create IP Groups* on page 156), and then create only one firewall rule.

➢ **To create a service group:**

1. Select **Network Security > Services > Service Group**. The Service Group screen displays. (The following figure shows two groups in the Custom Service Group table as an example.)
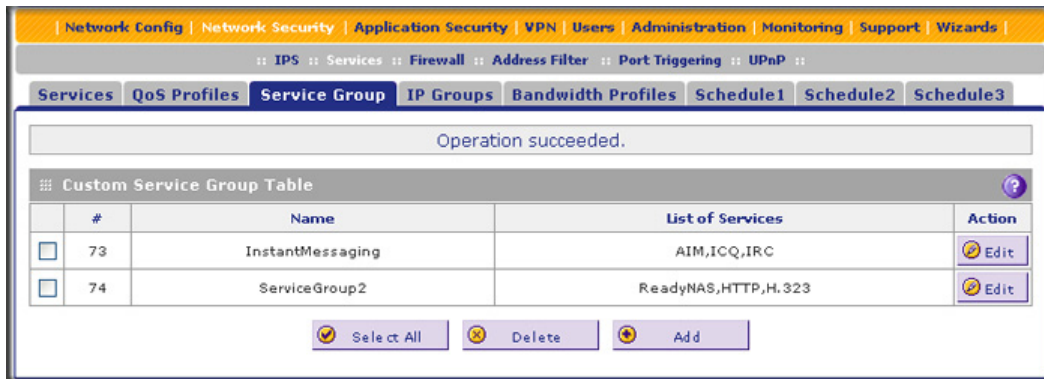
Figure 87.

2. Under the Custom Service Group table, click the **Add** table button. The Add Service Group screen displays:
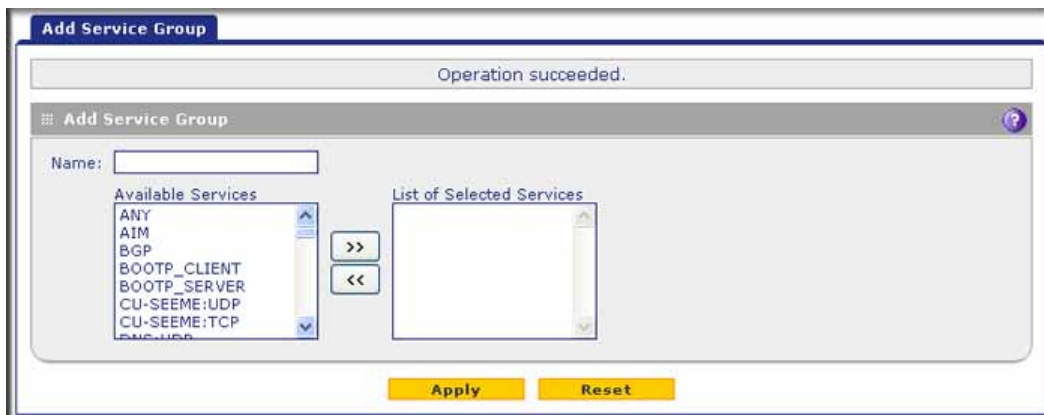

Figure 88.

3. In the Name field, enter a name for the service.

4. Use the move buttons (<< and >>) to move services between the Available Services field and the List of Selected Services field to specify the services that you want to be part of the group.

5. Click **Apply** to save your changes. The new service group is displayed in the Custom Services Group table on the Service Groups screen.

➢ **To edit a service group:**

1. In the Custom Services Group table, click the **Edit** table button to the right of the service group that you want to edit. The Edit Service group screen displays.

2. Modify the settings that you wish to change (see *step 3* and *step 4* in the previous procedure).

3. Click **Apply** to save your changes. The modified service group is displayed in the Custom Services Group table.

Create IP Groups

An IP group contains a collection of individual IP addresses that do not need to be within the same IP address range. You specify an IP group as either a LAN group or WAN group and use the group as a firewall object to which you apply a firewall rule.

➢ **To create an IP group:**

1. Select **Network Security > Services > IP Groups**. The IP Groups screen displays. (The following figure shows three groups in the Custom IP Groups table as an example.)
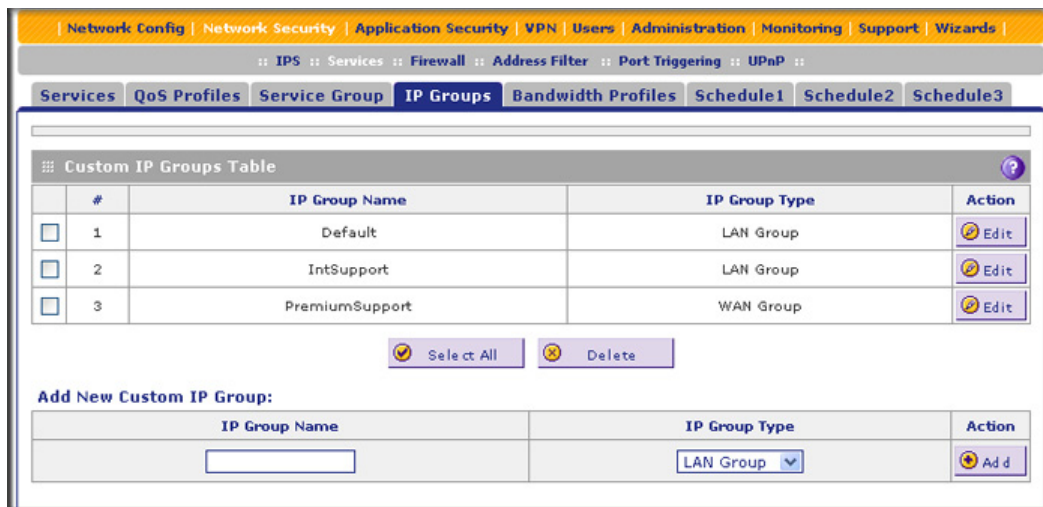

Figure 89.

2. In the Add New Custom IP Group section of the screen, do the following:
   • In the IP Group Name field, enter a name for the group.
   • From the IP Group Type drop-down list, select **LAN Group** or **WAN Group**.

3. Click **Apply** to save your changes. The new IP group is displayed in the Custom IP Groups table.

4. In the Custom IP Groups table, click the **Edit** table button to the right of the IP group that you just created. The Edit IP Group screen displays. (The following figure shows three IP addresses in the IP Addresses Grouped table as an example.)

Figure 90.

5. In the IP Address fields, type an IP address.

6. Click the **Add** table button to add the IP address to the IP Addresses Grouped table.

7. Repeat the previous two steps to add more IP addresses to the IP Addresses Grouped table.

8. Click the **Edit** table button to return to IP Groups screen.

➢ **To edit a service group:**

1. In the Custom IP Groups table, click the **Edit** table button to the right of the IP group that you want to edit. The Edit IP Group screen displays.

2. In the Edit New Custom IP Group section of the screen, modify the settings that you wish to change:
   - You can change the group name.
   - You can change the group type.
   - You can delete an IP address from the IP Addresses Grouped table by selecting the check box to the left of the IP address that you want to delete and then clicking the **Delete** table button. You can delete all IP addresses by selecting the **Select All** table button and clicking the **Delete** table button.
   - You can add IP addresses to the IP Addresses Grouped table (see *step 4*, *step 5*, and *step 6* in the previous procedure).

3. Click the **Edit** table button to return to IP Groups screen.

➢ **To delete an IP group:**

1. In the Custom IP Groups table, select the check box to the left of each IP group that you want to delete, or click the **Select All** table button to select all groups.

2. Click the **Delete** table button.

Create Quality of Service Profiles

A Quality of Service (QoS) profile defines the relative priority of an IP packet when multiple connections are scheduled for simultaneous transmission on the UTM. A QoS profile becomes active only when it is associated with a nonblocking inbound or outbound firewall rule, and traffic matching the firewall rule is processed by the UTM.

After you have created a QoS profile, you can assign the QoS profile to firewall rules on the following screens:

- Add LAN WAN Outbound Services screen (see *Figure 66* on page 132).
- Add LAN WAN Inbound Services screen (see *Figure 67* on page 133).
- Add DMZ WAN Outbound Services screen (see *Figure 69* on page 135).
- Add DMZ WAN Inbound Services screen (see *Figure 70* on page 136).

Priorities are defined by the Type of Service (ToS) in the Internet Protocol Suite standards, RFC 1349.

There is no default QoS profile on the UTM. Following are examples of QoS profiles that you *could* create:

- **Normal service profile**. Used when no special priority is given to the traffic. You would typically mark the IP packets for services with this priority with a ToS value of 0.
- **Minimize-cost profile**. Used when data needs to be transferred over a link that has a lower cost. You would typically mark the IP packets for services with this priority with a ToS value of 1.
- **Maximize-reliability profile**. Used when data needs to travel to the destination over a reliable link and with little or no retransmission. You would typically mark the IP packets for services with this priority with a ToS value of 2.
- **Maximize-throughput profile**. Used when the volume of data transferred during an interval is important even if the latency over the link is high. You would typically mark the IP packets for services with this priority with a ToS value of 3 or 4.
- **Minimize-delay profile**. Used when the time required (latency) for the packet to reach the destination needs to be low. You would typically mark the IP packets for services with this priority with a ToS value of 7.

➢ **To create a QoS profile:**

1. Select **Network Security > Services > QoS Profiles**. The QoS Profiles screen displays. (The following figure shows some profiles in the List of QoS Profiles table as an example.)
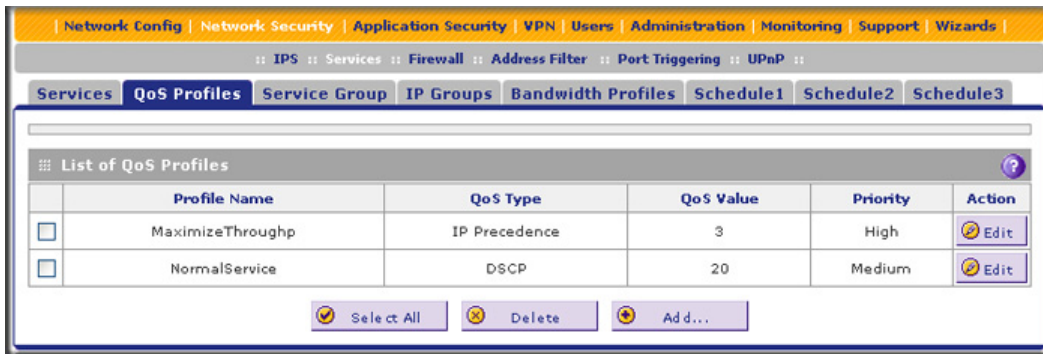
Figure 91.

The screen displays the List of QoS Profiles table with the user-defined profiles.

2. Under the List of QoS Profiles table, click the **Add** table button. The Add QoS Profile screen displays:
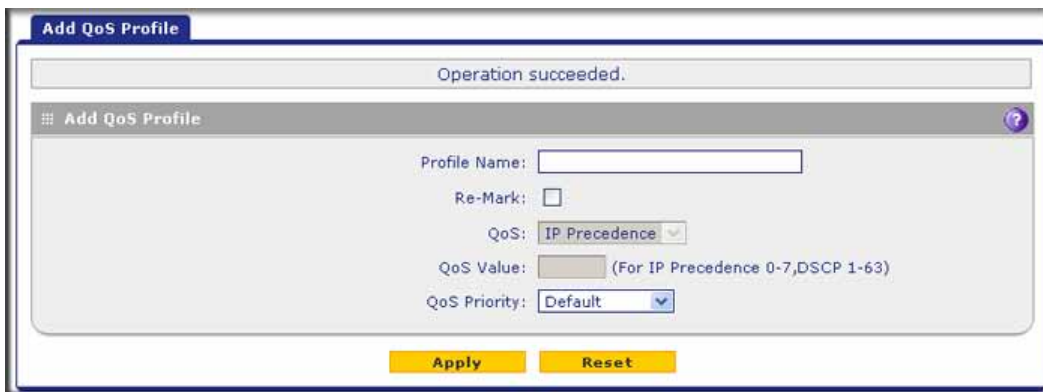

Figure 92.

3. Enter the settings as explained in the following table.

Note: This document assumes that you are familiar with QoS concepts such QoS priority queues, IP precedence, DHCP, and their values.

Table 33. Add QoS Profile screen settings

Setting	Description
Profile Name	A descriptive name of the QoS profile for identification and management purposes.
Re-Mark	Select the **Re-Mark** check box to set the differentiated services (DiffServ) mark in the Type of Service (ToS) byte of an IP header by specifying the QoS type (IP precedence or DHCP) and QoS value. If you clear the Re-Mark check box, the QoS type and QoS value are ignored, and you can configure the QoS priority only.

Table 33. Add QoS Profile screen settings (continued)

Setting	Description
QoS	From the QoS drop-down list, select one of the following traffic classification methods: • **IP Precedence**. A legacy method that sets the priority in the ToS byte of an IP header. • **DSCP**. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (which is the same as the ToS byte) of an IP header.
QoS Value	The QoS value in the ToS or Diffserv byte of an IP header. The QoS value that you enter depends on your selection from the QoS drop-down list: • For IP precedence, select a value from 0 to 7. • For DSCP, select a value from 0 to 63.
QoS Priority	From the QoS Priority drop-down list, select one of the following priority queues: • **Default** • **High** • **Medium High** • **Medium** • **Low**

4. Click **Apply** to save your settings. The new QoS profile is added to the List of QoS Profiles table.

➢ **To edit a QoS profile:**

1. In the List of QoS Profiles table, click the **Edit** table button to the right of the QoS profile that you want to edit. The Edit QoS Profile screen displays.

2. Modify the settings that you wish to change (see the previous table).

3. Click **Apply** to save your changes. The modified QoS profile is displayed in the List of QoS Profiles table.

➢ **To delete one ore more QoS profiles:**

1. In the List of QoS Profiles table, select the check box to the left of each QoS profile that you want to delete, or click the **Select All** table button to select all profiles.

2. Click the **Delete** table button.

Create Bandwidth Profiles

Bandwidth profiles determine the way in which data is communicated with the hosts. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic, thus allocating LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN link. A single bandwidth profile can be for both outbound and inbound traffic.

For outbound traffic, you can apply bandwidth profiles on the available WAN interfaces in both the primary WAN mode and auto-rollover modes, and in load balancing mode on the

interface that you specify. For inbound traffic, you can apply bandwidth profiles to a LAN interface for all WAN modes. Bandwidth profiles do not apply to the DMZ interface.

When a new connection is established by a device, the device locates the firewall rule corresponding to the connection.

- If the rule has a bandwidth profile specification, the device creates a bandwidth class in the kernel.
- If multiple connections correspond to the same firewall rule, the connections all share the same bandwidth class.

An exception occurs for an individual bandwidth profile if the classes are per-source IP address classes. The source IP address is the IP address of the first packet that is transmitted for the connection. So for outbound firewall rules, the source IP address is the LAN-side IP address; for inbound firewall rules, the source IP address is the WAN-side IP address. The class is deleted when all the connections that are using the class expire.

After you have created a bandwidth profile, you can assign the bandwidth profile to firewall rules on the following screens:

- Add LAN WAN Outbound Services screen (see *Figure 66* on page 132).
- Add LAN WAN Inbound Services screen (see *Figure 67* on page 133).

➢ **To add and enable a bandwidth profile:**

1. Select **Network Security > Services > Bandwidth Profiles**. The Bandwidth Profiles screen displays. (The following figure shows one user-defined profile in the List of Bandwidth Profiles table as an example.)
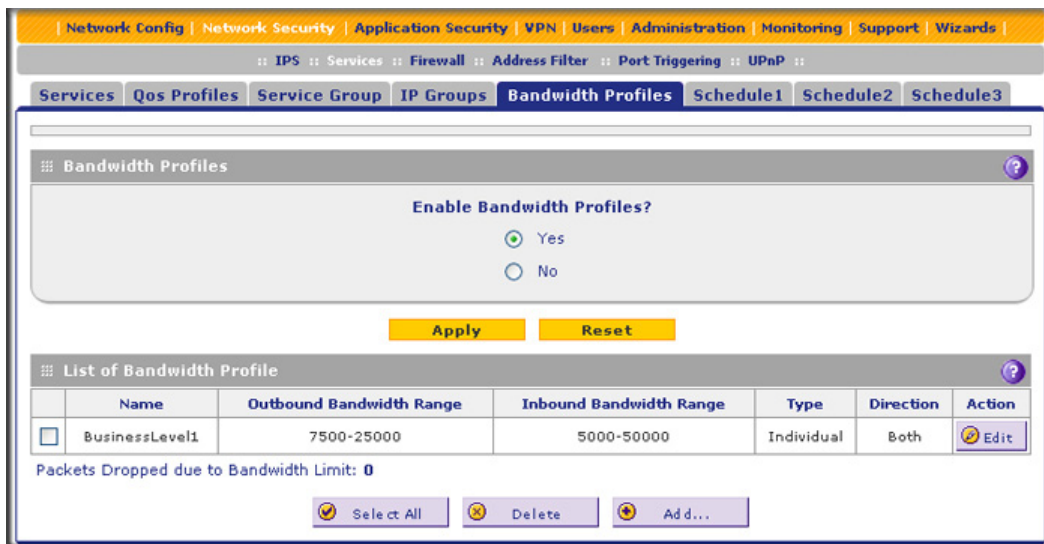
Figure 93.

2. Under the List of Bandwidth Profiles table, click the **Add** table button. The Add Bandwidth Profile screen displays:

Figure 94.

3. Enter the settings as explained in the following table:

Table 34. Add Bandwidth Profile screen settings

Setting	Description
Profile Name	A descriptive name of the bandwidth profile for identification and management purposes.
Direction	From the Direction drop-down list, select the traffic direction for the bandwidth profile: • **Outbound Traffic**. The bandwidth profile is applied only to outbound traffic. Specify the outbound minimum and maximum bandwidths. • **Inbound Traffic**. The bandwidth profile is applied only to inbound traffic. Specify the inbound minimum and maximum bandwidths. • **Both**. The bandwidth profile is applied to both outbound and inbound traffic. Specify both the outbound and inbound minimum and maximum bandwidths.
Outbound Minimum Bandwidth	The outbound minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.
Outbound Maximum Bandwidth	The outbound maximum allowed bandwidth in Kbps. The default setting is 100 Kbps (you cannot configure less than 100 Kbps); the maximum allowable bandwidth is 100000 Kbps.
Inbound Minimum Bandwidth	The inbound minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.
Inbound Maximum Bandwidth	The inbound maximum allowed bandwidth in Kbps. The default setting is 100 Kbps (you cannot configure less than 100 Kbps); the maximum allowable bandwidth is 100000 Kbps.

Table 34. Add Bandwidth Profile screen settings (continued)

Setting	Description	
Type	From the Type drop-down list, select the type for the bandwidth profile: • **Group**. The profile applies to all users, that is, all users share the available bandwidth. • **Individual**. The profile applies to an individual user, that is, each user can use the available bandwidth.	
	Maximum Number of Instances	If you select Individual from the Type drop-down list, you need to specify the maximum number of class instances that can be created by the individual bandwidth profile.

4. Click **Apply** to save your settings. The new bandwidth profile is added to the List of Bandwidth Profiles table.

5. In the Bandwidth Profiles section of the screen, select the **Yes** radio button under Enable Bandwidth Profiles? (By default the No radio button is selected.)

6. Click **Apply** to save your setting.

➢ **To edit a bandwidth profile:**

1. In the List of Bandwidth Profiles table, click the **Edit** table button to the right of the bandwidth profile that you want to edit. The Edit Bandwidth Profile screen displays.

2. Modify the settings that you wish to change (see the previous table).

3. Click **Apply** to save your changes. The modified bandwidth profile is displayed in the List of Bandwidth Profiles table.

➢ **To delete one or more bandwidth profiles:**

1. In the List of Bandwidth Profiles table, select the check box to the left of each bandwidth profile that you want to delete, or click the **Select All** table button to select all profiles.

2. Click the **Delete** table button.

Set a Schedule to Block or Allow Specific Traffic

Schedules define the time frames under which firewall rules can be applied. Three schedules, Schedule 1, Schedule 2, and Schedule 3, can be defined, and you can select any one of these when defining firewall rules.

➢ **To set a schedule:**

1. Select **Network Security > Services > Schedule 1**. The Schedule 1 screen displays:

Figure 95.

2. In the Scheduled Days section, select one of the following radio buttons:
    - **All Days**. The schedule is in effect all days of the week.
    - **Specific Days**. The schedule is in effect only on specific days. To the right of the radio buttons, select the check box for each day that you want the schedule to be in effect.

3. In the Scheduled Time of Day section, select one of the following radio buttons:
    - **All Day**. The schedule is in effect all hours of the selected day or days.
    - **Specific Times**. The schedule is in effect only during specific hours of the selected day or days. To the right of the radio buttons, fill in the Start Time and End Time fields (Hour, Minute, AM/PM) during which the schedule is in effect.

4. Click **Apply** to save your settings to Schedule 1.

Repeat these steps to set to a schedule for Schedule 2 and Schedule 3.

Enable Source MAC Filtering

The Source MAC Filter screen enables you to permit or block traffic coming from certain known PCs or devices.

By default, the source MAC address filter is disabled. All the traffic received from PCs with any MAC address is allowed. When the source MAC address filter is enabled, depending on the selected policy, traffic is either permitted or blocked if it comes from any PCs or devices whose MAC addresses are listed in MAC Addresses table.

> **Note:** For additional ways of restricting outbound traffic, see *Outbound Rules (Service Blocking)* on page 123.

➢ **To enable MAC filtering and add MAC addresses to be permitted or blocked:**

1. Select **Network Security > Address Filter**. The Address Filter submenu tabs display, with the Source MAC Filter screen in view. (The following figure shows one address in the MAC Addresses table as an example.)
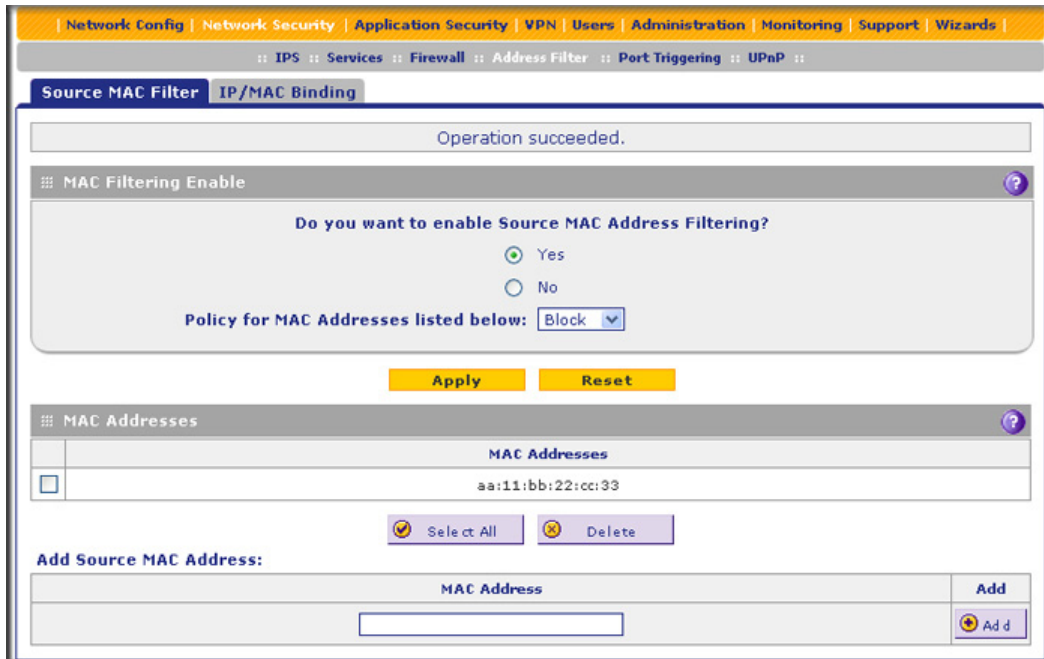
Figure 96.

2. In the MAC Filtering Enable section, select the **Yes** radio button.

3. In the same section, from the Policy for MAC Addresses listed below drop-down list, select one of the following options:

   • **Block**. Traffic coming from all addresses in the MAC Addresses table is blocked.

   • **Permit**. Traffic coming from all addresses in the MAC Addresses table is permitted.

4. Click **Apply** to save your settings. The MAC Address field in the Add Source MAC Address section of the screen now becomes available.

5. Build your list of source MAC addresses to be permitted or blocked by entering the first MAC address in the MAC Address field. A MAC address needs to be entered in the format xx:xx:xx:xx:xx:xx, in which x is a numeric (0 to 9) or a letter between a and f (inclusive), for example: aa:11:bb:22:cc:33.

6. Click the **Add** table button. The MAC address is added to the MAC Addresses table.

7. Repeat the previous two steps to add more MAC addresses to the MAC Addresses table.

➢ **To remove one or more entries from the table:**

1. Select the check box to the left of each MAC address that you want to delete, or click the **Select All** table button to select all entries.

2. Click the **Delete** table button.

Set Up IP/MAC Bindings

IP/MAC binding allows you to bind an IP address to a MAC address and the other way around. Some PCs or devices are configured with static addresses. To prevent users from changing their static IP addresses, the IP/MAC binding feature needs to be enabled on the UTM. If the UTM detects packets with an IP address that matches the IP address in the IP/MAC Bindings table but does not match the related MAC address in the IP/MAC Bindings table (or the other way around), the packets are dropped. If you have enabled the logging option for the IP/MAC binding feature, these packets are logged before they are dropped. The UTM displays the total number of dropped packets that violate either the IP-to-MAC binding or the MAC-to-IP binding.

> **Note:** You can bind IP addresses to MAC addresses for DHCP assignment on the LAN Groups submenu. See *Manage the Network Database* on page 107.

As an example, assume that three computers on the LAN are set up as follows, and that their IP and MAC addresses are added to the IP/MAC Bindings table:

- Host 1. MAC address (00:01:02:03:04:05) and IP address (192.168.10.10)
- Host 2. MAC address (00:01:02:03:04:06) and IP address (192.168.10.11)
- Host 3. MAC address (00:01:02:03:04:07) and IP address (192.168.10.12)

There are three possible scenarios in relation to the addresses in the IP/MAC Bindings table:

- Host 1 has not changed its IP and MAC addresses. A packet coming from Host 1 has IP and MAC addresses that match those in the IP/MAC Bindings table.

- Host 2 has changed its MAC address to 00:01:02:03:04:09. The packet has an IP address that matches the IP address in the IP/MAC Bindings table but a MAC address that does not match the MAC address in the IP/MAC Bindings table.

- Host 3 has changed its IP address to 192.168.10.15. The packet has a MAC address that matches the MAC address in the IP/MAC Bindings table but an IP address that does not match the IP address in the IP/MAC Bindings table.

In this example, the UTM blocks the traffic coming from Host 2 and Host 3, but allows the traffic coming from Host 1 to any external network. The total count of dropped packets is displayed.

➢ **To set up IP/MAC bindings:**

1. Select **Network Security > Address Filter > IP/MAC Binding**. The IP/MAC Binding screen displays. (The following figure shows some bindings in the IP/MAC Binding table as an example.)
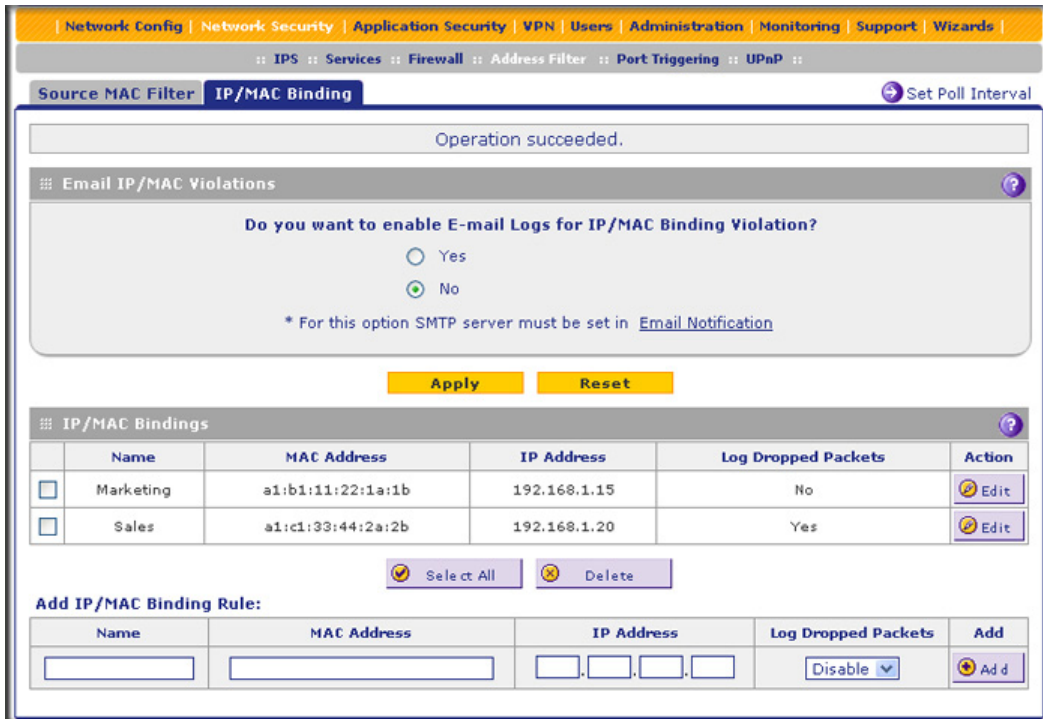

Figure 97.

2. Enter the settings as explained in the following table:

Table 35. IP/MAC Binding screen settings

Setting	Description
Email IP/MAC Violations	
Do you want to enable E-mail Logs for IP/MAC Binding Violation?	Select one of the following radio buttons: • **Yes**. IP/MAC binding violations are emailed. • **No**. IP/MAC binding violations are not emailed. **Note:** Click the **Email Notification** link to ensure that emailing of logs is enabled on the Email and Syslog screen (see *Configure Logging, Alerts, and Event Notifications* on page 422).
IP/MAC Bindings	
Name	A descriptive name of the binding for identification and management purposes.
MAC Address	The MAC address of the PC or device that is bound to the IP address.

Table 35. IP/MAC Binding screen settings (continued)

Setting	Description
IP Address	The IP address of the PC or device that is bound to the MAC address.
Log Dropped Packets	To log the dropped packets, select **Enable** from the drop-down list. The default setting is Disable.

3. Click the **Add** table button. The new IP/MAC rule is added to the IP/MAC Bindings table.
4. Click **Apply** to save your changes.

➢ **To edit an IP/MAC binding:**

1. In the IP/MAC Bindings table, click the **Edit** table button to the right of the IP/MAC binding that you want to edit. The Edit IP/MAC Binding screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified IP/MAC binding displays in the IP/MAC Bindings table.

➢ **To remove one or more IP/MAC bindings from the table:**

1. Select the check box to the left of each IP/MAC binding that you want to delete, or click the **Select All** table button to select all bindings.
2. Click the **Delete** table button.

Configure Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port-triggering feature requires that you know the port numbers used by the application.

Once configured, port triggering operates as follows:

1. A PC makes an outgoing connection using a port number that is defined in the Port Triggering Rules table.
2. The UTM records this connection, opens the additional incoming port or ports that are associated with the rule in the port triggering table, and associates them with the PC.
3. The remote system receives the PC's request and responds using the incoming port or ports that are associated with the rule in the port triggering table on the UTM.
4. The UTM matches the response to the previous request and forwards the response to the PC.

Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a request from the LAN network. As such, it would be handled in accordance with the inbound port-forwarding rules, and most likely would be blocked.

Note these restrictions on port triggering:

- Only one PC can use a port-triggering application at any time.
- After a PC has finished using a port-triggering application, there is a short time-out period before the application can be used by another PC. This time-out period is required so the UTM can determine that the application has terminated.

> **Note:** For additional ways of allowing inbound traffic, see *Inbound Rules (Port Forwarding)* on page 126.

> **To add a port-triggering rule:**

1. Select **Network Security > Port Triggering**. The Port Triggering screen displays. (The following figure shows a rule in the Port Triggering Rule table as an example.)
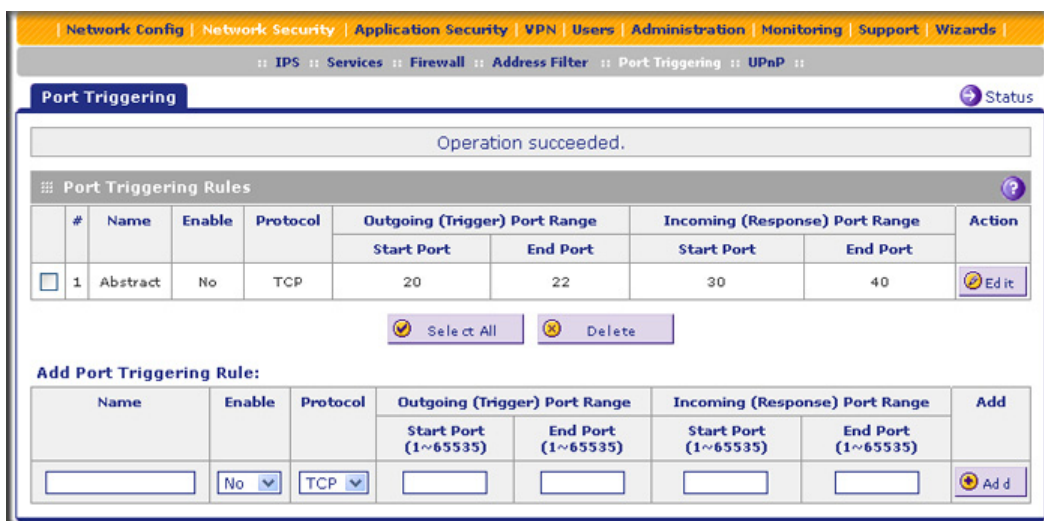
Figure 98.

2. In the Add Port Triggering Rule section, enter the settings as explained in the following table:

Table 36. Port Triggering screen settings

Setting	Description
Name	A descriptive name of the rule for identification and management purposes.
Enable	From the drop-down list, select **Yes** to enable the rule. (You can define a rule but not enable it.) The default setting is No.
Protocol	From the drop-down list, select the protocol to which the rule applies: • **TCP**. The rule applies to an application that uses the Transmission Control Protocol (TCP). • **UDP**. The rule applies to an application that uses the User Datagram Protocol (UDP).

Table 36. Port Triggering screen settings (continued)

Setting		Description
Outgoing (Trigger) Port Range	Start Port	The start port (1–65534) of the range for triggering.
	End Port	The end port (1–65534) of the range for triggering.
Incoming (Response) Port Range	Start Port	The start port (1–65534) of the range for responding.
	End Port	The end port (1–65534) of the range for responding.

3. Click the **Add** table button. The new port-triggering rule is added to the Port Triggering Rules table.

➢ **To edit a port-triggering rule:**

1. In the Port Triggering Rules table, click the **Edit** table button to the right of the port-triggering rule that you want to edit. The Edit Port Triggering Rule screen displays.

2. Modify the settings that you wish to change (see the previous table).

3. Click **Apply** to save your changes. The modified port-triggering rule is displayed in the Port Triggering Rules table.

➢ **To remove one or more port-triggering rules from the table:**

1. Select the check box to the left of each port-triggering rule that you want to delete, or click the **Select All** table button to select all rules.

2. Click the **Delete** table button.

➢ **To display the status of the port-triggering rules:**

Click the **Status** option arrow in the upper right of the Port Triggering screen. A pop-up screen displays, showing the status of the port-triggering rules.
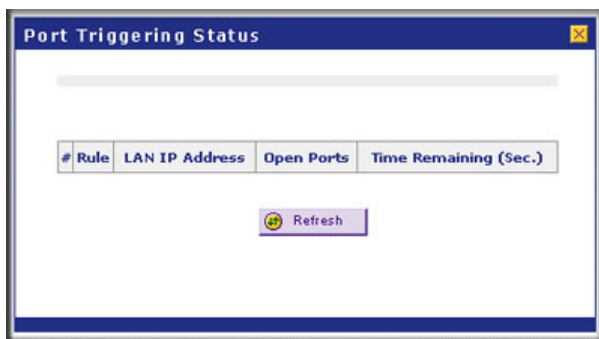
Figure 99.

Configure Universal Plug and Play

The Universal Plug and Play (UPnP) feature enables the UTM to automatically discover and configure devices when it searches the LAN and WAN.

1. Select **Security > UPnP**. The UPnP screen displays:

Figure 100.

The UPnP Portmap Table in the lower part of the screen shows the IP addresses and other settings of UPnP devices that have accessed the UTM and that have been automatically detected by the UTM:

- **Active**. A Yes or No indicates if the UPnP device port that established a connection is currently active.
- **Protocol**. Indicates the network protocol such as HTTP or FTP that is used by the device to connect to the VPN firewall.
- **Int. Port**. Indicates if any internal ports are opened by the UPnP device.
- **Ext. Port**. Indicates if any external ports are opened by the UPnP device.
- **IP Address**. Lists the IP address of the UPnP device accessing the VPN firewall.

2. To enable the UPnP feature, select the **Yes** radio button. (The feature is disabled by default.) To disable the feature, select **No**.

3. Fill in the following fields:
- **Advertisement Period**. Enter the period in minutes that specifies how often the UTM should broadcast its UPnP information to all devices within its range. The default setting is 40 minutes.
- **Advertisement Time to Live**. Enter a number that specifies how many steps (hops) each UPnP packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range. The default setting is 4 hops.

4. Click **Apply** to save your settings.

To refresh the contents of the UPnP Portmap Table, click **Refresh**.

Use the Intrusion Prevention System

The Intrusion Prevention System (IPS) of the UTM monitors all network traffic to detect, in real time, network attacks and port scans and to protect your network from such intrusions. You can set up alerts, block source IP addresses from which port scans are initiated, and drop traffic that carries attacks. You can configure detection of and protection from specific attacks such as web, email, database, malware, and other attacks. The IPS differs from the malware scan mechanism (see *Configure Web Malware Scans* on page 197) in that it monitors individual packets, whereas the malware scan mechanism monitors files.

The IPS also allows you to configure port scan detection to adjust it to your needs and to protect the network from unwanted port scans that could compromise the network security.

The IPS is disabled by default.

➢ **To enable intrusion prevention and configure port scan detection:**

1. Select **Network Security > IPS**. The IPS submenu tabs display, with the Global screen in view.
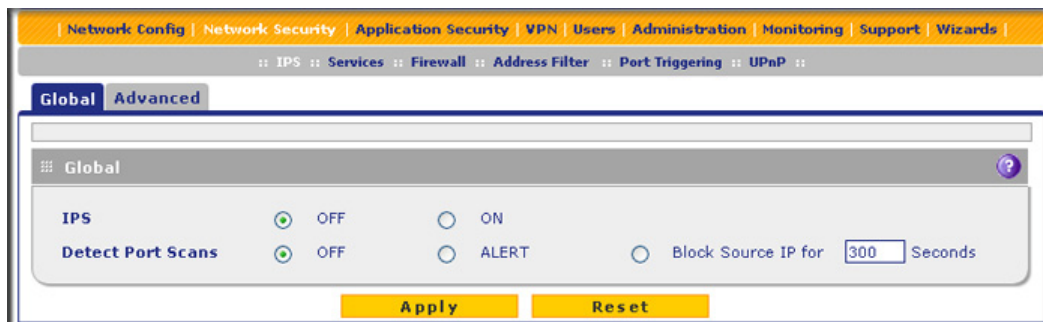
Figure 101.

2. To enable the IPS, select the **ON** radio button. The default setting is OFF.

3. Configure port scan detection by selecting one of the following radio buttons:
   - **OFF**. Port scan detection is disabled. This is the default setting.
   - **ALERT**. When a port is scanned, an alert is emailed to the administrator that is specified in the Email Notification screen.
   - **Block Source IP**. When a port is scanned, the IP address of the PC or device that scans the port is blocked for the duration that you specify in the Seconds field. The default setting is 300 seconds.

4. Click **Apply** to save your settings.

Note: Traffic that passes on the UTM's VLANs and on the secondary IP addresses that you have configured on the LAN Multi-homing screen (see *Configure Multihome LAN IPs on the Default VLAN* on page 104) is also scanned by the IPS.

When you enable the IPS, the default IPS configuration goes into effect. The default IPS configuration is the configuration that the Advanced screen returns to when you click the factory default reset button.

➢ **To modify the default IPS configuration:**

1. Select **Network Security > IPS > Advanced**. The Advanced screen displays. This screen displays sections for the different categories of attacks such as Web, Mail, Databases, and so on. The Action column shows the default settings (Alert or Drop).
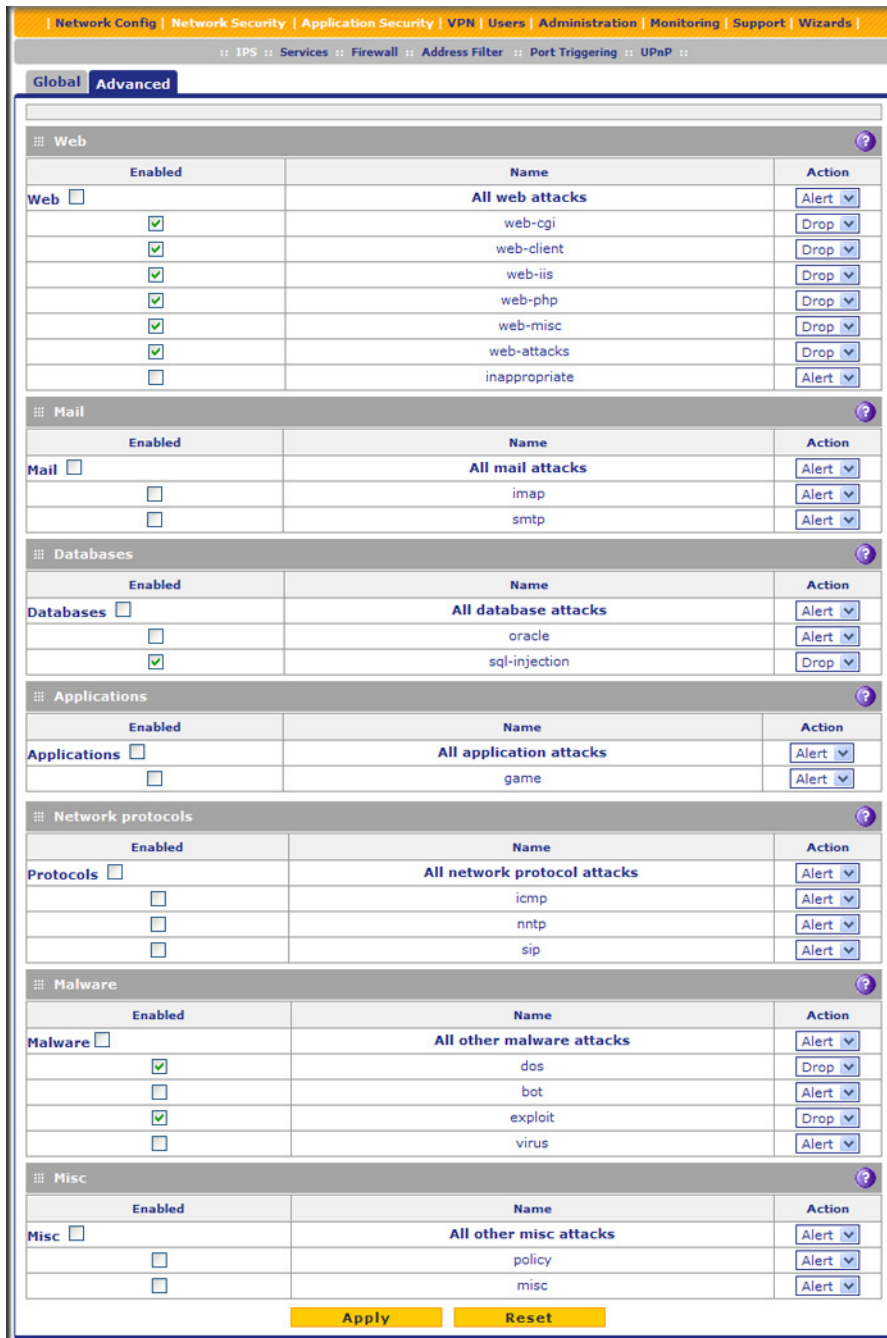
Figure 102.

2. In the Enabled column for each section, either select individual attacks by selecting the check boxes to the left of the names, or select all attacks for that category by selecting the top leftmost check box to the left of All web attacks.

3. In the Action column for each section, either select the actions for individual attacks by making selections from the drop-down lists to the right of the names, or select a global action for all attacks for that category by making a selection from the top drop-down list. Some of the less familiar web and miscellaneous attacks are explained in the following table.

   The drop-down lists let you select one of the following actions:

   • **Alert**. When an attack occurs, an alert is logged but the traffic that carries the attack is not dropped.

   • **Drop**. The traffic that carries the attack is dropped, and an alert is logged.

4. Click **Apply** to save your settings.

Table 37. IPS: uncommon attack names

Attack Name	Description
Web	
web-misc	Detects some specific web attack tools, such as the fingerprinting tool and the password-cracking tool.
web-attacks	Detects the web attacks that cannot be placed under other web categories, such as DoS and overflow attacks against specific web services. These web services include IMail Web Calendaring, ZixForum, ScozNet, ScozNews, and other services.
inappropriate	Detects traffic that involves visiting pornographic websites.
Misc	
policy	Detects traffic that violates common policies, such as traffic that flows because of certain network installer applications, and traffic that flows when Google SafeSearch is turned off.
misc	Detects the web attacks that cannot be placed in other categories, such as attacks specifically against SNMP or DNS.

> **Note:** To ensure that alerts are emailed to an administrator, you need to configure the email notification server (see *Configure the Email Notification Server* on page 422) and the IPS alerts (see *Configure and Activate Update Failure and Attack Alerts* on page 429).

Content Filtering and Optimizing Scans 6

This chapter describes how to apply the content-filtering features of the UTM and how to optimize scans to protect your network. This chapter contains the following sections:

- *About Content Filtering and Scans*
- *Configure Email Protection*
- *Configure Web and Services Protection*
- *Set Web Access Exception Rules*
- *Set Scanning Exclusions*

About Content Filtering and Scans

The UTM provides very extensive web content and email content-filtering options, web browsing activity reporting, email antivirus and antispam options, and instant alerts via email. You can establish restricted web access policies that are based on the time of day, web addresses, and web address keywords. You can also block Internet access by applications and services, such as instant messaging and peer-to-peer file-sharing clients.

Note: Traffic that passes on the UTM's VLANs and on the secondary IP addresses that you have configured on the LAN Multi-homing screen (see *Configure Multihome LAN IPs on the Default VLAN* on page 104) is also scanned for content and malware threats.

Note: For information about how to monitor blocked content and malware threats in real time, see *Monitor Real-Time Traffic, Security, and Statistics* on page 433. For information about how to view blocked content and malware threats in the logs, see *Query the Logs* on page 460.

> **Note:** The UTM9S can quarantine spam and malware only if you have
> integrated a ReadyNAS (see *Connect to a ReadyNAS* on page 415)
> and configured the quarantine settings (see *Configure the
> Quarantine Settings* on page 416).

Default Email and Web Scan Settings

For most network environments, the default scan settings and actions that are shown in the
following table work well, but you can adjust these to the needs of your specific environment.

Table 38. Default email and web scan settings

Scan type	Default scan setting	Default action (if applicable)
Email server protocols		
SMTP	Enabled	Block infected email
POP3	Enabled	Delete attachment if infected
IMAP	Enabled	Delete attachment if infected
Web server protocols[a]		
HTTP	Enabled	Delete file if malware threat detected
HTTPS	Disabled	No action (scan disabled)
FTP	Enabled	Delete file if malware threat detected
Instant messaging services		
Google Talk	Allowed	
ICQ	Allowed	
mIRC	Allowed	
MSN Messenger	Allowed	
QQ	Allowed	
Yahoo Messenger	Allowed	
Peer-to-peer (P2) services		
BitTorrent	Allowed	
eDonkey	Allowed	
Gnutella	Allowed	

Table 38. Default email and web scan settings (continued)

Scan type	Default scan setting	Default action (if applicable)
Media applications		
iTunes (Music Store, update)	Allowed	
QuickTime (Update)	Allowed	
Real Player (Guide)	Allowed	
Rhapsody (Guide, Music Store)	Allowed	
Winamp (Internet Radio/TV)	Allowed	
Tools		
Alexa Toolbar	Allowed	
GoToMyPC	Allowed	
Weatherbug	Allowed	
Yahoo Toolbar	Allowed	
SSL Handshaking to Websites		
Note: SSL handshaking is supported on the UTM9S only.		
Facebook	Allowed	
Web objects		
Embedded Objects (ActiveX/Java/Flash	Allowed	
Javascript	Allowed	
Proxy	Allowed	
Cookies	Allowed	
Web content categories		
Commerce	Allowed	
Drugs and Violence	Blocked	
Education	Allowed with the exception of School Cheating	
Gaming	Blocked	
Inactive Sites	Allowed	
Internet Communication and Search	Allowed with the exception of Anonymizers	
Leisure and News	Allowed	
Malicious	Blocked	

Content Filtering and Optimizing Scans

Table 38. Default email and web scan settings (continued)

Scan type	Default scan setting	Default action (if applicable)
Politics and Religion	Allowed	
Sexual Content	Blocked	
Technology	Allowed	

a. Files or messages that are larger than 2048 KB are skipped by default.

Configure Email Protection

The UTM lets you configure the following settings to protect the network's email communication:

- The email protocols that are scanned for malware threats
- Actions that are taken when infected emails are detected
- The maximum file sizes that are scanned
- Keywords, file types, and file names in emails that are filtered to block objectionable or high-risk content
- Customer notifications and email alerts that are sent when events are detected
- Rules and policies for spam detection

Customize Email Protocol Scan Settings

➢ **To configure the email protocols and ports to scan:**

1. Select **Application Security > Services**. The Services screen displays. (The following figure shows the upper part of the Services screen only.)
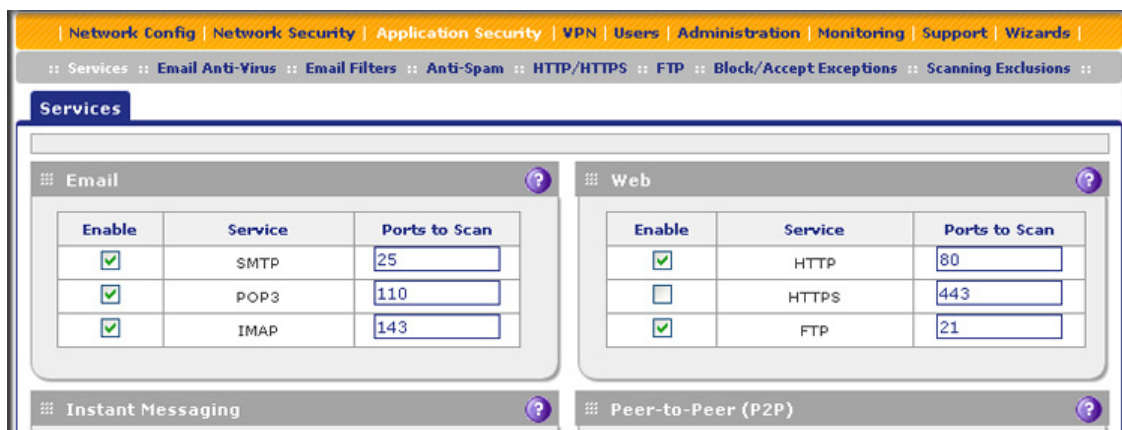
Figure 103.

2. In the Email section of the screen, select the protocols to scan by selecting the **Enable** check boxes, and enter the port numbers if different from the default port numbers:

   - **SMTP**. Simple Mail Transfer Protocol (SMTP) scanning is enabled by default on port 25.

   - **POP3**. Post Office Protocol 3 (POP3) scanning is enabled by default on port 110.

   - **IMAP**. Internet Message Access Protocol (IMAP) scanning is enabled by default on port 143.

3. If a protocol uses a port other than the standard service port (for example, port 25 for SMTP), enter this nonstandard port in the Ports to Scan field. For example, if the SMTP service on your network uses both port 25 and port 2525, enter both port numbers in the Ports to Scan field and separate them by a comma.

   The following protocols are not supported by the UTM:

   - SMTP over SSL using port number 465
   - POP3 over SSL using port number 995
   - IMAP over SSL using port number 993

4. Click **Apply** to save your settings.

Customize Email Antivirus and Notification Settings

Whether or not the UTM detects an email virus, you can configure it to take a variety of actions (some of the default actions are listed in *Table 38* on page 176) and send notifications, emails, or both to the end users.

➢ **To configure the email antivirus settings:**

1. Select **Application Security > Email Anti-Virus**. The Email Anti-Virus screen displays:

Figure 104.

2. Enter the settings as explained in the following table:

Table 39. Email Anti-Virus screen settings

Setting	Description
Action	
SMTP	From the SMTP drop-down list, select one of the following actions to be taken when an infected email is detected: • **Block infected email**. This is the default setting. The email is blocked, and a log entry is created. • **Delete attachment**. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The email is not blocked, and the attachment is not deleted. • **Quarantine attachment** (UTM9S only). The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176). • **Quarantine infected email** (UTM9S only). The email is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176).
POP3	From the POP3 drop-down list, select one of the following actions to be taken when an infected email is detected: • **Delete attachment**. This is the default setting. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The email is not blocked, and the attachment is not deleted. • **Quarantine attachment** (UTM9S only). The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176).
IMAP	From the IMAP drop-down list, select one of the following actions to be taken when an infected email is detected: • **Delete attachment**. This is the default setting. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The email is not blocked, and the attachment is not deleted. • **Quarantine attachment** (UTM9S only). The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176).
Scan Exceptions	
The default maximum size of the email message that is scanned is 2048 KB, but you can define a maximum size of up to 10240 KB. However, setting the maximum size to a high value might affect the UTM's performance (see *Performance Management* on page 389). From the drop-down list, select one of the following actions to be taken when the file or message exceeds the maximum size: • **Skip**. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • **Block**. The file is blocked and does not reach the end user.	

Table 39. Email Anti-Virus screen settings (continued)

Setting	Description
Notification Settings	
Insert Warning into Email Subject (SMTP)	For SMTP email messages, select this check box to insert a warning into the email subject line: • **Malware Found**. If a malware threat is found, a [MALWARE INFECTED] message is inserted. You can change this default message. • **No Malware Found**. If no malware threat is found, a [MALWARE FREE] message is inserted. You can change this default message. By default, this check box is cleared, and no warnings are inserted.
Append Safe Stamp (SMTP and POP3)	For SMTP and POP3 email messages, select this check box to insert a default safe stamp message at the end of an email. The safe stamp insertion serves as a security confirmation to the end user. You can change the default message. By default, this check box is cleared, and no safe stamp is inserted.
Append Warning if Attachment Exceeds Scan Size Limit (SMTP and POP3)	Select this check box to append a default warning message to an email if the message or an attachment to the message exceeds the scan size limit. The warning message informs the end user that the attachment was skipped and might not be safe to open. You can change the default message. By default, this check box is selected, and a warning message is appended to the email.
Replace Infected Attachments with the Following Warning Message	Select this check box to replace an email that is infected with a default warning message. The warning message informs the end user about the name of the malware threat. You can change the default message to include the action that the UTM has taken (see the following note). By default, this check box is selected, and a warning message replaces an infected email. **Note:** Make sure that you keep the %VIRUSINFO% metaword in a message to enable the UTM to insert the correct malware information. The following is a sample message in which the %VIRUSINFO% metaword is replaced with the Trojan.Cyxorp virus: This attachment contains malware: File 1.exe contains malware Trojan.Cyxorp Action: Delete.
Email Alert Settings	
Note: Ensure that the email notification server (see *Configure the Email Notification Server* on page 422) is configured before you specify the email alert settings.	
Send alert to	In addition to inserting a warning message to replace an infected email, you can configure the UTM to send a notification email to the sender, the recipient, or both by selecting the corresponding check box or check boxes. By default, both check boxes are cleared, and no notification email is sent.

Table 39. Email Anti-Virus screen settings (continued)

Setting	Description
Subject	The default subject line for the notification email is *Malware detected!* You can change this subject line.
Message	The warning message informs the sender, the recipient, or both about the name of the malware threat. You can change the default message to include more information. **Note:** Make sure that you keep the %VIRUSINFO% metaword in a message to enable the UTM to insert the correct malware information. In addition to the %VIRUSINFO% metaword, you can insert the following metawords in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.

3. Click **Apply** to save your settings.

Email Content Filtering

The UTM provides several options to filter unwanted content from emails. You can filter content from emails based on keywords in the subject line, file type of the attachment, and file name of the attachment. You can also set an action to perform on emails with password-protected attachments.

Several types of email blocking are available:

- **Keyword blocking**. You can specify words that, should they appear in the email subject line, cause that email to be blocked by the UTM.

- **Password-protected attachments**. You can block emails based on password-protected attachments such as .zip or .rar attachments.

- **File extension blocking**. You can block emails based on the extensions of attached files. Such files can include executable files, audio and video files, and compressed files.

- **File name blocking**. You can block emails based on the names of attached files. Such names can include, for example, names of known malware threat such as the Netsky worm (which usually arrives as netsky.exe).

➢ **To configure email content filtering:**

1. Select **Application Security > Email Filters**. The Email Filters screen displays:
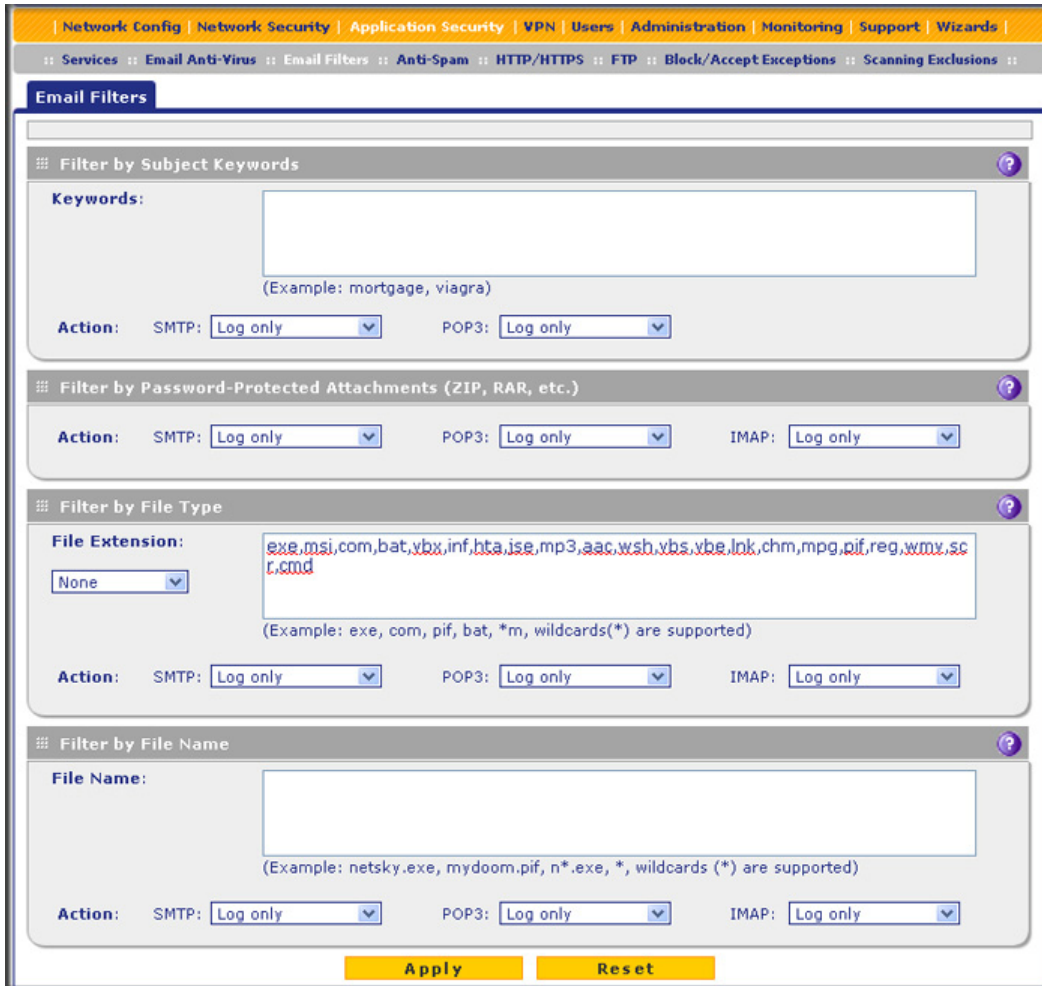
Figure 105.

2. Enter the settings as explained in the following table:

Table 40. Email Filters screen settings

Setting	Description
Filter by Subject Keywords	
Keywords	Enter keywords that should be detected in the email subject line. Use commas to separate different keywords. The total maximum length of this field is 2048 characters, excluding duplicate words and delimiter commas.

Table 40. Email Filters screen settings (continued)

Setting		Description
Action	SMTP	From the SMTP drop-down list, select one of the following actions when a keyword that is defined in the Keywords field is detected: • **Block email**. The email is blocked, and a log entry is created. • **Log only**. This is the default setting. Only a log entry is created. The email is not blocked.
	POP3	From the POP3 drop-down list, select one of the following actions when a keyword that is defined in the Keywords field is detected: • **Block email**. The email is blocked, and a log entry is created. • **Log only**. This is the default setting. Only a log entry is created. The email is not blocked.
Filter by Password-Protected Attachments (ZIP, RAR, etc.)		
Action	SMTP	From the SMTP drop-down list, select one of the following actions when a password-protected attachment to an email is detected: • **Block email**. The email is blocked, and a log entry is created. • **Delete attachment**. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. This is the default setting. Only a log entry is created. The email is not blocked, and the attachment is not deleted.
	POP3	From the POP3 drop-down list, select one of the following actions when a password-protected attachment to an email is detected: • **Delete attachment**. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. This is the default setting. Only a log entry is created. The email is not blocked, and the attachment is not deleted.
	IMAP	From the IMAP drop-down list, select one of the following actions when a password-protected attachment to an email is detected: • **Delete attachment**. The email is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. This is the default setting. Only a log entry is created. The email is not blocked, and the attachment is not deleted.
Filter by File Type		
File Extension		By default, the File Extension field lists the most common file extensions. You can manually add or delete extensions. Use commas to separate different extensions. You can enter a maximum of 40 file extensions. The maximum total length of this field, excluding the delimiter commas, is 160 characters. You can also use the drop-down list to add predefined file extensions from a specific category to the File Extension field: • **None**. No file extensions are added to the File Extension field. This is the default setting. • **Executables**. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field. • **Audio/Video**. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field. • **Compressed Files**. Compressed file extensions (zip, rar, gz, tar, and bz2) added to the File Extension field.

Table 40. Email Filters screen settings (continued)

Setting		Description
Action	SMTP	From the drop-down list, select an action to be taken when an email attachment with a file extension that is defined in the File Extension field is detected. The drop-down list selections and defaults are the same as the ones for the Filter by Password-Protected Attachments (ZIP, RAR, etc.) section that is described earlier in this table.
	POP3	
	IMAP	
Filter by File Name		
File Name		Enter the file names that are detected. Use commas to separate multiple file names. For example, to block the Netsky worm (which normally arrives as netsky.exe), enter **netsky.exe**.
Action	SMTP	From the drop-down list, select an action to be taken when an email attachment with a name that is defined in the File Name field is detected. The drop-down list selections and defaults are the same as the ones for the Filter by Password-Protected Attachments (ZIP, RAR, etc.) section that is described earlier in this table.
	POP3	
	IMAP	

3. Click **Apply** to save your settings.

Protect Against Email Spam

The UTM integrates multiple antispam technologies to provide comprehensive protection against unwanted email. You can enable all or a combination of these antispam technologies. The UTM implements these spam-prevention technologies in the following order:

1. Whitelist. Emails from the specified sources or to the specified recipients are not considered spam and are accepted.

2. Blacklist. Emails from the specified sources are considered spam and are blocked.

3. Real-time blacklist. Emails from known spam sources that are collected by blacklist providers are blocked.

4. Distributed spam analysis. Emails that are detected as spam by the NETGEAR Spam Classification Center are either tagged or blocked.

This order of implementation ensures the optimum balance between spam prevention and system performance. For example, if an email originates from a whitelisted source, the UTM delivers the email immediately to its destination inbox without implementing the other spam-prevention technologies, thereby speeding up mail delivery and conserving the UTM system resources. However, regardless of whether or not an email is whitelisted, the email is still scanned by the UTM's antimalware engines.

You can configure these antispam options in conjunction with content filtering to optimize blocking of unwanted mails.

Note: Emails that are processed through the UTM over an authenticated email connection between a client and a mail server are not checked for spam.

Note: An email that has been checked for spam by the UTM contains an X-STM-SMTP (for SMTP emails) or X-STM-POP3 (for POP-3 emails) tag in its header.

Set Up the Whitelist and Blacklist

You can specify that emails are accepted or blocked based on the originating IP address, domain, and email address by setting up the whitelist and blacklist. You can also specify that emails are accepted based on the destination domain and email address.

The whitelist ensures that emails from listed (that is, trusted) sources and recipients are not mistakenly tagged as spam. Emails going to and from these sources and recipients are delivered to their destinations immediately, without being scanned by the antispam engines. This can help to speed up the system and network performance. The blacklist, on the other hand, lists sources from which all email messages are blocked. You can enter up to 200 entries per list, separated by commas.

Note: The whitelist takes precedence over the blacklist, which means that if an email source is on both the blacklist and the whitelist, the email is not scanned by the antispam engines.

➢ **To configure the whitelist and blacklist:**

1. Select **Application Security > Anti-Spam**. The Anti-Spam submenu tabs display, with the Whitelist/Blacklist screen in view.

Figure 106.

2. Enter the settings as explained in the following table:

Table 41. Whitelist/Blacklist screen settings

Setting	Description
Sender IP Address (SMTP Only)	
Whitelist	Enter the source IP addresses from which emails can be trusted.
Blacklist	Enter the source IP addresses from which emails are blocked.
Click **Apply** to save your settings, or click **Reset** to clear all entries from these fields.	
Sender Domain (SMTP Only)	
Whitelist	Enter the email domains from which emails can be trusted.
Blacklist	Enter the sender email domains from which emails are blocked.
Click **Apply** to save your settings, or click **Reset** to clear all entries from these fields.	
Sender Email Address (SMTP Only)	
Whitelist	Enter the email addresses from which emails can be trusted.
Blacklist	Enter the email addresses from which emails are blocked.
Click **Apply** to save your settings, or click **Reset** to clear all entries from these fields.	
Recipients Domain (SMTP Only)	
Whitelist	Enter the sender email domains of the recipients to which emails can be safely delivered.
Click **Apply** to save your settings, or click **Reset** to clear all entries from this field.	
Recipients Email Address (SMTP Only)	
Whitelist	Enter the email addresses of the recipients to which emails can be safely delivered.
Click **Apply** to save your settings, or click **Reset** to clear all entries from this field.	

Note: In the fields of the Whitelist/Blacklist screen, use commas to separate multiple entries. For IP addresses, use a hyphen to indicate a range (for example, 192.168.32.2-192.168.32.8).

Configure the Real-Time Blacklist

Blacklist providers are organizations that collect IP addresses of verified open SMTP relays that might be used by spammers as media for sending spam. These known spam relays are compiled by blacklist providers and are made available to the public in the form of real-time blacklists (RBLs). By accessing these RBLs, the UTM can block spam originating from known spam sources.

By default, the UTM comes with three pre-defined blacklist providers: Dsbl, Spamhaus, and Spamcop. There is no limit to the number of blacklist providers that you can add to the RBL sources.

➢ **To enable the real-time blacklist:**

1. Select **Application Security > Anti-Spam > Real-time Blacklist**. The Real-Time Blacklist screen displays:
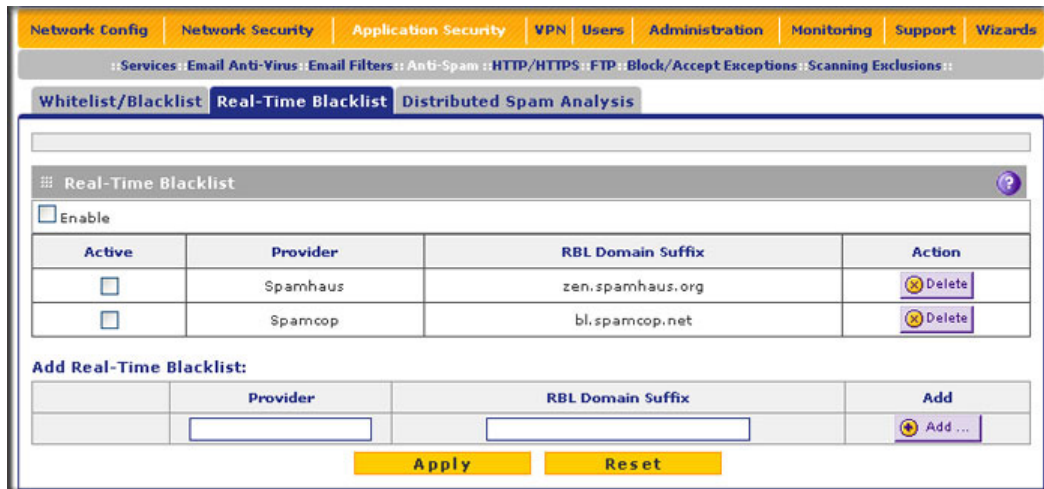
Figure 107.

2. To enable the Real-Time Blacklist function, select the **Enable** check box.

3. Select the **Active** check boxes to the left of the default blacklist providers (Spamhaus, and Spamcop) that you want to activate.

4. Click **Apply** to save your settings.

➢ **To add a blacklist provider to the real-time blacklist:**

1. In the Add Real-Time Blacklist section, add the following information:
   • In the Provider field, add the name of the blacklist provider.
   • In the RBL Domain Suffix field, enter the domain suffix of the blacklist provider.

2. Click the **Add** table button in the Add column. The new blacklist provider is added to the real-time blacklist, and it is disabled by default.

➢ **To delete a blacklist provider from the real-time blacklist:**

1. In the real-time blacklist, click the **Delete** table button next to the blacklist provider that you want to delete.

2. Click **Apply** to save your settings.

Configure Distributed Spam Analysis

Spam, phishing, and other email-borne threats consist of millions of messages intentionally composed differently to evade commonly used filters. Nonetheless, all messages within the same outbreak share at least one unique, identifiable value that can be used to distinguish the outbreak.

With distributed spam analysis, message patterns are extracted from the message envelope, headers, and body with no reference to the content itself. Pattern analysis can then be applied to identify outbreaks in any language, message format, or encoding type. Message patterns can be divided into distribution patterns and structure patterns. Distribution patterns determine if the message is legitimate or a potential threat through analysis of the way it is distributed to the recipients, while structure patterns determine the volume of the distribution.

The UTM uses a distributed spam analysis architecture to determine whether or not an email is spam for SMTP and POP3 emails. Any email that is identified as spam is tagged as spam (an option for both SMTP and POP3) or blocked (an option possible only for SMTP).

Note: Unlike other scans, you do not need to configure the spam score because the NETGEAR Spam Classification Center performs the scoring automatically as long as the UTM is connected to the Internet. However, this does mean that the UTM needs to be connected to the Internet for the spam analysis to be performed correctly.

Note: The UTM transfers normal email (also referred to as HAM) to the users and marks this email as *Pass* in the traffic logs.

➢ **To configure distributed spam analysis and the antispam engine settings:**

1. Select **Application Security > Anti-Spam > Distributed Spam Analysis**. The Distributed Spam Analysis screen displays:
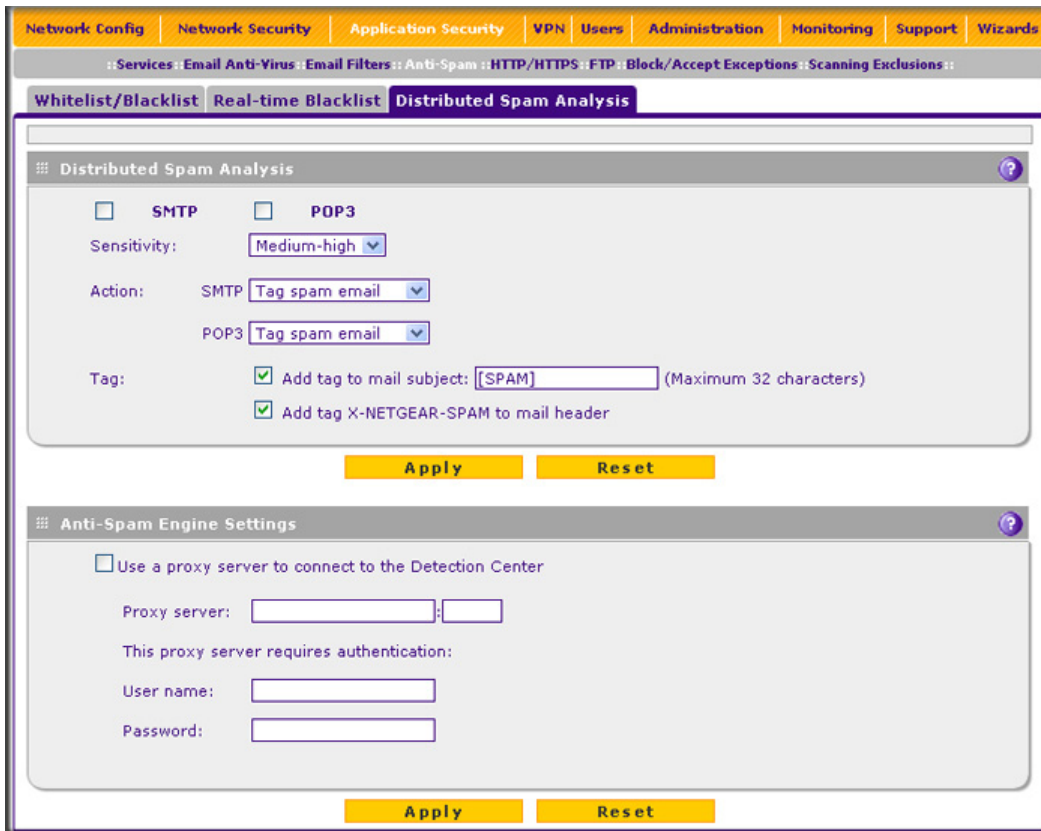
Figure 108.

The UTM9S also has a Send Quarantine Spam Report section at the bottom of the Distributed Spam Analysis screen:
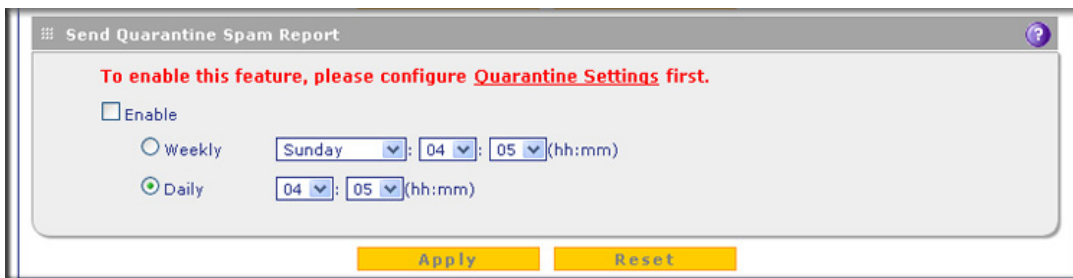
Figure 109.

2. Enter the settings as explained in the following table:

Table 42. Distributed Spam Analysis screen settings

Setting	Description
Distributed Spam Analysis	
SMTP	Select the **SMTP** check box to enable distributed spam analysis for the SMTP protocol. (You can enable distributed spam analysis for both SMTP and POP3.)

Table 42. Distributed Spam Analysis screen settings (continued)

Setting	Description	
POP3	Select the **POP3** check box to enable distributed spam analysis for the POP3 protocol. (You can enable distributed spam analysis for both SMTP and POP3.)	
Sensitivity	From the Sensitivity drop-down list, select the level of sensitivity for the antispam engine that performs the analysis: **Low**. **Medium-Low**. **Medium**. **Medium High**. This is the default setting. **High**. **Note:** A low sensitivity allows more emails to pass through but increases the risk of spam messages. A high sensitivity allows fewer emails to pass through but diminishes the risk of spam messages.	
Action	SMTP	From the SMTP drop-down list, select the action that is taken when spam is detected by the antispam engine: • **Tag spam email**. This is the default setting. The email is tagged as spam, and a log entry is created. • **Block spam email**. The email is blocked, and a log entry is created. • **Quarantine spam email** (UTM9S only). The email is quarantined on a ReadyNAS, and a log entry is created (see the Note on page 176).
	POP3	The only option is to tag spam email.
Tag	Add tag to mail subject	When Tag spam email is selected from the Action drop-down list (see the preceding explanation in this table), select this check box to add a tag to the email subject line. The default tag is [SPAM], but you can customize this tag. The default setting is to add the default tag to the subject line.
	Add tag X-NETGEAR-SPAM to mail header	When Tag spam email is selected from the Action drop-down list (see the explanation earlier in this table), select this check box to add the X-NETGEAR-SPAM tag to the email header. The default setting is to add the default tag to the email header.
Anti-Spam Engine Settings		
Use a proxy server to connect to the Detection Center	Select this check box if the UTM connects to the Netgear Spam Classification Center (also referred to as the Detection Center) over a proxy server. Then specify the following information.	
	Proxy server	The IP address and the port number of the proxy server.
	User name	Optional: The user name for proxy server authentication.
	Password	Optional: The password for proxy server authentication.

Table 42. Distributed Spam Analysis screen settings (continued)

Setting	Description
Send Quarantine Spam Report **Note:** This option is supported on the UTM9S only (see the Note on page 176).	
Enable	To enable the UTM9S to automatically email a spam report, select the **Enable** check box, and specify when the reports should be sent.
	Specify when the reports should be sent by selecting one of the following radio buttons: • **Weekly**. From the drop-down lists, specify the day, hour, and minute that the report should be sent. • **Daily**. From the drop-down lists, specify the hour and minute that the report should be sent.

3. Click **Apply** to save your settings. The Distributed Spam Analysis section and the Anti-Spam Engine Settings section each have their own Apply and Reset buttons to enable you to make changes to these sections separately.

Configure Web and Services Protection

The UTM lets you configure the following settings to protect the network's Internet and web services communication:

- The web protocols, instant messaging applications, peer-to-peer applications, media applications, and web tools that are scanned for malware threats
- Actions that are taken when infected web files or objects are detected
- The maximum file sizes that are scanned
- Web objects that are blocked
- Web categories, keywords, and file types that are filtered to block objectionable or high-risk content
- Domains and URLs that are blocked for objectionable or high-risk content
- Customer notifications and email alerts that are sent when events are detected
- Schedules that determine when content filtering is active

Customize Web Protocol Scan Settings and Services (Web Applications)

You can specify the web protocols (HTTP, HTTPS, and FTP) that are scanned for malware threats and the instant messaging applications, peer-to-peer applications, media applications, and web tools that are allowed or blocked.

Scanning all protocols enhances network security but might affect the performance of the UTM. For an optimum balance between security and performance, enable scanning of only the most commonly used protocols on your network. For example, you can scan FTP and

HTTP, but not HTTPS (if this last protocol is not often used). For more information about performance, see *Performance Management* on page 389.

➢ **To configure the web protocols, ports, and applications to scan:**

1. Select **Application Security > Services**. The Services screen displays:
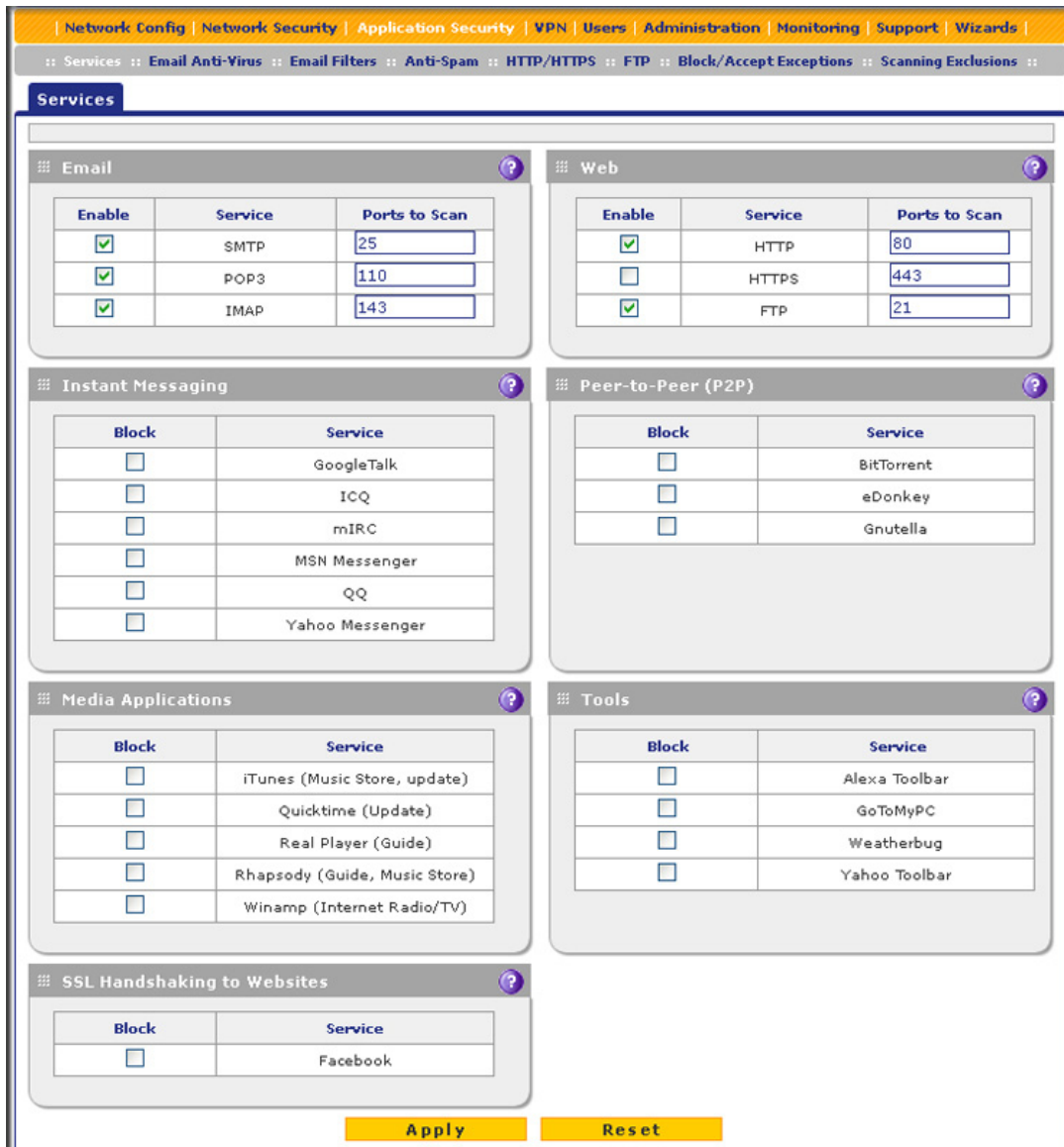
Figure 110.

2. Enter the settings as explained in the following table.

Content Filtering and Optimizing Scans

195

> **Note:** For information about email protocols and ports, see *Customize Email Protocol Scan Settings* on page 178.

Table 43. Services screen settings

Setting	Description
Web	
HTTP	Select the **HTTP** check box to enable Hypertext Transfer Protocol (HTTP) scanning. This service is enabled by default and uses default port 80.
HTTPS	Select the **HTTPS** check box to enable Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). This service is disabled by default. The default port is 443.
FTP	Select the **FTP** check box to enable File Transfer Protocol (FTP). This service is enabled by default and uses default port 21. You cannot change the default port in the corresponding Ports to Scan field.
Note: If a protocol uses a port other than the standard service port (for example, port 80 for HTTP), enter this nonstandard port in the Ports to Scan field. For example, if the HTTP service on your network uses both port 80 and port 8080, enter both port numbers in the Ports to Scan field and separate them by a comma.	
Instant Messaging	
Google Talk	Scanning of these instant messaging services is disabled by default. To enable any of these services, select the corresponding check box.
ICQ	
mIRC	
MSN Messenger	**Note:** For instant messaging services, the following services can be blocked: logging in, sharing files, sharing video, sharing audio, and text messaging.
QQ	
Yahoo Messenger	
Peer-to-Peer (P2P)	
BitTorrent	Scanning of these file-sharing applications is disabled by default. To enable any of these services, select the corresponding check box.
eDonkey	
Gnutella	

Table 43. Services screen settings (continued)

Setting	Description
Media Applications	
iTunes (Music Store, update)	Scanning of these media applications is disabled by default. To enable any of these applications, select the corresponding check box.
QuickTime (Update)	
Real Player (Guide)	
Rhapsody (Guide, Music Store)	
Winamp (Internet Radio/TV)	
SSL Handshaking to Websites **Note:** SSL handshaking is supported on the UTM9S only. (This option is not shown in the previous figure.)	
Facebook	Scanning of Facebook is disabled by default. To enable it, select the corresponding check box.
Tools	
Alexa Toolbar	Scanning of these tools is disabled by default. To enable any of these tools, select the corresponding check box.
GoToMyPC	
Weatherbug	
Yahoo Toolbar	

3. Click **Apply** to save your settings.

Configure Web Malware Scans

Whether or not the UTM detects web-based malware threats, you can configure it to take a variety of actions (some of the default actions are listed in *Table 38* on page 176) and send notifications, emails, or both to the end users.

➢ **To configure the web-based malware settings:**

1. Select **Application Security > HTTP/HTTPS**. The HTTP/HTTPS submenu tabs display, with the Malware Scan screen in view:
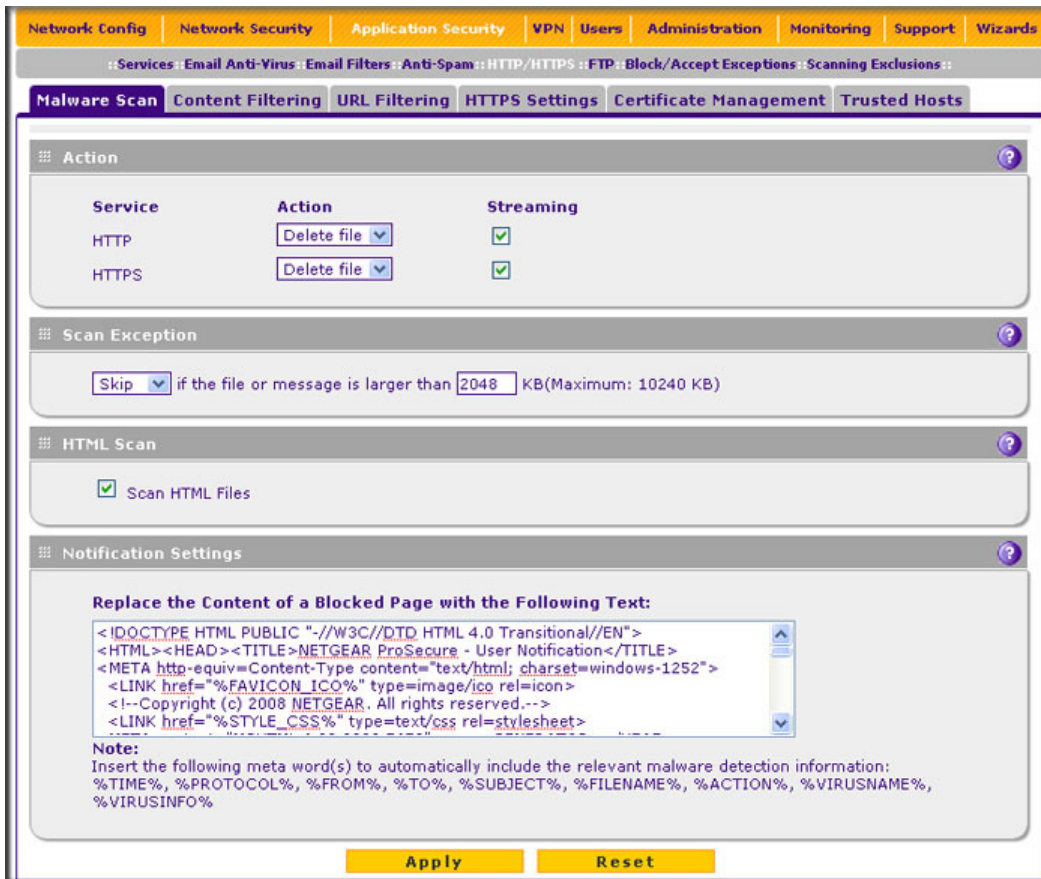
Figure 111.

2. Enter the settings as explained in the following table:

Table 44. Malware Scan screen settings

Setting		Description
Action		
HTTP and HTTPS	Action	From the HTTP or HTTPS drop-down list, specify one of the following actions to be taken when an infected web file or object is detected: • **Delete file**. This is the default setting. The web file or object is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The web file or object is not deleted. • **Quarantine file** (UTM9S only). The web file or object is quarantined, and a log entry is created (see the Note on page 176).
	Streaming	Select the **Streaming** check box to enable streaming of partially downloaded and scanned HTTP or HTTPS file parts to the user. This method allows the user to experience more transparent web downloading. Streaming is enabled by default.

Table 44. Malware Scan screen settings (continued)

Setting	Description
Scan Exception	
	The default maximum size of the file or object that is scanned is 2048 KB, but you can define a maximum size of up to 10240 KB. However, setting the maximum size to a high value might affect the UTM's performance (see *Performance Management* on page 389).
	From the drop-down list, select one of the following actions to be taken when the file or message exceeds the maximum size:
	• **Skip**. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting.
	• **Block**. The file is blocked and does reach the end user.
HTML Scan	
Scan HTML Files	Select this check box to enable scanning of HyperText Markup Language (HTML) files, which is enabled by default.
Notification Settings	
	By default, the content of a web page that is blocked because of a detected malware threat is replaced with the following text, which you can customize:
	NETGEAR ProSecure UTM has detected and stopped malicious code embedded in this web site or web mail, for protecting your computer and network from infection. %VIRUSINFO%
	Note: Make sure that you keep the %VIRUSINFO% metaword in a message to enable the UTM to insert the correct malware information. In addition to the %VIRUSINFO% metaword, you can insert the following metawords in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.

3. Click **Apply** to save your settings.

Configure Web Content Filtering

If you want to restrict access by internal LAN users to certain types of information and objects on the Internet, use the UTM's content filtering and web objects filtering. With the exception of the web content categories that are mentioned in *Default Email and Web Scan Settings* on page 176, all requested traffic from any website is allowed. You can specify a message such as *Blocked by NETGEAR* that is displayed onscreen if a LAN user attempts to access a blocked site (see the Notification Settings section that is described at the bottom of *Table 45* on page 203).

Several types of web content blocking are available:

• **File extension blocking**. You can block files based on their extension. Such files can include executable files, audio and video files, and compressed files.

• **Keyword blocking**. You can specify words that, should they appear in the website name (URL) or in a newsgroup name, cause that site or newsgroup to be blocked by the UTM.

The following are keyword blocking examples:

- If the keyword XXX is specified, the URL www.zzyyqq.com/xxx.html is blocked, as is the newsgroup alt.pictures.XXX.
- If the keyword .com is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- If a period (**.**) is specified as the keyword, all Internet browsing access is blocked.

> **Note:** Wildcards (*) are supported. For example, if www.net*.com is specified, any URL that begins with www.net is blocked, and any URL that ends with .com is blocked.

You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled are blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

> **Note:** The whitelist has priority over the blacklist (for these lists, see *Configure Web URL Filtering* on page 206), and both the whitelist and the blacklist have priority over keyword blocking.

- **Web object blocking**. You can block the following web objects: embedded objects (ActiveX, Java, Flash), proxies, and cookies, and you can disable JavaScripts. Even sites on the whitelist (see *Configure Web URL Filtering* on page 206) are subject to web object blocking when the blocking of a particular web object is enabled.
- **Web category blocking**. You can block entire web categories because their content is undesired, offensive, or not relevant, or simply to reduce traffic.

> **Note:** You can bypass any type of web blocking for trusted hosts by adding the exact matching domain names to the trusted host list (see *Specify Trusted Hosts* on page 218). Access to the domains on the trusted host list is allowed for PCs in the groups for which file extension, keyword, object, or category blocking, or a combination of these types of web blocking has been enabled.

Note: You can bypass any type of web blocking for trusted URLs by adding the URLs to the whitelist (see *Configure Web URL Filtering* on page 206). Access to the URLs on the whitelist is allowed for PCs in the groups for which file extension, keyword, object, or category blocking, or a combination of these types of web blocking has been enabled.

➢ **To configure web content filtering:**

1. Select **Application Security > HTTP/HTTPS > Content Filtering**. The Content Filtering screen displays. Because of the large size of this screen, it is presented in this manual in three figures (the following figure, *Figure 113* on page 202, and *Figure 114* on page 203).
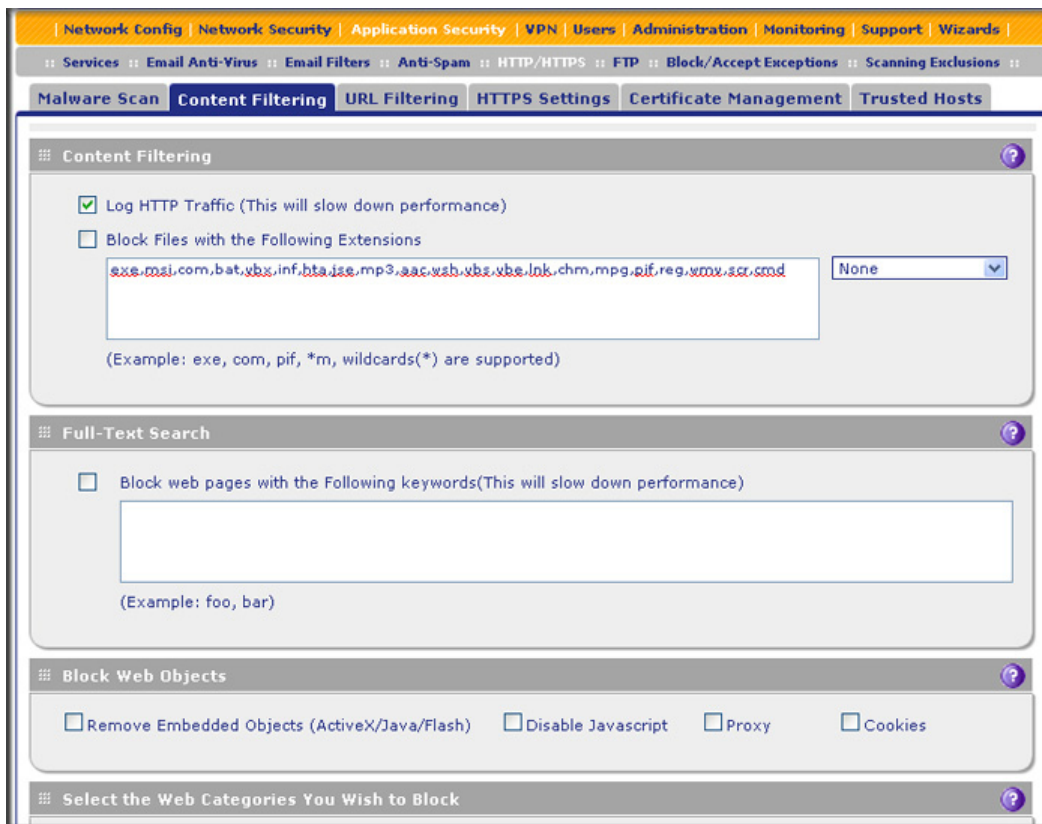
Figure 112. Content filtering, screen 1 of 3

::: Select the Web Categories You Wish to Block

☐ Enable Blocking

Allow All   **Block All**   **Set to Defaults**

☐ **Commerce**
- ■ ☐ Advertisements & Pop-Ups   ■ ☐ Business   ■ ☐ Banking/Finance
- ■ ☐ Real Estate   ■ ☐ Shopping

☐ **Drugs and Violence**
- ■ ☑ Alcohol & Tabacco   ■ ☑ Hate & Intolerance   ■ ☑ Illegal Drugs
- ■ ☑ Tasteless   ■ ☑ Violence   ■ ☑ Weapons

☐ **Education**
- ■ ☐ Education   ■ ☐ Health & Medicine   ■ ☑ School Cheating

☐ **Gaming**
- ■ ☑ Gambling   ■ ☑ Games

☐ **Inactive Sites**
- ■ ☐ Network Errors   ■ ☐ Parked Domain

☐ **Internet Communication and Search**
- ■ ☑ Anonymizers   ■ ☐ Chat   ■ ☐ Forums
- ■ ☐ General   ■ ☐ Image/Photo Sharing   ■ ☐ Instant Messaging
- ■ ☐ Job Search   ■ ☐ Peer-to-Peer   ■ ☐ Private IP Addresses
- ■ ☐ Streaming Media & Downloads   ■ ☐ Search Engines & Portals   ■ ☐ Translators
- ■ ☐ Webmail

☐ **Leisure and News**
- ■ ☐ Arts   ■ ☐ Dating & Personals   ■ ☐ Entertainment
- ■ ☐ Fashion & Beauty   ■ ☐ Greeting Cards   ■ ☐ Leisure & Recreation
- ■ ☐ News   ■ ☐ Non-Profits   ■ ☐ Personal Sites
- ■ ☐ Restaurants & Dining   ■ ☐ Social Networking   ■ ☐ Sports
- ■ ☐ Transportation   ■ ☐ Travel

☐ **Malicious**
- ■ ☑ Botnets   ■ ☑ Criminal Activity   ■ ☑ Hacking
- ■ ☑ Illegal Software   ■ ☑ Malware   ■ ☑ Phishing & Fraud
- ■ ☑ Spam Sites   ■ ☑ Virus Infected/Compromised

☐ **Politics and Religion**
- ■ ☐ Cults   ■ ☐ Government   ■ ☐ Politics
- ■ ☐ Religion

☐ **Sexual Content**
- ■ ☑ Child Abuse Images   ■ ☑ Nudity   ■ ☑ Pornography/Sexually Explicit
- ■ ☑ Sex Education

☐ **Technology**
- ■ ☐ Computers & Technology   ■ ☐ Download Sites   ■ ☐ Information Security

☐ **UnCategorized**
- ■ ☑ UnCategorized

Note:
■ Allowed by Default
■ Blocked by Default

::: Blocked Categories Scheduled Days:

Figure 113. Content filtering, screen 2 of 3
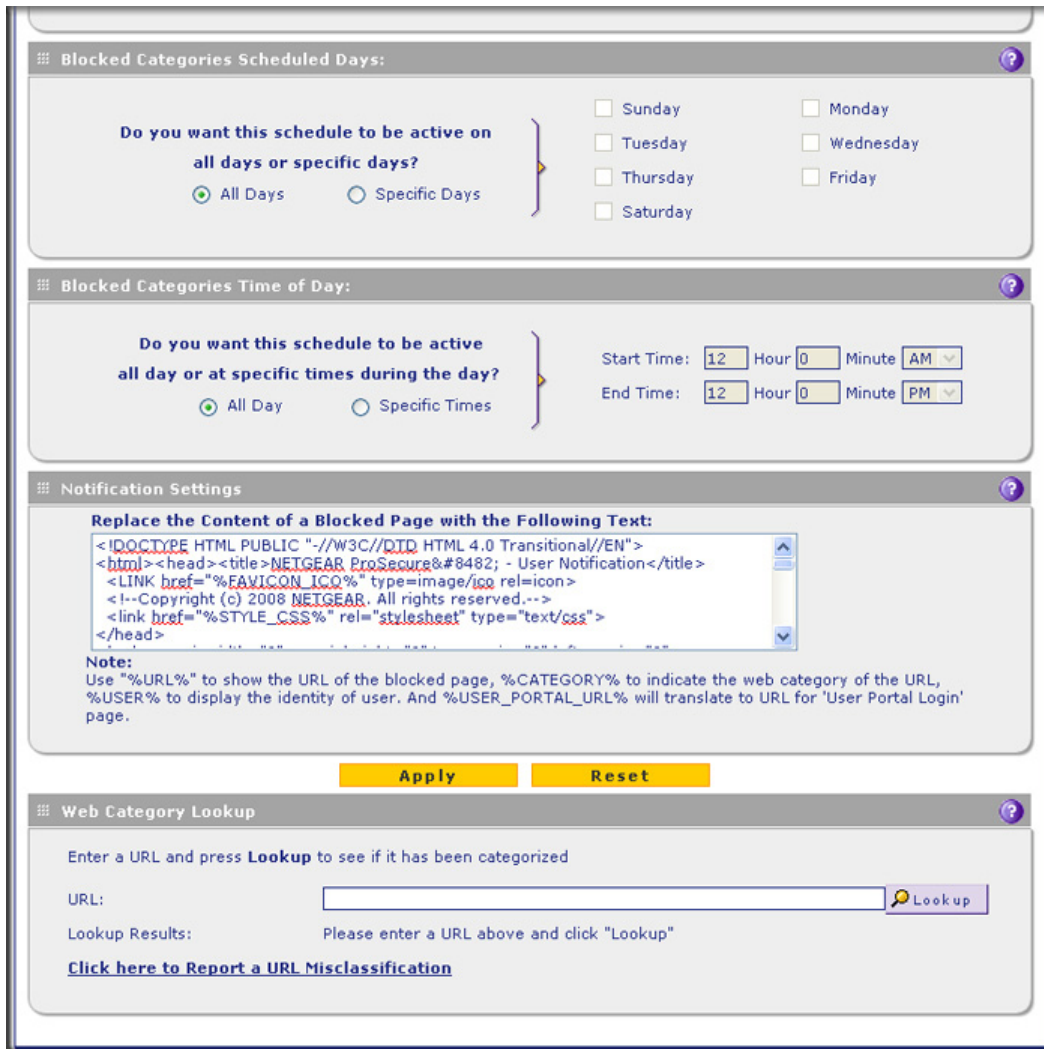
Figure 114. Content filtering, screen 3 of 3
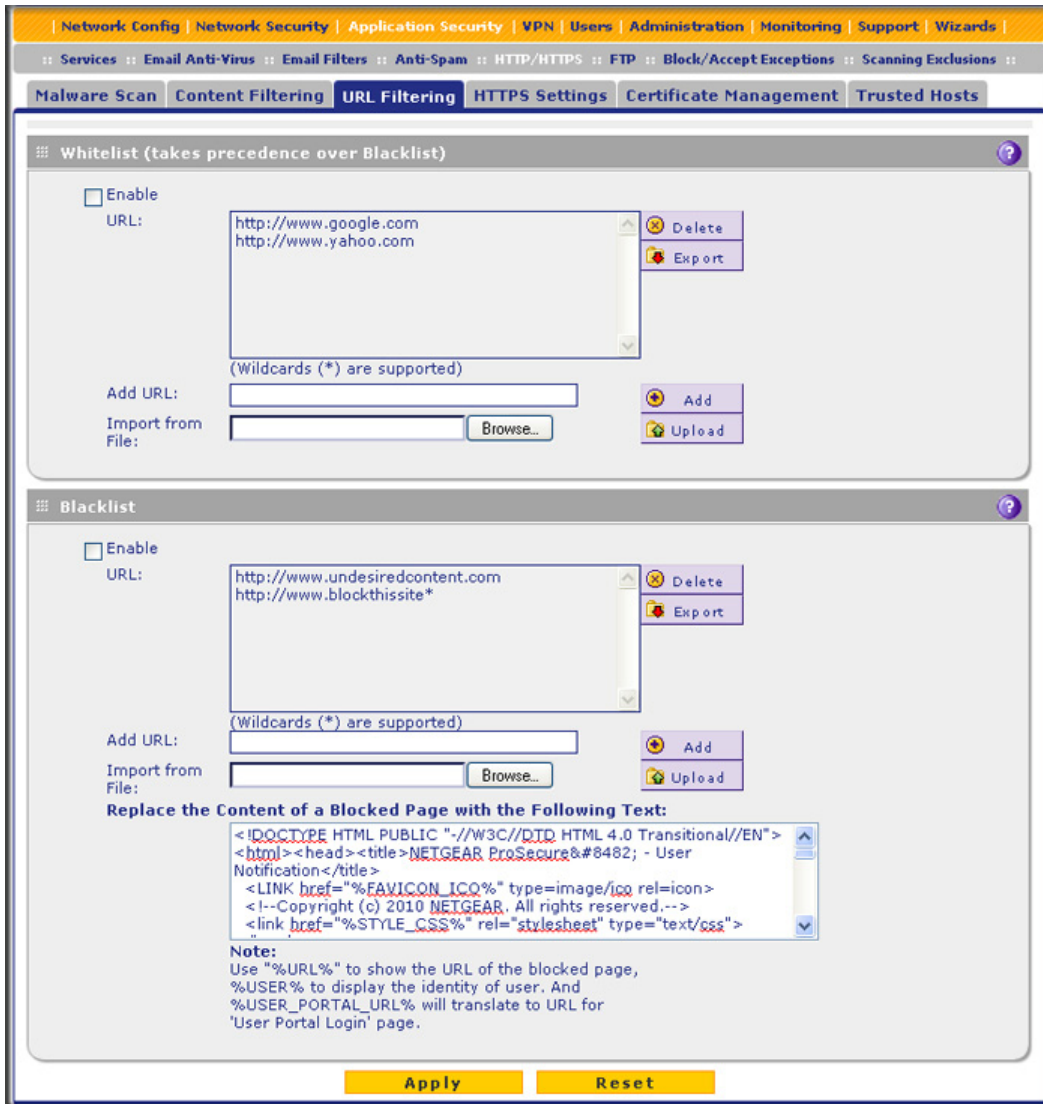
2. Enter the settings as explained in the following table:

Table 45. Content Filtering screen settings

Setting	Description
Content Filtering	
Log HTTP Traffic	Select this check box to log HTTP traffic. For information about how to view the logged traffic, see *Query the Logs* on page 460. By default, HTTP traffic is logged. **Note:** Logging HTTP traffic might affect the UTM's performance (see *Performance Management* on page 389). **Note:** If you want to generate web traffic reports (see *View, Schedule, and Generate Reports* on page 473), you do need to select the Log HTTP Traffic check box.

Table 45. Content Filtering screen settings (continued)

Setting	Description
Block Files with the Following Extensions	By default, the File Extension field lists the most common file extensions. You can manually add or delete extensions. Use commas to separate different extensions. You can enter a maximum of 40 file extensions. The maximum total length of this field, excluding the delimiter commas, is 160 characters. You can also use the drop-down list to add predefined file extensions from a specific category to the File Extension field: • **None**. No file extensions are added to the File Extension field. This is the default setting. • **Executables**. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field. • **Audio/Video**. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field. • **Compressed Files**. Compressed file extensions (zip, rar, gz, tar, and bz2) added to the File Extension field.
Full-Text Search **Note:** Full-text search allows you to block keywords.	
Block web pages with the Following keywords	Select the check box to enable keyword blocking. Then, enter keywords that you want to be blocked. Separate the keywords by a comma. **Note:** Keywords searching and blocking might affect the UTM's performance (see *Performance Management* on page 389).
Block Web Objects Select any or all of the following check boxes:	
Remove Embedded Objects	All embedded objects such as ActiveX, Java, and Flash objects are removed from downloaded web pages. **Note:** Because embedded objects are commonly used on legitimate websites, blocking embedded objects globally might have a negative impact on a user's web browsing experience.
Disable Javascript	JavaScript is disabled on downloaded web pages.
Proxy	All web proxy servers are blocked.
Cookies	All cookies are blocked.

Table 45. Content Filtering screen settings (continued)

Setting	Description
Select the Web Categories You Wish to Block	
	Select the **Enable Blocking** check box to enable blocking of web categories. (By default, this check box is selected.) Select the check boxes of any web categories that you want to block. Use the action buttons at the top of the section in the following way: • **Allow All**. All web categories are allowed. • **Block All**. All web categories are blocked. • **Set to Defaults**. Blocking and allowing of web categories are returned to their default settings. See *Table 38* on page 176 for information about the web categories that are blocked by default. Categories that are preceded by a green square are allowed by default; categories that are preceded by a pink square are blocked by default.
Blocked Categories Scheduled Days	
	Select one of the following radio buttons: • **All Days**. The schedule is in effect all days of the week. • **Specific Days**. The schedule is in effect only on specific days. To the right of the radio buttons, select the check box for each day that you want the schedule to be in effect.
Blocked Categories Time of Day	
	Select one of the following radio buttons: • **All Day**. The schedule is in effect all hours of the selected day or days. • **Specific Times**. The schedule is in effect only on specific hours of the selected day or days. To the right of the radio buttons, fill in the Start Time and End Time fields (Hour, Minute, AM/PM) during which the schedule is in effect.
Notification Settings	
	The UTM replaces the content of a web page that is blocked because of violating content with the following text, which you can customize: Internet Policy has restricted access to this location: %URL% Full-text search found the content to have the keyword: %KEYWORD% Belongs to category : %CATEGORY% Click here to Report a URL Misclassification You are logged in as %USER% Click here to login as another user %USER_PORTAL_URL% **Note:** The text is displayed on the Content Filtering screen with HTML tags. However, when the UTM replaces the content of a blocked web page, the screen displays the notification text in HTML format. **Note:** Make sure that you keep the %URL% and %KEYWORD% metawords in the text to enable the UTM to insert the blocked URL and the keyword that caused the web page to be blocked in the notification text. The %CATEGORY% metaword enables the UTM to insert the category of the blocked URL; the %USER% metaword enables the UTM to insert the user login name; the %USER_PORTAL_URL% metaword enables the UTM to insert the User Portal Login screen.

Table 45. Content Filtering screen settings (continued)

Setting	Description
Web Category Lookup	
URL	Enter a URL to find out if it has been categorized, and if so, in which category. Then click the **lookup** button. If the URL has been categorized, the category displays next to Lookup Results. If the URL appears to be uncategorized, you can submit it to NETGEAR for analysis.
Submit to NETGEAR	To submit an uncategorized URL to NETGEAR for analysis, select the category in which you think that the URL needs to be categorized from the drop-down list. Then click the **Submit** button.

3. Click **Apply** to save your settings.

> **Note:** When the UTM blocks access to a link of a certain blocked web category, the UTM displays an HTML warning screen that includes a link to submit a URL misclassifiation. To submit a misclassified or uncategorized URL to NETGEAR for analysis, click the **Click here to Report a URL Misclassification** link. A second screen opens that allows you to select (from drop-down lists) up to two categories in which you think that the URL could be categorized. Then click the **Submit** button.

Configure Web URL Filtering

If you want to allow or block access by internal LAN users to certain sites on the Internet, use the UTM's web URL filtering. You can create or import a whitelist that contains domain names and URLs that are accepted and a blacklist with domain names and URLs that are blocked. The whitelist takes precedence over the blacklist. Both the whitelist and the blacklist take precedence over keyword blocking.

> **Note:** A URL that you enter on the whitelist or blacklist might contain other embedded URLs such as URLs for advertisements or sponsors, causing unexpected behavior. If you want to allow a URL by placing it on the whitelist, make sure that all embedded URLs are also placed on the whitelist. Similarly, if you want to block a URL by placing it on the blacklist, make sure that all embedded URLs are also placed on the blacklist.

➢ **To configure web URL filtering:**

1. Select **Application Security > HTTP/HTTPS > URL Filtering**. The URL Filtering screen displays. The following figure shows some URLs as examples:
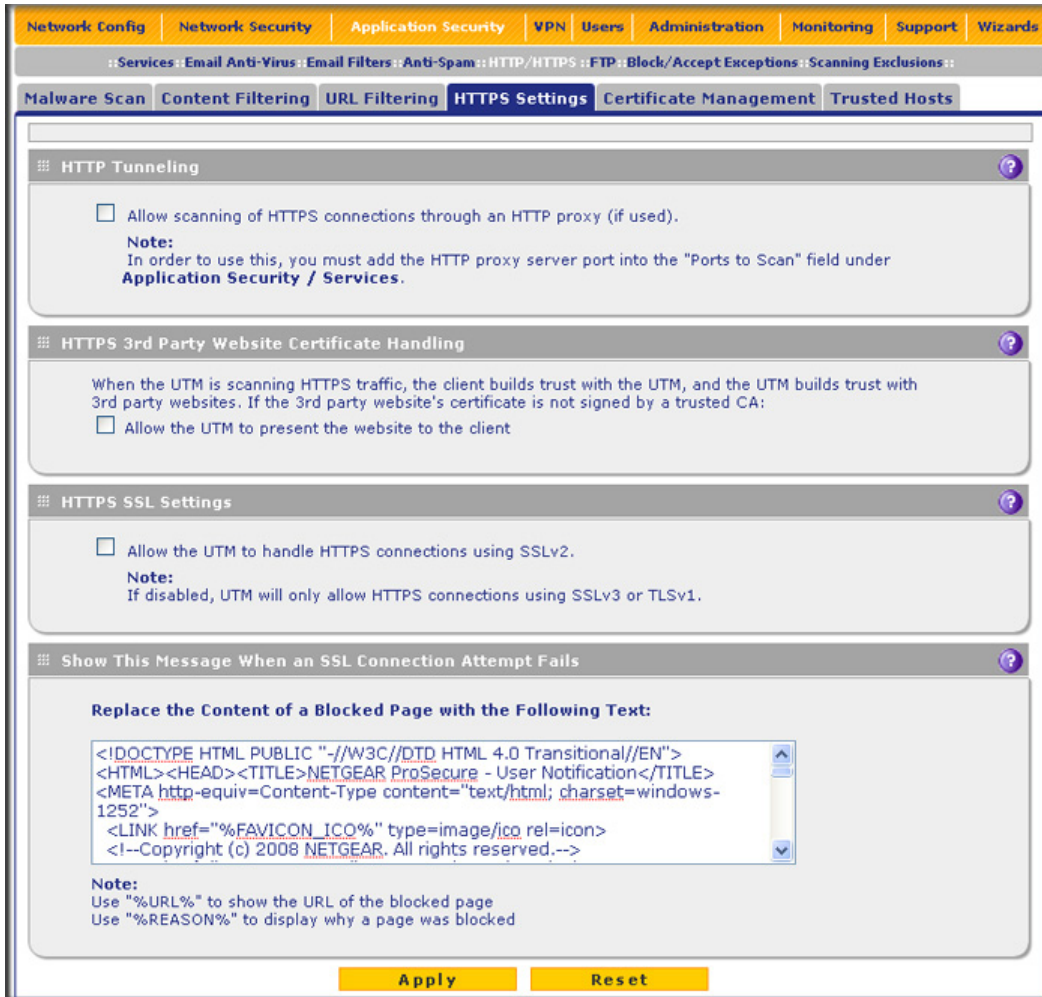

Figure 115.

2. Enter the settings as explained in the following table:

Table 46. URL Filtering screen settings

Setting	Description	
Whitelist		
Enable	Select this check box to bypass scanning of the URLs that are listed in the URL field. Users are allowed to access the URLs that are listed in the URL field.	
URL	This field contains the URLs for which scanning is bypassed. To add a URL to this field, use the Add URL field or the Import from File tool (see the explanation later in this table). You can add a maximum of 200 URLs. **Note:** If a URL is in both on the whitelist and blacklist, then the whitelist takes precedence, and URLs on the whitelist are not scanned. **Note:** Wildcards (*) are supported. For example, if you enter www.net*.com in the URL field, any URL that begins with www.net is allowed, and any URL that ends with .com is allowed.	
	Delete	To delete one or more URLs, highlight the URLs, and click the **Delete** table button.
	Export	To export the URLs, click the **Export** table button, and follow the instructions of your browser.
Add URL	Type or copy a URL in the Add URL field. Then click the **Add** table button to add the URL to the URL field. **Note:** Start the URL with http:// or https://. If you do not specify http:// or https://, the UTM automatically adds http://.	
Import from File	To import a list with URLs into the URL field, click the **Browse** button and navigate to a file in .txt format that contains line-delimited URLs (that is, one URL per line). Then click the **Upload** table button to add the URLs to the URL field. **Note:** Any existing URLs in the URL field are overwritten when you import a list of URLs from a file.	
Blacklist		
Enable	Select this check box to block the URLs that are listed in the URL field. Users attempting to access these URLs receive a notification (see the explanation later in this table).	
URL	This field contains the URLs that are blocked. To add a URL to this field, use the Add URL field or the Import from File tool (see the explanation later in this table). You can add a maximum of 200 URLs. **Note:** If a URL is in both the whitelist and blacklist, then the whitelist takes precedence, and URLs on the whitelist are not scanned. **Note:** Wildcards (*) are supported. For example, if you enter www.net*.com in the URL field, any URL that begins with www.net is blocked, and any URL that ends with .com is blocked.	

Table 46. URL Filtering screen settings (continued)

Setting	Description	
URL (continued)	Delete	To delete one or more URLs, highlight the URLs, and click the **Delete** table button.
	Export	To export the URLs, click the **Export** table button, and follow the instructions of your browser.
Add URL	Type or copy a URL in the Add URL field. Then click the **Add** table button to add the URL to the URL field. **Note:** Start the URL with http:// or https://. If you dot no specify http:// or https://, the UTM automatically adds http://.	
Import from File	To import a list with URLs into the URL field, click the **Browse** button and navigate to a file in .txt format that contains line-delimited URLs (that is, one URL per line). Then click the **Upload** table button to add the URLs to the URL field. **Note:** Any existing URLs in the URL field are overwritten when you import a list of URLs from a file.	

Replace the Content of a Blocked Page with the Following Text	By default, a blocked URL is replaced with the following text, which you can customize:
	      Internet Policy has restricted access to this location:
	      %URL%
	      You are logged in as %USER%
	      Click here to login as another user %USER_PORTAL_URL%
	
	Note: The text is displayed on the URL Filtering screen with HTML tags. However, when the UTM replaces the content of a blocked web page, the screen displays the notification text in HTML format.
	
	Note: Make sure that you keep the %URL% metaword in the text to enable the UTM to insert the blocked URL in the notification text. The %USER% metaword enables the UTM to insert the user login name; the %USER_PORTAL_URL% metaword enables the UTM to insert the User Portal Login screen.	

3. Click **Apply** to save your settings.

HTTPS Scan Settings

HTTPS traffic is encrypted traffic that cannot be scanned or the data stream would not be secure. However, the UTM can scan HTTPS traffic that is transmitted through an HTTP proxy. The UTM can break up the SSL connection between the HTTPS server and the HTTP client, scan the HTTPS traffic, and then rebuild the SSL connection. The following figure shows the HTTPS scanning traffic flow.
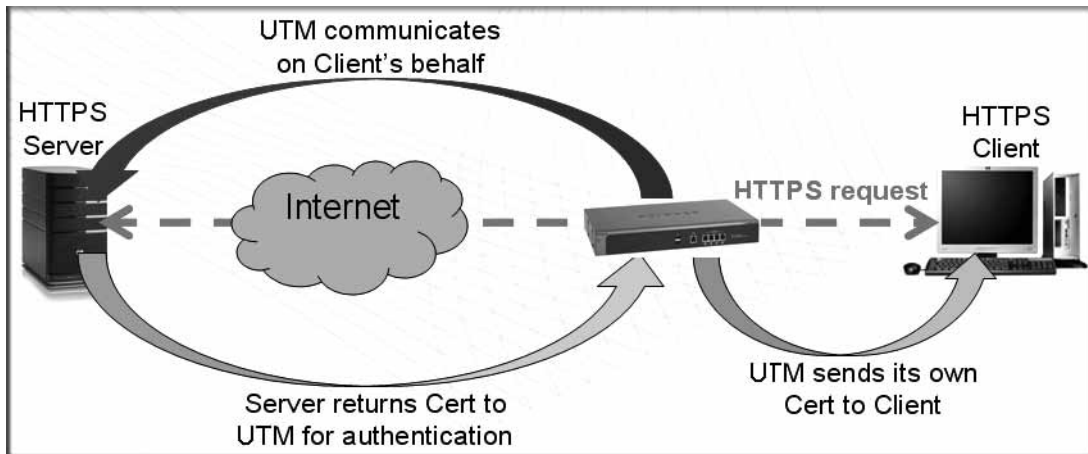
Figure 116.

The HTTPS scanning process functions with the following principles:

- The UTM breaks up an SSL connection between an HTTPS server and an HTTP client in two parts:
  - A connection between the HTTPS client and the UTM
  - A connection between the UTM and the HTTPS server
- The UTM simulates the HTTPS server communication to the HTTPS client, including the SSL negotiation, certificate exchange, and certificate authentication. In effect, the UTM functions as the HTTPS server for the HTTPS client.
- The UTM simulates the HTTPS client communication to the HTTPS server, including the SSL negotiation, certificate exchange, and certificate authentication. In effect, the UTM functions as the HTTPS client for the HTTPS server.

During SSL authentication, the HTTPS client authenticates three items:

- Is the certificate trusted?
- Has the certificate expired?
- Does the name on the certificate match that of the website?

If one of these items is not authenticated, a security alert message displays in the browser window:

Figure 117.

However, even when a certificate is trusted or still valid, or when the name of a certificate does match the name of the website, a security alert message still displays when a user who is connected to the UTM visits an HTTPS site. The appearance of this security alert message is expected behavior because the HTTPS client receives a certificate from the UTM instead of directly from the HTTPS server. If you want to prevent this security alert message from displaying, install a root certificate on the client PC. The root certificate can be downloaded from the UTM's Manager Login screen (see *Figure 19* on page 39).

If client authentication is required, the UTM might not be able to scan the HTTPS traffic because of the nature of SSL. SSL has two parts—client and server authentication. HTTPS server authentication occurs with every HTTPS request, but HTTPS client authentication is not mandatory, and rarely occurs. Therefore it is of less importance whether the HTTPS request comes from the UTM or from the real HTTPS client.

However, certain HTTPS servers do require HTTPS client certificate authentication for every HTTPS request. Because of the design of SSL, the HTTPS client needs to present its own certificate in this situation rather than using the one from the UTM, preventing the UTM from scanning the HTTPS traffic. For information about certificates, see *Manage Digital Certificates for HTTPS Scans* on page 213.

You can specify trusted hosts for which the UTM bypasses HTTPS traffic scanning. For more information, see *Specify Trusted Hosts* on page 218.

➢ **To configure the HTTPS scan settings:**

1. Select **Application Security > HTTP/HTTPS > HTTPS Settings**. The HTTPS Settings screen displays:
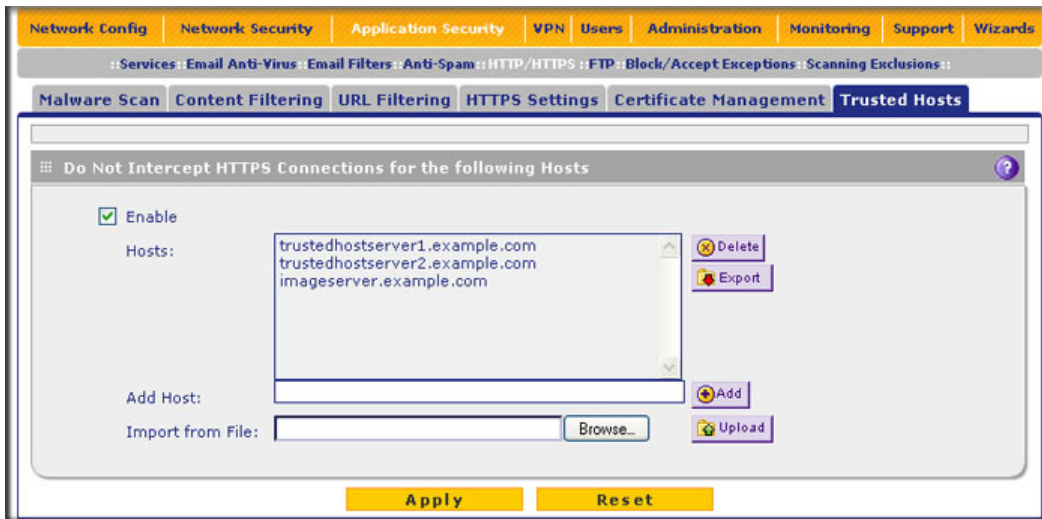
Figure 118.

2. Enter the settings as explained in the following table:

Table 47. HTTPS Settings screen settings

Setting	Description
HTTP Tunneling	
Select this check box to allow scanning of HTTPS connections through an HTTP proxy, which is disabled by default. Traffic from trusted hosts is not scanned (see *Specify Trusted Hosts* on page 218). **Note:** For HTTPS scanning to occur correctly, you need to add the HTTP proxy server port in the Ports to Scan field for the HTTPS service on the Services screen (see *Customize Web Protocol Scan Settings and Services (Web Applications)* on page 194).	
HTTPS 3rd Party Website Certificate Handling	
Select the **Allow the UTM to present the website to the client** check box to allow a Secure Sockets Layer (SSL) connection with a valid certificate that is not signed by a trusted certification authority (CA). The default setting is to block such a connection.	

Table 47. HTTPS Settings screen settings (continued)

Setting	Description
HTTPS SSL Settings	
Select the **Allow the UTM to handle HTTPS connections using SSLv2** check box to allow HTTPS connections using SSLv2, SSLv3, or TLSv1. If this check box is cleared, the UTM allows HTTPS connections using SSLv3 or TLSv1, but not using SSLv2.	
Show This Message When an SSL Connection Attempt Fails	
By default, a rejected SSL connection is replaced with the following text, which you can customize: The SSL connection to %URL% cannot be established because of %REASON%. **Note:** Make sure that you keep the %URL% and %REASON% metawords in a message to enable the UTM to insert the correct URL information and the reason for the rejection.	

3. Click **Apply** to save your settings.

> **Note:** For information about certificates that are used for SSL connections and HTTPS traffic, see *Manage Digital Certificates for VPN Connections* on page 381.

Manage Digital Certificates for HTTPS Scans

> **Note:** For information about digital certificates for VPN connections, see *Manage Digital Certificates for VPN Connections* on page 381.

Before enabling HTTPS scanning, you can specify which digital certificate is used by the UTM to handle HTTPS requests. The UTM uses digital certificates to authenticate connecting HTTPS servers, and to allow HTTPS clients to be authenticated by remote entities. A digital certificate that authenticates a server, for example, is a file that contains the following elements:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

When a security alert is generated (see the following figure), the user can decide whether or not to trust the host.

Figure 119.

The UTM contains a self-signed certificate from NETGEAR. This certificate can be downloaded from the UTM login screen or from the Certificate Management screen for browser import. However, before you deploy the UTM in your network, NETGEAR recommends that you replace this digital certificate with a digital certificate from a well-known commercial certification authority (CA) such as an internal Windows server or an external organization such as Verisign or Thawte. Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity. On the UTM, the uploaded digital certificate is checked for validity and purpose. The digital certificate is accepted when it passes the validity test and the purpose matches its use.

To display the Certificate Management screen, select **Web Security > Certificate Management**. Because of the size of this screen, and because of the way the information is presented, the Certificate Management screen is divided and presented in this manual in three figures (the following figure, *Figure 121* on page 216, and *Figure 122* on page 217).

The UTM's Certificate Management screen lets you view the currently loaded digital certificate for HTTPS scans, upload a new digital certificate, manage the trusted CA authorities list, and manage the untrusted certificates list.

Manage the Active HTTPS Certificate

To manage the UTM's active certificate that is used for HTTPS scans, select **Web Security > Certificate Management**. The Certificate Management screen displays. The following figure shows only the Certificate Used for HTTPS Scans section of the screen:
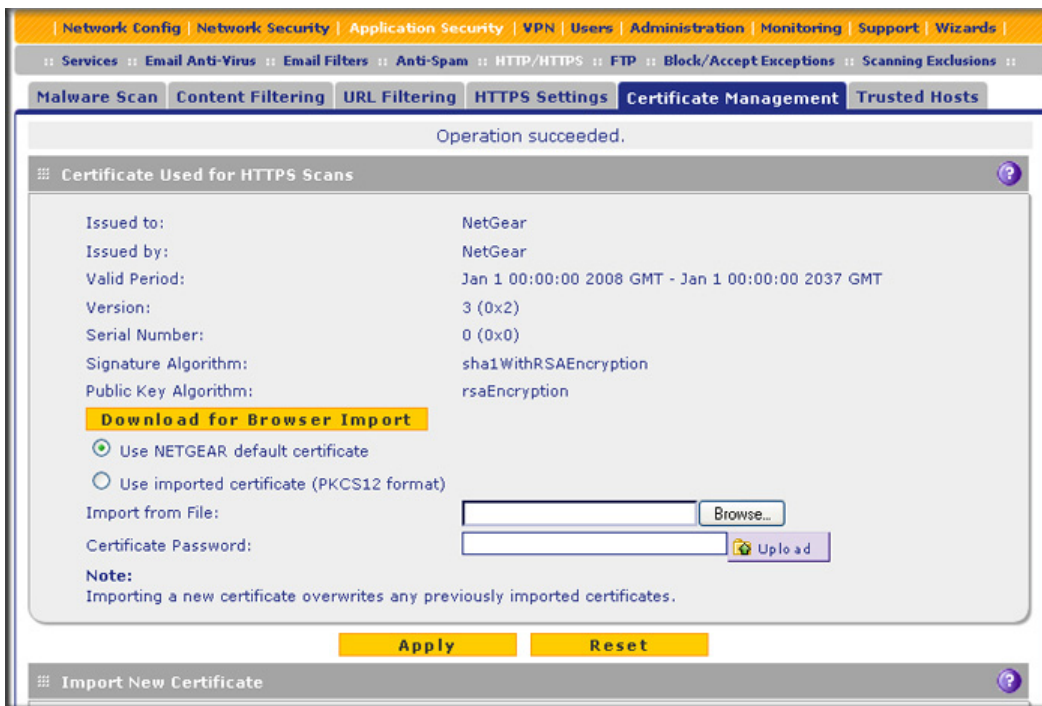
Figure 120. Certificate management, screen 1 of 3

The top part of the Certificate Used for HTTPS Scans section displays information about the current certificate that is used for HTTPS scans.

Note: For information about the HTTPS scanning process, see *HTTPS Scan Settings* on page 209.

➢ **To download the current certificate into your browser:**

1. Click **Download for Browser Import**.
2. Follow the instructions of your browser to save the RootCA.crt file on your computer.

➢ **To reload the default NETGEAR certificate:**

1. Select the **Use NETGEAR default certificate** radio button.
2. Click **Apply** to save your settings.

➢ **To import a new certificate:**

1. Select the **Use imported certificate (PKCS12 format)** radio button.
2. Click **Browse** next to the Import from File field.
3. Navigate to a trusted certificate file on your computer. Follow the instructions of your browser to place the certificate file in the Import from File field.
4. If required, enter the appropriate password in the Certificate Password field.

---

5. Click the **Upload** button.

Note: If the certificate file is not in the pkcs12 format, the upload fails. Importing a new certificate overwrites any previously imported certificates.

---

6. Click **Apply** to save your settings.

Manage Trusted HTTPS Certificates

To manage trusted certificates, select **Web Security > Certificate Management**. The Certificate Management screen displays. The following figure shows only the Import New Certificate and Trusted Certificates sections of the screen:

Figure 121. Certificate management, screen 2 of 3

The Trusted Certificates table contains the trusted certificates from third-party websites that are signed by the Certificate Authorities. The UTM comes standard with trusted certificates that are preloaded in the Trusted Certificates table.

➢ **To import a trusted certificate:**

1. In the Import New Certificate section of the screen, click **Browse** next to the Import from File field.

2. Navigate to a trusted certificate file on your computer. Follow the instructions of your browser to place the certificate file in the Import from File field.

3. Click the **Upload** button. The newly imported trusted certificate is added to the Trusted Certificates table.

➢ **To view details of a trusted certificate:**

1. From the Trusted Certificates table, select the certificate.

2. Click **View Details**. A new screen opens that displays the details of the certificate.

➢ **To delete a trusted certificate:**

1. From the Trusted Certificates table, select the certificate.

2. Click **Delete Selected**.

Manage Untrusted HTTPS Certificates

To manage untrusted certificates, select **Web Security > Certificate Management**. The Certificate Management screen displays. The following figure shows only the Exceptions - Untrusted Certificates But Granted Access section of the screen:

Figure 122. Certificate management, screen 3 of 3

When the UTM detects an untrusted or invalid certificate, it automatically places the certificate in the Exceptions - Untrusted Certificates But Granted Access table.

➢ **To view details of an untrusted certificate:**

1. From the Exceptions - Untrusted Certificates But Granted Access table, select the certificate.

2. Click **View Details**. A new screen opens that displays the details of the certificate.

➢ **To delete an untrusted certificate:**

1. From the Exceptions - Untrusted Certificates But Granted Access table, select the certificate.

2. Click **Delete Selected**.

➢ **To move an untrusted certificate to the Trusted Certificate Authorities table:**

1. From the Exceptions - Untrusted Certificates But Granted Access table, select the certificate.

2. Click **Add to Trusted List**. The previously untrusted certificate is added to the Trusted Certificates table.

Specify Trusted Hosts

You can specify trusted hosts for which the UTM bypasses HTTPS traffic scanning and security certificate authentication. The security certificate is sent directly to the client for authentication, which means that the user does not receive a security alert for trusted hosts. For more information about security alerts, see *Manage Self-Signed Certificates* on page 384.

Note that certain sites contain elements from different HTTPS hosts. As an example, assume that the https://example.com site contains HTTPS elements from the following three hosts:

- trustedhostserver1.example.com
- trustedhostserver2.example.com
- imageserver.example.com

To completely bypass the scanning of the https://example.com site, you need to add all three hosts to the trusted hosts list because different files from these three hosts are also downloaded when a user attempts to access the https://example.com site.

➢ **To specify trusted hosts:**

1. Select **Application Security > HTTP/HTTPS > Trusted Hosts**. The Trusted Hosts screen displays. (The following figure shows some hosts as examples.)

Figure 123.

2. Enter the settings as explained in the following table:

Table 48. Trusted Hosts screen settings

Setting	Description
Do Not Intercept HTTPS Connections for the following Hosts	
Enable	Select this check box to bypass scanning of trusted hosts that are listed in the Hosts field. Users do not receive a security alert for trusted hosts that are listed in the Hosts field.

Table 48. Trusted Hosts screen settings (continued)

Setting	Description	
Hosts	This field contains the trusted hosts for which scanning is bypassed. To add a host to this field, use the Add Host field or the Import from File tool (see the explanation later in this table). You can add a maximum of 200 URLs.	
	Delete	To delete one or more hosts, highlight the hosts, and click the **Delete** table button.
	Export	To export the hosts, click the **Export** table button, and follow the instructions of your browser.
Add Host	Type or copy a trusted host in the Add Host field. Then click the **Add** table button to add the host to the Hosts field.	
Import from File	To import a list with trusted hosts into the Hosts field, click the **Browse** button, and navigate to a file in .txt format that contains line-delimited hosts (that is, one host per line). Then click the **Upload** table button to add the hosts to the Hosts field. **Note:** Any existing hosts in the Hosts field are overwritten when you import a list of hosts from a file.	

3. Click **Apply** to save your settings.

Configure FTP Scans

Some malware threats are specifically developed to spread through the FTP protocol. By default, the UTM scans FTP traffic, but you can specify how the UTM scans FTP traffic and which action is taken when a malware threat is detected.

> **Note:** The UTM does not scan password-protected FTP files.

> **To configure the FTP scan settings:**

1. Select **Application Security > FTP**. The FTP screen displays:
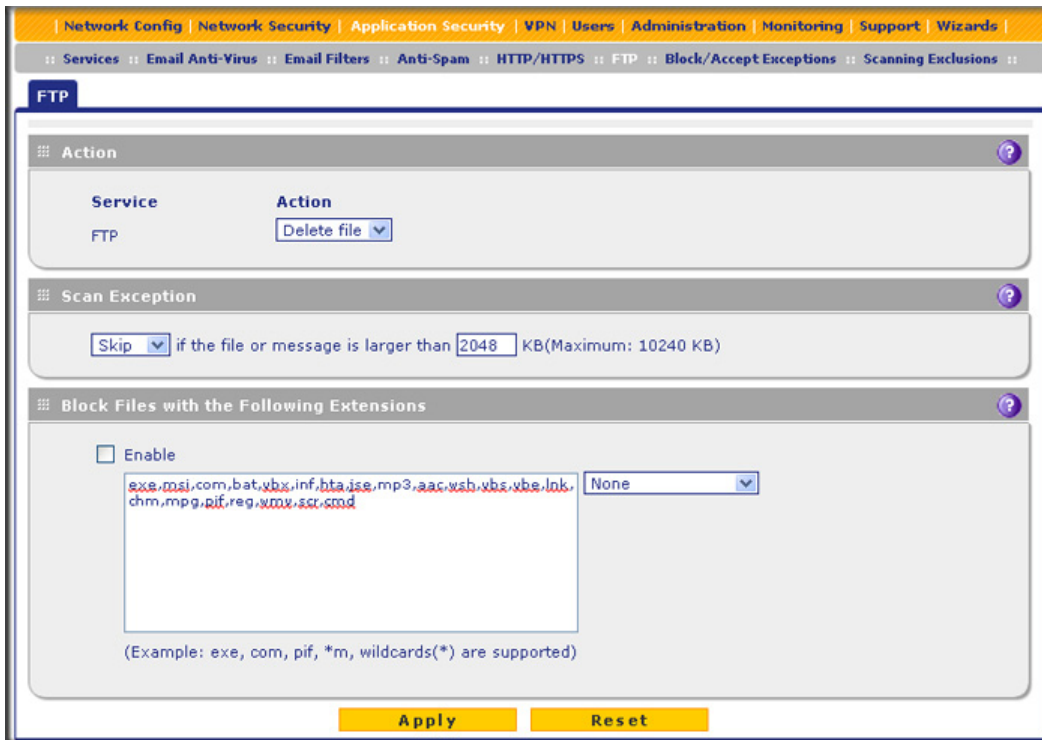
Figure 124.

2. Enter the settings as explained in the following table:

Table 49. FTP screen settings

Setting	Description	
Action		
FTP	Action	From the FTP drop-down list, select one of the following actions to be taken when an infected FTP file or object is detected: • **Delete file**. This is the default setting. The FTP file or object is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The FTP file or object is not deleted. • **Quarantine file** (UTM9S only). The FTP file or object is quarantined, and a log entry is created (see the Note on page 176).
Scan Exception		
The default maximum size of the file or object that is scanned is 2048 KB, but you can define a maximum size of up to 10240 KB. However, setting the maximum size to a high value might affect the UTM's performance (see *Performance Management* on page 389). From the drop-down list, select one of the following actions to be taken when the file or message exceeds the maximum size: • **Skip**. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • **Block**. The file is blocked and does not reach the end user.		

Table 49. FTP screen settings (continued)

Setting	Description
Block Files with the Following Extensions	
By default, the File Extension field lists the most common file extensions. You can manually add or delete extensions. Use commas to separate different extensions. You can enter a maximum of 40 file extensions. The maximum total length of this field, excluding the delimiter commas, is 160 characters. You can also use the drop-down list to add predefined file extensions from a specific category to the File Extension field: • **None**. No file extensions are added to the File Extension field. This is the default setting. • **Executables**. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field. • **Audio/Video**. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field. • **Compressed Files**. Compressed file extensions (zip, rar, gz, tar, and bz2) added to the File Extension field.	

3. Click **Apply** to save your settings.

Set Web Access Exception Rules

You can set up to 200 exception rules for users and members of a group to allow access to applications, file extensions and protocols, web categories, and URLs that you have blocked for all other users. Or you can do it the other way around—block access to applications, file extensions and protocols, web categories, and URLs that you have allowed access to for all other users.

If you have not created a custom group, an exception rule can apply to either *one* of the following groups or individual users:

- All users
- All authenticated users
- All unauthenticated users
- A local group or local user
- A group or users that is defined by its IP address
- A Lightweight Directory Access Protocol (LDAP) group or LDAP user
- A RADIUS VLAN group

To further refine exception rules, you can create custom groups that allow you to include a combination of local groups and local users, groups and users that are defined by their IP address, LDAP groups and users, and RADIUS groups and users. For more information, see *Create Custom Groups for Web Access Exceptions* on page 228.

> **Note:** Users and groups to which access exception rules apply are not the same as LAN groups. For information about how to specify members of a LAN group and to customize LAN group names, see *Configure Authentication Domains, Groups, and Users* on page 345.

If you have not created a custom category, an exception rule can apply to either *one* of the following components:

- One built-in application group or built-in individual application
- A combination of file extensions and protocols
- One URL or URL expression
- One built-in web category group or built-in individual web category

To further refine exception rules, you can create custom categories that allow you to include either a selection of applications, or a selection of URLs, or a selection of web categories. For more information, see *Create Custom Categories for Web Access Exceptions* on page 231.

> **Tip:** If you want to use a custom group and custom category, first create the custom group and custom category, then create the exception rule.

➢ **To set web access exception rules:**

1. Select **Application Security > Block/Accept Exceptions**. The Block/Accept Exceptions submenu tabs display, with the Block/Accept Exceptions screen in view. This screen shows the Exceptions table, which is empty if you have not specified any exception rules. (The following figure shows several exception rules in the table as an example.)
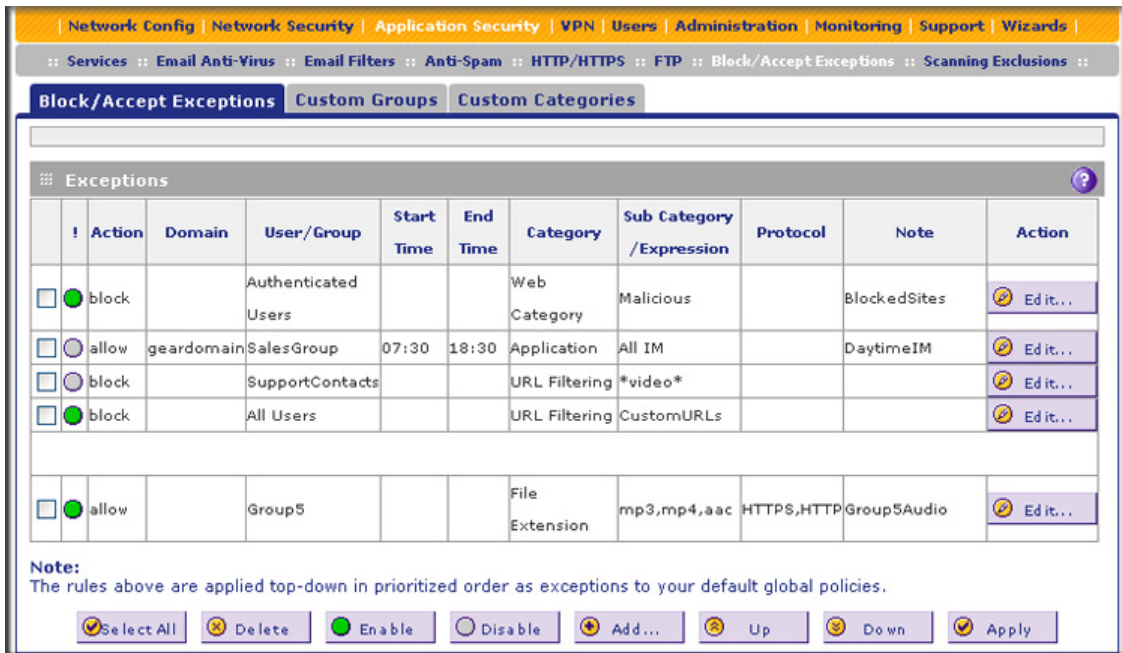
Figure 125.

2. Under the Exceptions table, click the **Add** table button to specify an exception rule. The Add or Edit or Block/Accept Exceptions screen displays:
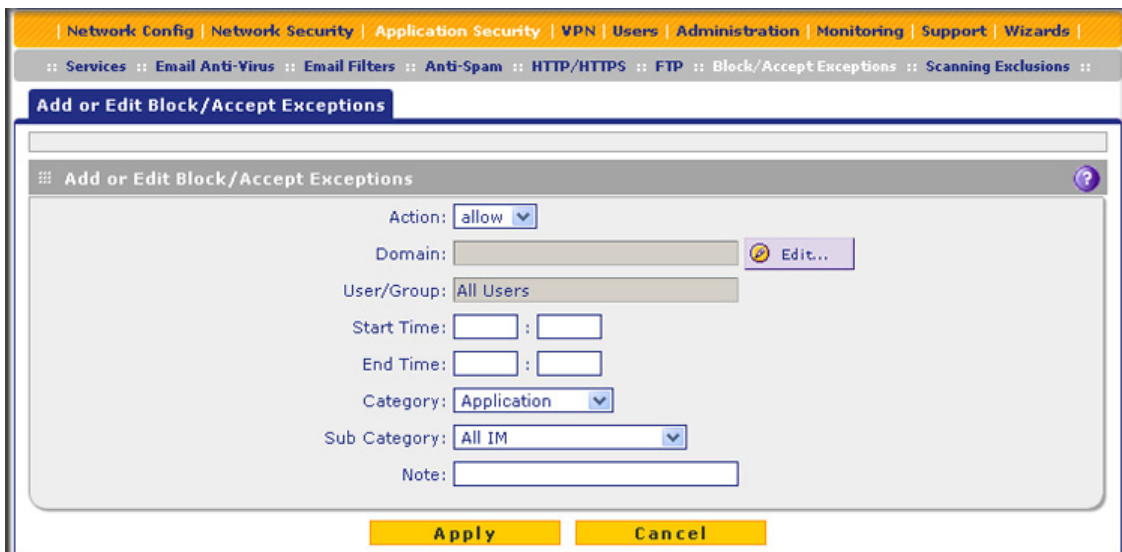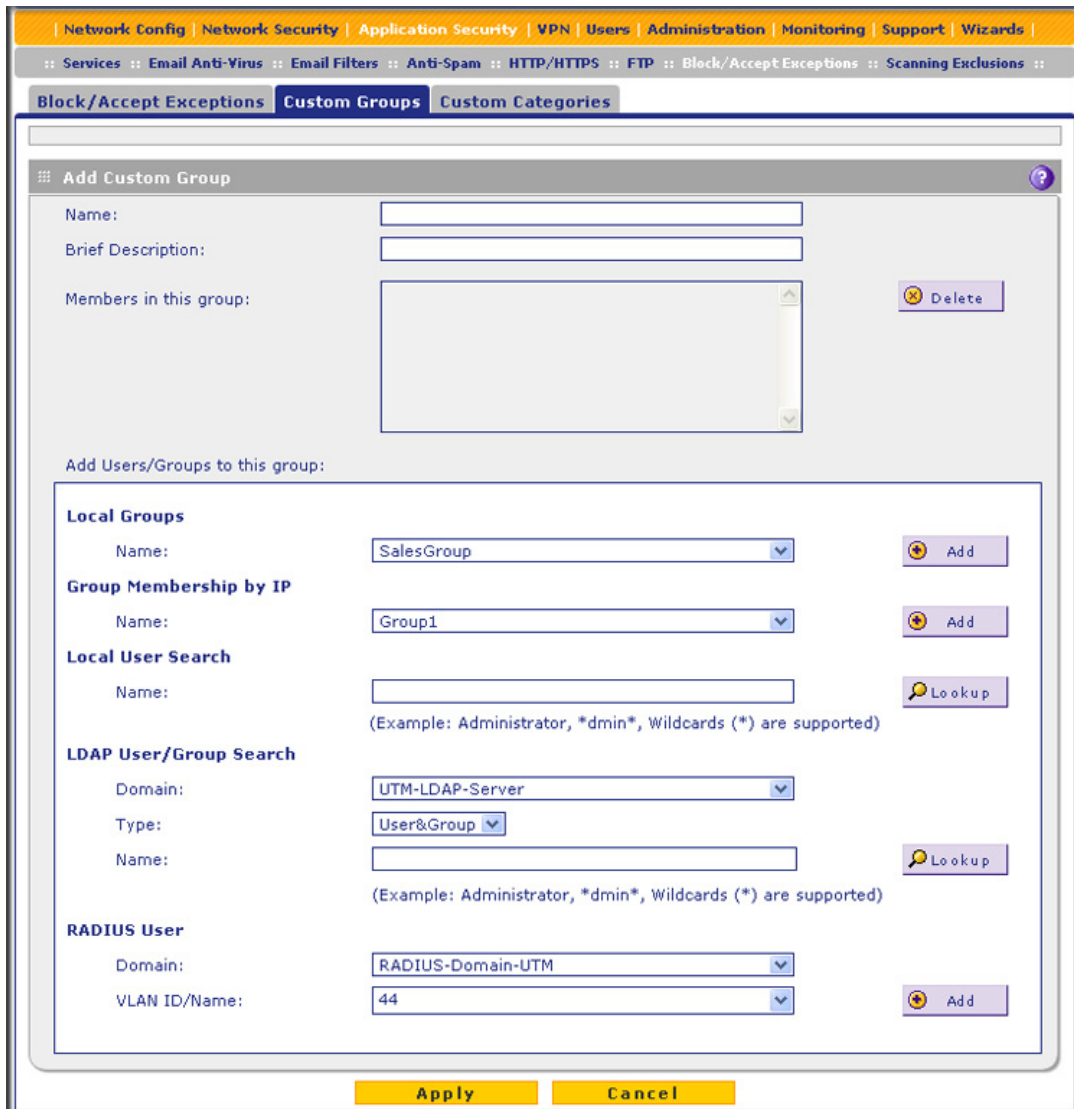

Figure 126.

3. Complete the fields and make your selections from the drop-down lists as explained in the following table:

Table 50. Edit or Block/Accept Exceptions screen settings
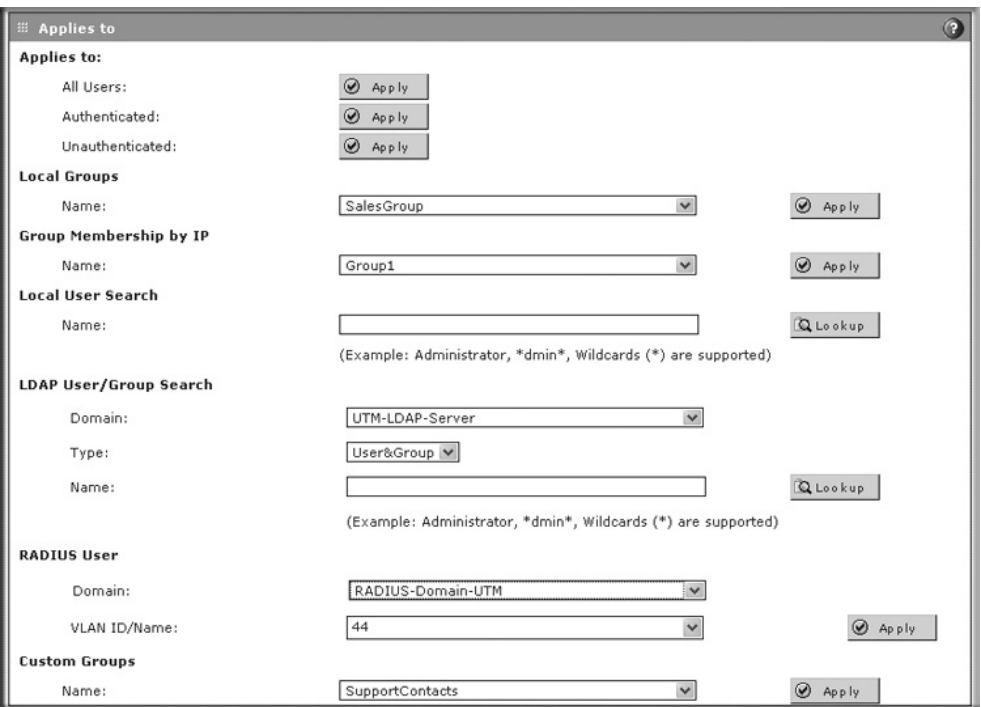
Setting	Description
Action	From the drop-down list, select the action that the UTM applies: • **Allow**. The exception allows access to an application, web category, or URL that is otherwise blocked. • **Block**. The exception blocks access to an application, web category, or URL that is otherwise allowed.
Domain User/Group	Click the **Edit** button to open the Applies To pop-up screen, which lets you configure a domain, group, or individual user to which the exception needs to apply (see the screen later in this table). If applicable, on the Applies To screen, click a **Lookup** button to retrieve a group or user. When you have made your decision, click an **Apply** button to add the domain to the Domain field on the Add Exception screen and the group and user to the User/Group field on the Add Exception screen. **Note:** The Domain field can remain blank for some special users or groups. The following screen and rows in this table explain the options on the Applies To screen.
	All Users — Click the **Apply** button to apply the exception to all users, both authenticated and unauthenticated.
	Authenticated — Click the **Apply** button to apply the exception to all authenticated users. These are users who have actively logged in to the UTM and who have been authenticated.

Table 50. Edit or Block/Accept Exceptions screen settings (continued)

Setting		Description
Domain User/Group (continued)	Unauthenticated	Click the **Apply** button to apply the exception to all unauthenticated users. These are users who have not actively logged in to the UTM. By default, these users are assigned the account name anonymous.
	Local Groups	Do the following: 1. From the Name drop-down list, select a local group. 2. Click the **Apply** button to apply the exception to the selected local group. You can specify local groups on the Groups screen (see *Create and Delete Groups* on page 359.
	Group Membership by IP	Do the following: 1. From the Name drop-down list, select a group that is defined by its IP address. 2. Click the **Apply** button to apply the exception to the selected group. You can specify groups that are defined by their IP address on the LAN Groups screen (see *Manage the Network Database* on page 107).
	Local User Search	Do the following: 1. In the Name field, enter a user name. 2. Click the **Lookup** button. If the user is found, he or she is listed to the left of the Apply button. 3. Click the **Apply** button to apply the exception to the selected user.
	LDAP User/Group Search	Do the following: 1. From the Domain drop-down list, select an LDAP domain. 2. From the Type drop-down list, select **User**, **Group**, or **User&Group**. 3. In the Name field, enter the name of the user, group, or user and group, or leave this field blank. 4. Click the **Lookup** button. If the user or group is found, it is listed to the left of the Apply button. If you left the Name field blank, all users, groups, or users and groups are listed; in this case, make a selection. 5. Click the **Apply** button to apply the exception to the selected user or group. You can specify LDAP domains, groups, and users on the Domains screen (see *Configure Domains* on page 353).
	RADIUS User	Do the following: 1. From the Domain drop-down list, select a RADIUS domain. 2. From the VLAN ID/Name drop-down list, select a VLAN ID or VLAN name. 3. Click the **Apply** button to apply the exception to the selected VLAN. You can specify RADIUS domains on the Domains screen (see *Configure Domains* on page 353) and RADIUS VLANs on the List of VLAN screen (see *Configure RADIUS VLANs* on page 376).

Table 50. Edit or Block/Accept Exceptions screen settings (continued)

Setting	Description	
Domain User/Group (continued)	Custom Groups	Do the following: 1. From the Name drop-down list, select a custom group. 2. Click the **Apply** button to apply the exception to the selected group. You can specify custom groups on the Custom Groups screen (see *Create Custom Groups for Web Access Exceptions* on page 228).
Start Time	The time in 24-hour format (hours and minutes) when the action starts. If you leave these fields empty, the action applies continuously.	
End Time	The time in 24-hour format (hours and minutes) when the action ends. If you leave these fields empty, the action applies continuously.	
Category (and related information)	From the Category drop-down list, select the category to which the action applies. Your selection determines which drop-down lists, fields, radio buttons, and check boxes display onscreen.	
	Applications	The action applies to an application. Select an application from the Sub Category drop-down list. For information about custom application categories, see *Create Custom Categories for Web Access Exceptions* on page 231.
	File Extensions	The action applies to one or more file extensions and one or more protocols. The following field and check boxes display onscreen: • **File Extensions**. Manually enter up to 40 file extensions. Use commas to separate multiple file extensions. Wildcards (*) are supported. A single asterisk (*) matches any file extension. You can also use the drop-down list to the right of the File Extension field to automatically add file extensions from the following categories: - **None**. No file extensions are added to the File Extension field. This is the default setting. - **Executables**. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field. - **Audio/Video**. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field. - **Compressed Files**. Compressed file extensions (zip, rar, gz, tar, and bz2) are added to the File Extension field. • **Protocols**. Select one or multiple check boxes to specify which protocols the action applies to: **- SMTP** **- POP3** **- IMAP** **- HTTP** **- HTTPS** **- FTP**

Table 50. Edit or Block/Accept Exceptions screen settings (continued)

Setting	Description	
Category (and related information) (continued)	URL Filtering	The action applies to a URL. The following radio buttons, field, and drop-down list display onscreen. Select a radio button to either enter a URL expression or select a custom URL list. • **Expression**. Select the upper radio button, and enter a URL or URL expression such as *video* or *chat*. Wildcards (*) are supported. The maximum supported size of the URL or URL expression is 1024 bytes. • **Custom List**. Select the lower radio button and a custom URL list from the drop-down list. For information about custom URL lists, see *Create Custom Categories for Web Access Exceptions* on page 231.
	Web Categories	The action applies to a web category. Select a web category from the Sub Category drop-down list. For information about custom web categories, see *Create Custom Categories for Web Access Exceptions* on page 231.
Note	A description of the exception rule for identification and management purposes or any other relevant information that you wish to include.	

4. Click **Apply** to save your settings. The new exception rule is added to the Exceptions table and is enabled by default. To return to the Exception screen without adding the rule, click **Cancel**.

5. Optional step: If you do not immediately want to enable a new rule, select the check box to the left of the rule that you want to disable (or click the **Select All** table button to select all rules). Then click the **Disable** table button to disable the selected rule or rules.

> **Note:** Enabled exception rules are preceded by a green circle in the ! column; disabled exception rules are preceded by a gray circle in the ! column.

> **To make changes to an existing exception rule:**

1. In the Action column to the right of to the exception rule, click the **Edit** table button. The Add or Edit Block/Accept Exception screen displays (see *Figure 126* on page 223).

2. Modify the settings that you wish to change (see the previous table).

3. Click **Apply** to save your changes. The modified exception rule is displayed in the Exceptions table.

> **To disable, enable, or delete one or more exception rules:**

1. Select the check box to the left of each rule that you want to delete or disable, or click the **Select All** table button to select all rules.

2. Click one of the following table buttons:

   • **Disable**. Disables the rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the rule is or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)

- **Enable**. Enables the rule or rules. The ! status icon changes from a gray circle to a green circle, indicating that the rule is or rules are enabled.

- **Delete**. Deletes the rule or rules.

The table rank of the exception rule in the Exceptions table determines the order in which the rule is applied (from the top down). To change the position of the rules in the table, select one or more a rules, and then click one of the following table buttons:

- **Up**. Moves the rule or rules up one position in the table rank.

- **Down**. Moves the rule or rules down one position in the table rank.

Create Custom Groups for Web Access Exceptions

After you have specified groups and users (see *Configure Authentication Domains, Groups, and Users* on page 345), you can create up to 200 custom groups, each of which can include a combination of local groups and local users, groups and users that are defined by their IP addresses, LDAP groups and users, and RADIUS groups and users. You use these custom groups to set web access exceptions on the Exceptions screen (see *Set Web Access Exception Rules* on page 221).

➢ **To create and manage custom groups:**

1. Select **Application Security > Block/Accept Exceptions > Custom Groups**. The Custom Groups screen displays. This screen shows the Custom Groups table, which is empty if you have not specified any custom groups. (The following figure shows one custom group in the table as an example.)
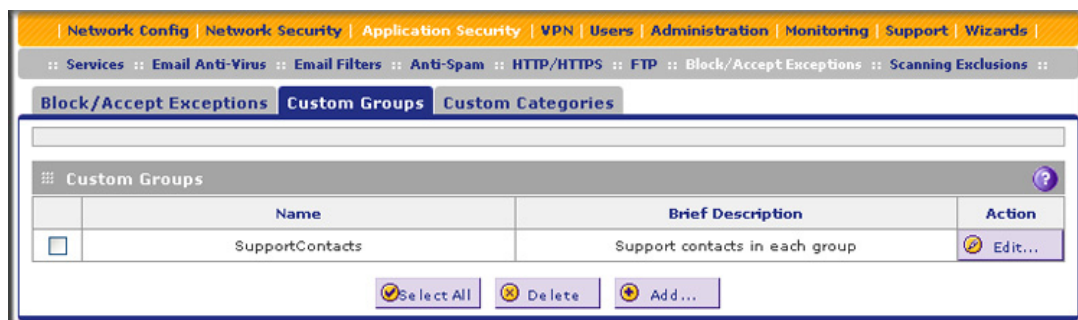
Figure 127.

2. Under the Custom Groups table, click the **Add** table button to specify a custom group. The Add Custom Group screen displays:

Figure 128.

3. Complete the fields and make your selections from the drop-down lists as explained in the following table:

Table 51. Custom Groups screen settings

Setting	Description
Name	A name of the custom group for identification and management purposes.
Brief Description	A description of the custom group for identification and management purposes.
Members in this group	When you click the **Add** button in the Add Users/Groups to this group section of the screen, the selected member is added to this field. To remove a member, highlight the member in this field, and then click the **Delete** button.

Table 51. Custom Groups screen settings (continued)

Setting	Description	
Add Users/Groups to this group	Local Groups	Do the following: 1. From the Name drop-down list, select a local group. 2. Click the **Add** button to add the selected local group to the custom group. Repeat this step to add more local groups to the custom group. You can specify local groups on the Groups screen (see *Create and Delete Groups* on page 359.
	Group Membership by IP	Do the following: 1. From the Name drop-down list, select a group that is defined by its IP address. 2. Click the **Add** button to add the selected group to the custom group. Repeat this step to add more users or groups, or both, to the custom group. You can specify groups that are defined by their IP address on the LAN Groups screen (see *Manage the Network Database* on page 107).
	Local User Search	Do the following: 1. In the Name field, enter a user name. 2. Click the **Lookup** button. If the user is found, he or she is listed to the left of the Apply button. 3. Click the **Add** button to add the selected local user to the custom group. Repeat this step to add more local users to the custom group.
	LDAP User/Group Search	Do the following: 1. From the Domain drop-down list, select an LDAP domain. 2. From the Type drop-down list, select **User**, **Group**, or **User&Group**. 3. In the Name field, enter the name of the user, group, or user and group, or leave this field blank. 4. Click the **Lookup** button. If the user or group is found, it is listed to the left of the Add button. If you left the Name field blank, all users, groups, or users and groups are listed. In this case, make a selection. 5. Click the **Add** button to add the selected user or group to the custom group. Repeat this step to add more users or groups, or both, to the custom group. You can specify LDAP domains, groups, and users on the Domains screen (see *Configure Domains* on page 353).

Table 51. Custom Groups screen settings (continued)

Setting	Description	
Add Users/Groups to this group (continued)	RADIUS User	Do the following: 1. From the Domain drop-down list, select a RADIUS domain. 2. From the VLAN ID/Name drop-down list, select a VLAN ID or VLAN name. 3. Click the **Add** button to add the selected VLAN ID or VLAN name to the custom group. Repeat this step to add more VLAN IDs or VLAN names to the custom group. You can specify RADIUS domains on the Domains screen (see *Configure Domains* on page 353) and RADIUS VLANs on the List of VLAN screen (see *Configure RADIUS VLANs* on page 376).

4. After you have specified all members of the custom group, click **Apply** to save your settings. The new custom group is added to the Custom Groups table. To return to the Custom Groups screen without adding the group, click **Cancel**.

➢ **To make changes to an existing custom group:**

1. In the Action column to the right of to the custom group, click the **Edit** table button. The Edit Custom Group screen displays. This screen is identical to the Add Custom Group screen (see *Figure 128* on page 229).

2. Modify the settings that you wish to change (see the previous table).

3. Click **Apply** to save your changes. The modified custom group is displayed in the Custom Groups table.

➢ **To delete one or more custom groups:**

1. Select the check box to the left of each custom group that you want to delete, or click the **Select All** table button to select all custom groups.

2. Click the **Delete** table button.

Create Custom Categories for Web Access Exceptions

Use custom categories to set web access exceptions on the Exceptions screen (see *Set Web Access Exception Rules* on page 221). A custom category can include a selection of applications, or a selection of URLs, or a selection of web categories, but no combination of applications, URLs, and web categories. You can create up to 200 custom categories.

➢ **To create and manage custom categories:**

1. Select **Global Settings > Exceptions > Custom Categories**. The Custom Categories screen displays. This screen shows the Custom Categories table, which is empty if you have not specified any custom categories. (The following figure shows three custom categories in the table as an example.)

Figure 129.

2. Under the Custom Categories table, click the **Add** table button to specify a custom category.

The Add Custom Category screen displays. The nature of the screen depends on your selection from the Category Type drop-down list, which is set by default to Applications (this selection is shown in the following figure). The URL Filtering and web Categories settings are shown in *Figure 131* on page 233 and *Figure 132* on page 233 respectively.
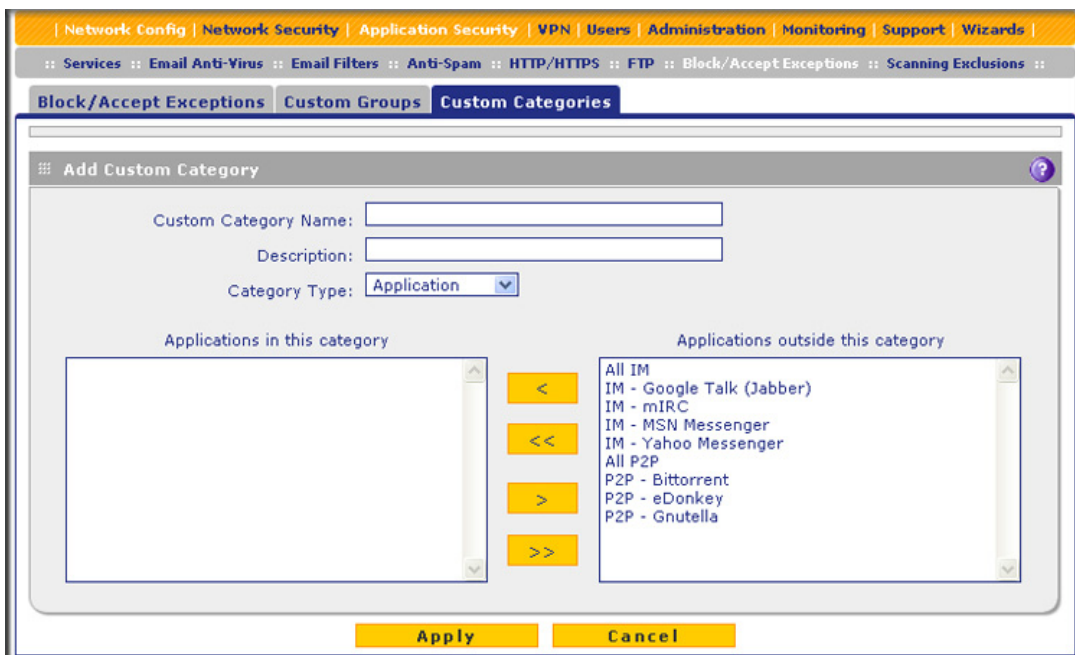
Figure 130. Custom categories: applications
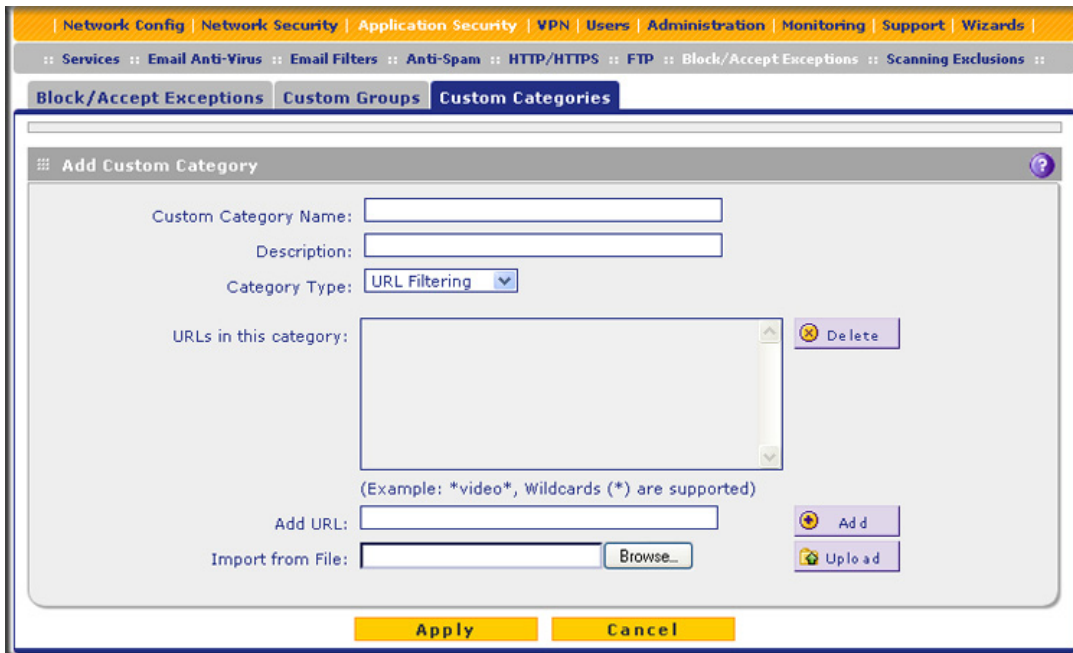
Figure 131. Custom categories: URL filtering
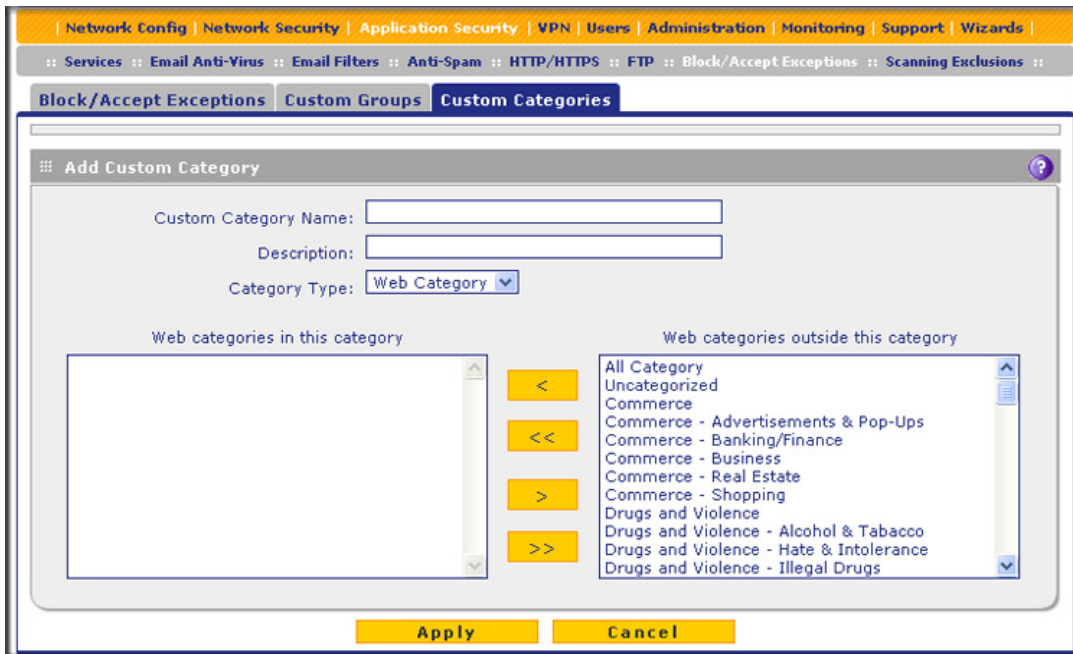
Figure 132. Custom categories: web categories

3. Complete the fields and make your selections from the drop-down lists as explained in the following table:

Table 52. Custom Categories screen settings

Setting	Description	
Name	A name of the custom category for identification and management purposes.	
Brief Description	A description of the category group for identification and management purposes.	
Category Type	From the Category Type drop-down list, select the type of category that you want to create. Your selection determines the nature of the screen.	
	Application	Use the move buttons to move entire application categories (for example, Instant Messaging), individual applications (for example, Instant Messaging - Google Talk), or combinations of both from the Applications outside this Category field to the Applications in this Category field (or the other way around).
		These are the functions of the move buttons:
		• **<** or **>** moves one or more highlighted selections from one field to the other.
		• **<<** or **>>** moves all entries from one field to the other.
	URL Filtering	URLs in this Category field:
		This field contains the URLs that are added to the custom category. To add a URL to this field, use the Add URL field or the Import from File tool (see explanations later in this table). You can add a maximum of 2000 URLs.
		Note: Wildcards (*) are supported. For example, if you enter www.net*.com in the Add URL field and then click the Add table button, any URL that begins with www.net and ends with .com is included in the custom category.
		Note: To delete one or more URLs, highlight the URLs, and click the **Delete** table button.
		Add URL field:
		Type or copy a URL in the Add URL field. Then click the **Add** table button to add the URL to the URLs in this Category field.
		Note: Start the URL with http:// or https://. If you dot no specify http:// or https://, the UTM automatically adds http://.

Table 52. Custom Categories screen settings (continued)

Setting	Description		
Category Type (continued)	URL Filtering (continued)	Import from File field: To import a list with URLs into the URLs in this Category field, click the **Browse** button and navigate to a file in .txt format that contains line-delimited URLs (that is, one URL per line). Then click the **Upload** table button to add the URLs to the URLs in this Category field. **Note:** Any existing URLs in the URLs in this Category field are overwritten when you import a list of URLs from a file.	
	Web Categories	Use the move buttons to move entire web categories (for example, Commerce), individual applications (for example, Commerce - Shopping), or combinations of both from the web categories outside this category field to the web categories in this category field (or the other way around). These are the functions of the move buttons: • **<** or **>** moves one or more highlighted selections from one field to the other. • **<<** or **>>** moves all entries from one field to the other.	

4. Click **Apply** to save your settings. The new category is added to the Custom Categories table. To return to the Custom Categories screen without adding the category, click **Cancel**.

> **To make changes to an existing custom category:**

1. In the Action column to the right of the custom category, click the **Edit** table button. The Edit Custom Category screen displays. This screen is identical to the Add Custom Category screen (see *Figure 130* on page 232, *Figure 131* on page 233, and *Figure 132* on page 233).
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified custom group is displayed in the Custom Categories table.

> **To delete one or more custom categories:**

1. Select the check box to the left of each custom category that you want to delete, or click the **Select All** table button to select all custom categories.
2. Click the **Delete** table button.

Set Scanning Exclusions

After you have specified which IP addresses and ports the UTM scans for malware threats, you can set scanning exclusion rules for certain IP addresses and ports.

To save resources, you can configure scanning exclusions for IP addresses and ports that you know are secure. For example, if your network includes a web server that hosts web pages that are accessible by anyone on the Internet, the files that are hosted by your web

server do not need to be scanned. To prevent the UTM from scanning these files, you can configure a scanning exclusion for your web server.

➢ **To configure scanning exclusion rules:**

1. Select **Application Security > Scanning Exclusions**. The Scanning Exclusions screen displays. This screen shows the Scanning Exclusions table, which is empty if you have not specified any exclusions. (The following figure shows one exclusion rule in the table as an example.)
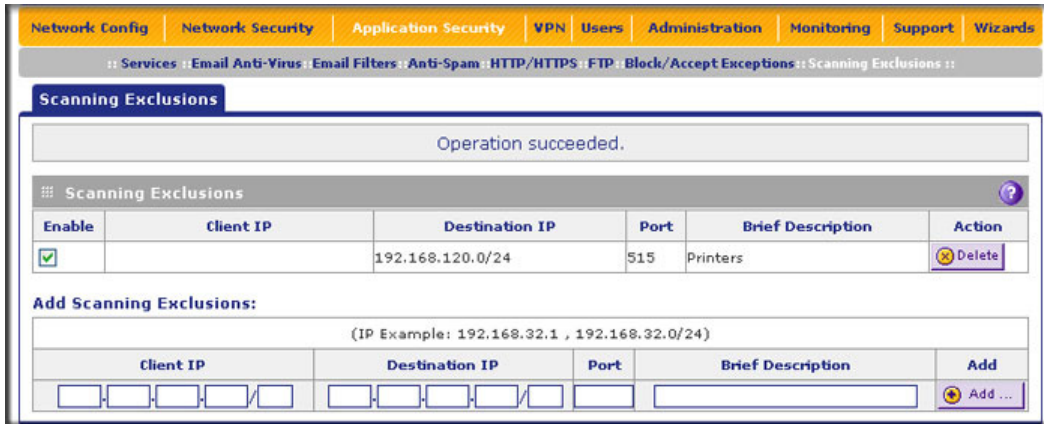
Figure 133.

2. In the Add Scanning Exclusions section of the screen, specify an exclusion rule as explained in the following table:

Table 53. Scanning Exclusion screen settings

Setting	Description
Client IP	Fill in the client IP address and optional subnet mask that are excluded from all scanning.
Destination IP	Fill in the destination IP address and optional subnet mask that are excluded from all scanning.
Port	Enter the number of the port that is excluded from all scanning.
Brief Description	Enter a description of the exclusion rule for identification and management purposes.

3. In the Add column, click the **Add** table button to add the exclusion rule to the Scanning Exclusions table. The new exclusion rule is enabled by default.

To disable a rule, select the check box in the Enable column for the rule. (Unlike the operation of the web management interface on other screens, you do not need to click any other button to disable the rule.)

To delete an exclusion rule from the Scanning Exclusions table, click the **Delete** table button in the Action column to the right of the rule that you want to delete.

Virtual Private Networking Using IPSec Connections

7

This chapter describes how to use the IP security (IPSec) virtual private networking (VPN) features of the UTM to provide secure, encrypted communications between your local network and a remote network or computer. This chapter contains the following sections:

- *Considerations for Dual WAN Port Systems (Multiple WAN Port Models Only)*
- *Use the IPSec VPN Wizard for Client and Gateway Configurations*
- *Test the Connection and View Connection and Status Information*
- *Manage IPSec VPN Policies*
- *Configure Extended Authentication (XAUTH)*
- *Assign IP Addresses to Remote Users (Mode Config)*
- *Configure Keep-Alives and Dead Peer Detection*
- *Configure NetBIOS Bridging with IPSec VPN*
- *Configure the PPTP Server (UTM9S Only)*
- *Configure the L2TP Server (UTM9S Only)*

> **Note:** The PPTP Server and L2TP Server configuration menus show on the UTM9S only.

Considerations for Dual WAN Port Systems (Multiple WAN Port Models Only)

On the multiple WAN port models only, if two WAN ports are configured, you can enable either auto-rollover mode for increased system reliability or load balancing mode for optimum bandwidth efficiency. Your WAN mode selection impacts how the VPN features need to be configured.

> **Note:** For the UTM9S only, you can also use a DSL interface in combination with a WAN interface for VPN tunnel failover.

The use of fully qualified domain names (FQDNs) in VPN policies is mandatory when the WAN ports function in auto-rollover mode or load balancing mode, and is also required for VPN tunnel failover. When the WAN ports function in load balancing mode, you cannot configure VPN tunnel failover. An FQDN is optional when the WAN ports function in load balancing mode if the IP addresses are static, but mandatory if the WAN IP addresses are dynamic.

See *Virtual Private Networks* on page 563 for more information about the IP addressing requirements for VPNs in the dual WAN modes.

For information about how to select and configure a Dynamic DNS service for resolving FQDNs, see *Configure Dynamic DNS* on page 87. For information about WAN mode configuration, see *Configure the WAN Mode* on page 75.

The following diagrams and table show how the WAN mode selection relates to VPN configuration.

WAN auto-rollover: FQDN required for VPN

Figure 134.

WAN load balancing: FQDN optional for VPN
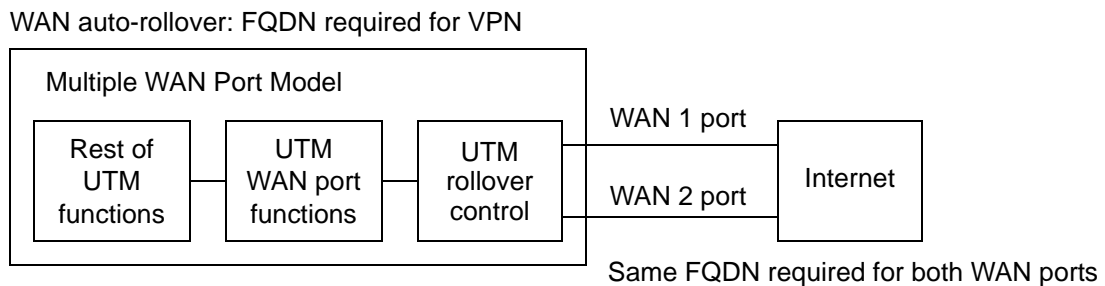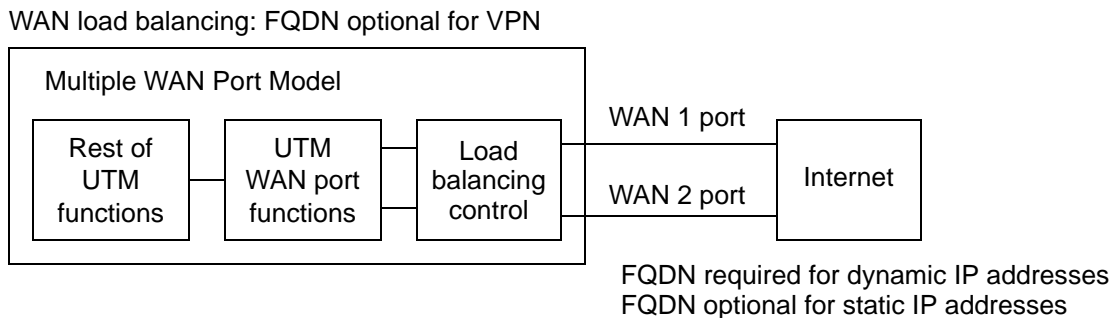
Figure 135.

The following table summarizes the WAN addressing requirements (FQDN or IP address) for a VPN tunnel in either dual WAN mode.

Table 54. IP addressing for VPNs in dual WAN port systems

Configuration and WAN IP address		Rollover mode[a]	Load balancing mode
VPN Road Warrior (client to gateway)	Fixed	FQDN required	FQDN Allowed (optional)
	Dynamic	FQDN required	FQDN required

Table 54. IP addressing for VPNs in dual WAN port systems (continued)

Configuration and WAN IP address		Rollover mode[a]	Load balancing mode
VPN Gateway-to-Gateway (gateway to gateway)	Fixed	FQDN required	FQDN Allowed (optional)
	Dynamic	FQDN required	FQDN required
VPN Telecommuter (client to gateway through a NAT router)	Fixed	FQDN required	FQDN Allowed (optional)
	Dynamic	FQDN required	FQDN required

a. After a rollover, all tunnels need to be reestablished using the new WAN IP address.

Use the IPSec VPN Wizard for Client and Gateway Configurations

You can use the IPSec VPN Wizard to configure multiple gateway or client VPN tunnel policies.

The following section provides wizard and NETGEAR ProSafe VPN Client software configuration procedures for the following scenarios:

• Using the wizard to configure a VPN tunnel between two VPN gateways

• Using the wizard to configure a VPN tunnel between a VPN gateway and a VPN client

Configuring a VPN tunnel connection requires that you specify all settings on both sides of the VPN tunnel to match or mirror each other precisely, which can be a daunting task. The VPN Wizard efficiently guides you through the setup procedure with a series of questions that determine the IPSec keys and VPN policies it sets up. The VPN Wizard also configures the settings for the network connection: security association (SA), traffic selectors, authentication algorithm, and encryption. The settings that are used by the VPN Wizard are based on the recommendations of the VPN Consortium (VPNC), an organization that promotes multivendor VPN interoperability.

Create Gateway-to-Gateway VPN Tunnels with the Wizard
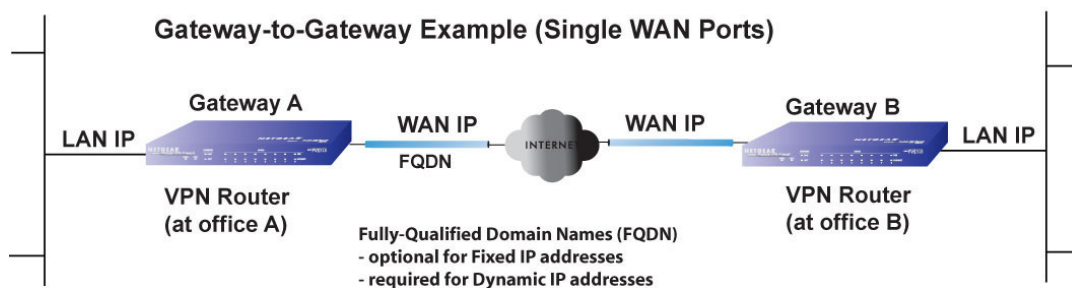
Figure 136.

➢ **To set up a gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays (see the following figure, which shows the VPN Wizard screen for the UTM50, and contains an example).

   The Connection Name and Remote IP Type section of the VPN Wizard screen shows the following minor differences for the various UTM models:

   • Single WAN port models. No WAN selection drop-down list.

   • Multiple WAN port models. A drop-down list to select the WAN interface, a check box to enable VPN rollover, and another drop-down list to select a WAN interface for VPN rollover. If the multiple WAN port model is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure this manually.

Figure 137.

To view the wizard default settings, click the **VPN Wizard Default Values** option arrow in the upper right of the screen. A pop-up screen displays (see the following figure), showing the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.

Figure 138.

2. Select the radio buttons and complete the fields and as explained in the following table:

Table 55. IPSec VPN Wizard settings for a gateway-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **Gateway** radio button. The local WAN port's IP address or Internet name displays in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.
This VPN tunnel will use following local WAN Interface (multiple WAN port models only)	Select a WAN interface from the drop-down list to specify which local WAN interface the VPN tunnel uses as the local endpoint.
	Select the **Enable RollOver?** check box to enable VPN rollover, and then select a WAN interface from the drop-down list to the right of the check box to specify the interface to which the VPN rollover should occur. **Note:** If the multiple WAN port model is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure this manually.

Table 55. IPSec VPN Wizard settings for a gateway-to-gateway tunnel (continued)

Setting	Description
End Point Information[a]	
What is the Remote WAN's IP Address or Internet Name?	Enter the IP address or Internet name (FQDN) of the WAN interface on the remote VPN tunnel endpoint.
What is the Local WAN's IP Address or Internet Name?	When you select the Gateway radio button in the About VPN Wizard section of the screen, the IP address of the UTM's active WAN interface is automatically entered.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	Enter the LAN IP address of the remote gateway. **Note:** The remote LAN IP address needs to be in a different subnet than the local LAN IP address. For example, if the local subnet is 192.168.1.x, then the remote subnet could be 192.168.10.x. but could not be 192.168.1.x. If this information is incorrect, the tunnel will fail to connect.
What is the remote LAN Subnet Mask?	Enter the LAN subnet mask of the remote gateway.

a. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and a FQDN is not supported.

Tip: To ensure that tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keep-alives, which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive. For more information, see *Configure Keep-Alives* on page 297.

Tip: For DHCP WAN configurations, first set up the tunnel with IP addresses. After you have validated the connection, you can use the wizard to create new policies using the FQDN for the WAN addresses.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen. By default, the VPN policy is enabled.
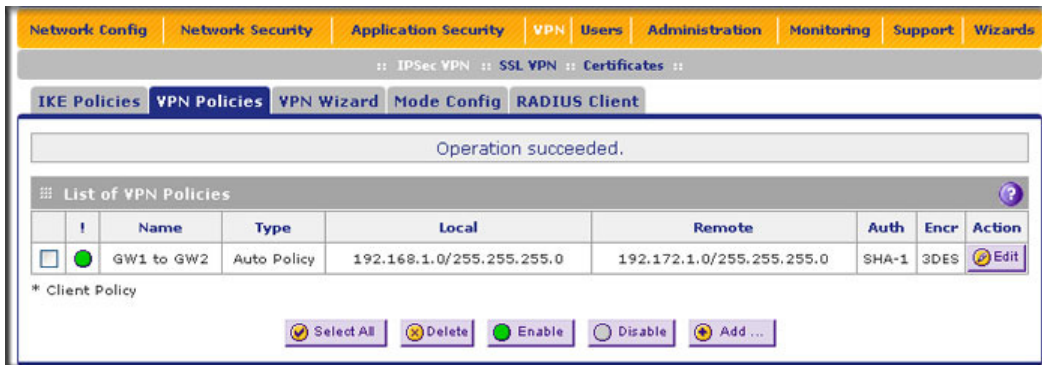
Figure 139.

4. Configure a VPN policy on the remote gateway that allows connection to the UTM.

5. Activate the IPSec VPN connection:

   a. Select **Monitoring > Active Users & VPNs > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays. (The UTM9S also shows the PPTP Active Users and L2TP Active Users tabs.)
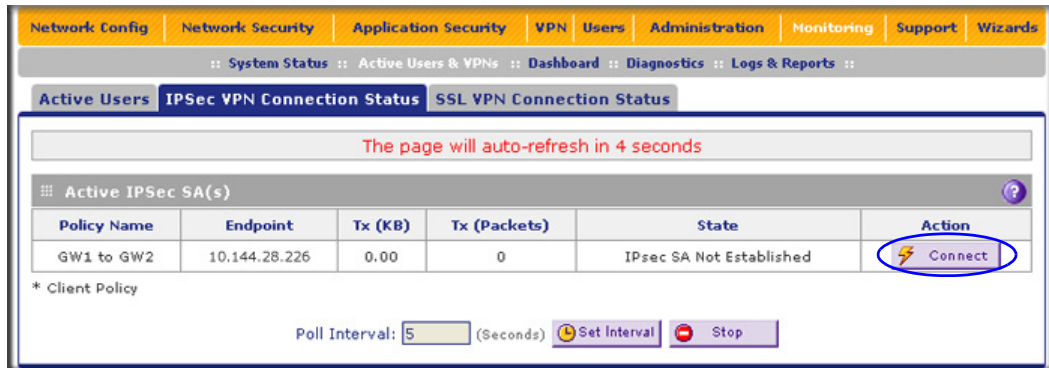
Figure 140.

   b. Locate the policy in the table, and click the **Connect** table button. The IPSec VPN connection becomes active.

Note: When using FQDNs, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

Create a Client-to-Gateway VPN Tunnel
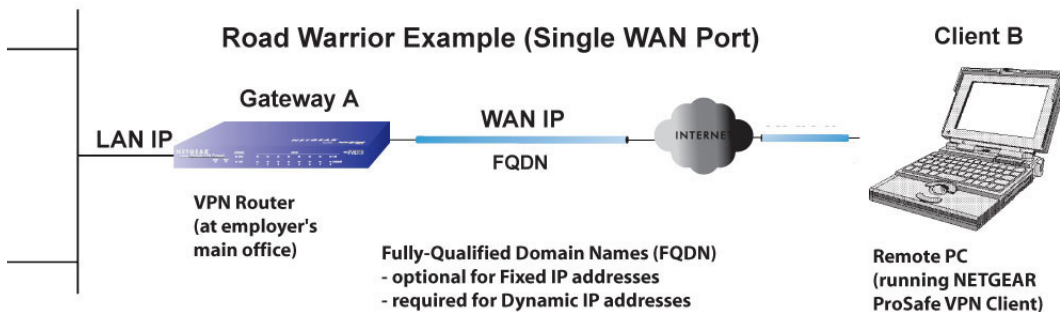
Figure 141.

To configure a VPN client tunnel, follow the steps in the following sections:

- *Use the VPN Wizard to Configure the Gateway for a Client Tunnel* on page 244.
- *Use the NETGEAR VPN Client Wizard to Create a Secure Connection* on page 246 or *Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 251.

Use the VPN Wizard to Configure the Gateway for a Client Tunnel

➢ **To set up a client-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays (see the following figure, which contains an example for a multiple WAN port model). The WAN radio drop-down lists are shown on the VPN Wizard screen for the multiple WAN port models but not on the VPN Wizard screen for the single WAN port models.

Figure 142.

To display the wizard default settings, click the **VPN Wizard default values** option arrow in the upper right of the screen. A pop-up screen displays (see *Figure 138* on page 241), showing the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.

2. Select the radio buttons and complete the fields and as explained in the following table:

Table 56. IPSec VPN Wizard settings for a client-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **VPN Client** radio button. The default remote FQDN (utm_remote.com) and the default local FQDN (utm_local.com) display in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway, or the remote VPN client. This key needs to have a minimum length of 8 characters and cannot exceed 49 characters.
This VPN tunnel will use following local WAN Interface (multiple WAN port models only)	Select a WAN interface from the drop-down list to specify which local WAN interface the VPN tunnel uses as the local endpoint.
	Select the **Enable RollOver?** check box to enable VPN rollover, and then select a WAN interface from the drop-down list to the right of the check box to specify the interface to which the VPN rollover should occur.
	Note: If the multiple WAN port model is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure this manually.
End Point Information[a]	
What is the Remote Identifier Information?	When you select the Client radio button in the About VPN Wizard section of the screen, the default remote FQDN (utm_remote.com) is automatically entered. Use the default remote FQDN, or enter another FQDN.
What is the Local Identifier Information?	When you select the Client radio button in the About VPN Wizard section of the screen, the default local FQDN (utm_local.com) is automatically entered. Use the default local FQDN, or enter another FQDN.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	These fields are masked out for VPN client connections.
What is the remote LAN Subnet Mask?	

a. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen. By default, the VPN policy is enabled.

Figure 143.

Note: When you are using FQDNs, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

---

4. Optional step: Collect the information that you need to configure the VPN client. You can print the following table to help you keep track of this information.

Table 57. Information required to configure the VPN client

Component	Example	Information to be collected
Pre-shared key	I7!KL39dFG_8	
Remote identifier information	utm_remote.com	
Local identifier information	utm_local.com	
Router's LAN network IP address	192.168.1.0	
Router's LAN network mask	255.255.255.0	
Router's WAN IP address	10.34.116.22	

Use the NETGEAR VPN Client Wizard to Create a Secure Connection

The VPN client lets you set up the VPN connection manually (see *Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 251) or with the integrated Configuration Wizard, which is the easier and preferred method. The Configuration Wizard configures the default settings and provides basic interoperability so that the VPN client can easily communicate with the UTM (or third-party VPN devices). The Configuration Wizard does not let you enter the local and remote IDs, so you need to manually enter this information.

Note: Perform these tasks from a PC that has the NETGEAR ProSafe VPN Client installed.

➢ **To use the Configuration Wizard to set up a VPN connection between the VPN client and the UTM:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.
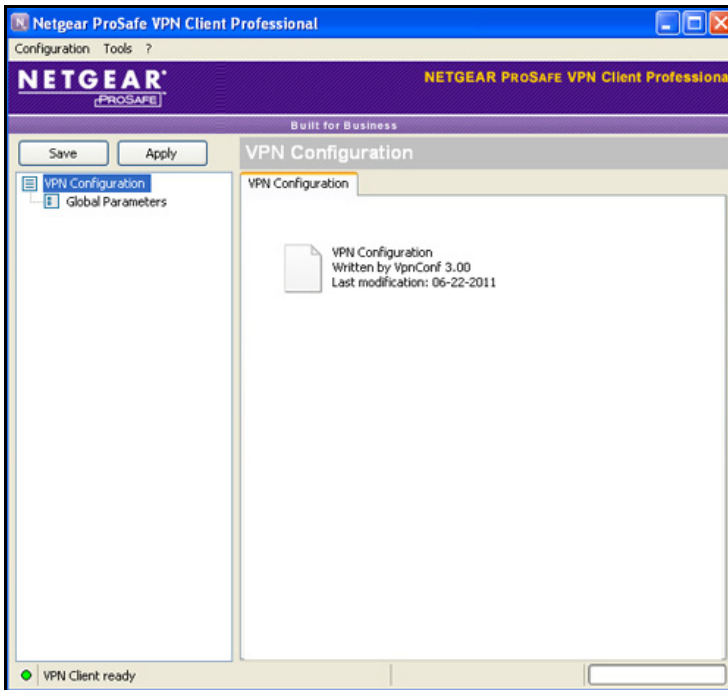
Figure 144.

1. From the main menu on the Configuration Panel screen, select **Configuration > Wizard**. The Choice of the remote equipment wizard screen (screen 1 of 3) displays.
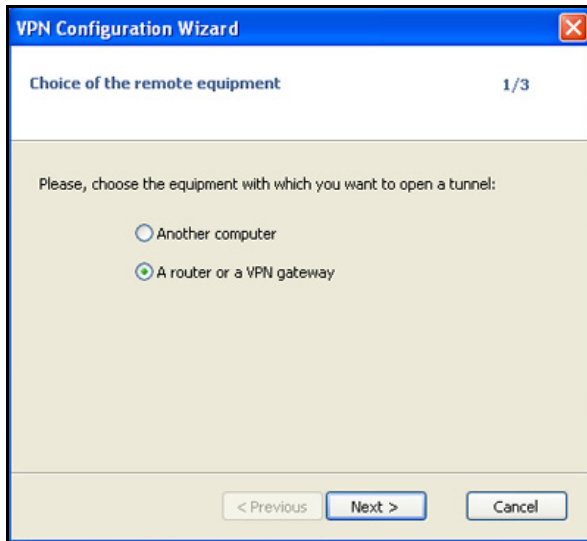
Figure 145.

2. Select the **A router or a VPN gateway** radio button, and click **Next**. The VPN tunnel parameters wizard screen (screen 2 of 3) displays.
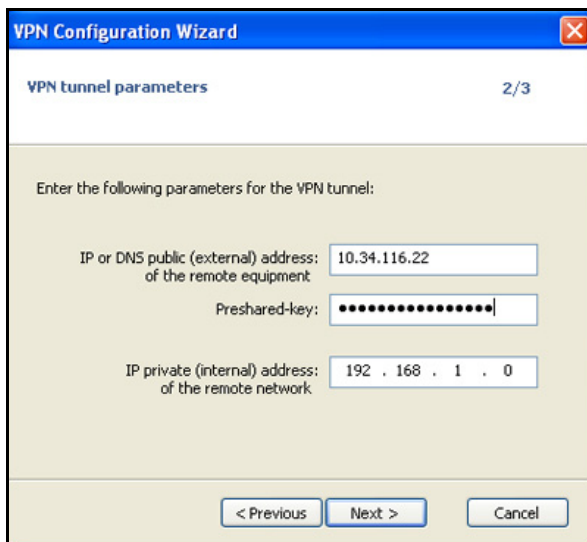
Figure 146.

3. Specify the following VPN tunnel parameters:

- **IP or DNS public (external) address of the remote equipment**. Enter the remote IP address or DNS name of the UTM. For example, enter **10.34.116.22**.

- **Preshared key**. Enter the pre-shared key that you already specified on the UTM. For example, enter **I7!KL39dFG_8**.

- **IP private (internal) address of the remote network**. Enter the remote private IP address of the UTM. For example, enter **192.168.1.0**. This IP address enables communication with the entire 192.168.1.x subnet.

4. Click **Next**. The Configuration Summary wizard screen (screen 3 of 3) displays.
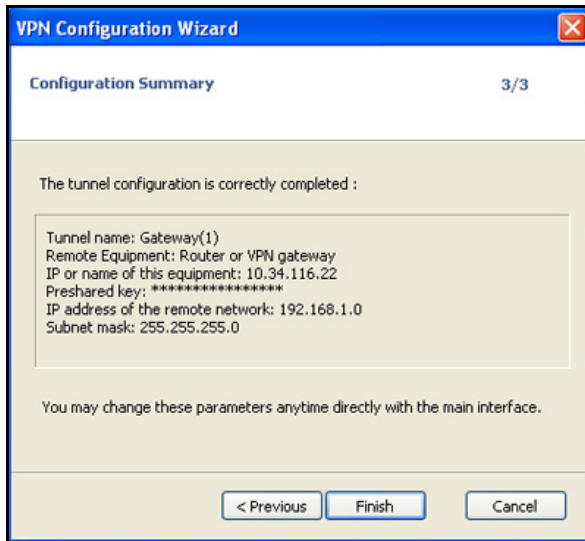
Figure 147.

5. This screen is a summary screen of the new VPN configuration. Click **Finish**.

6. Specify the local and remote IDs:

   a. In the tree list pane of the Configuration Panel screen, click **Gateway** (the default name given to the authentication phase). The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

   b. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.
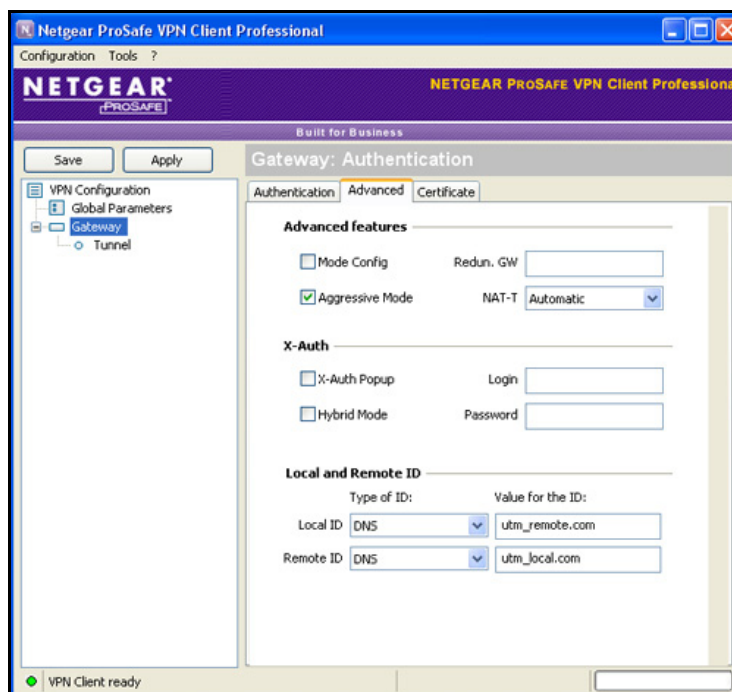
Figure 148.

c. Specify the settings that are explained in the following table.

Table 58. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the UTM.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and UTM to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the UTM configuration. As the value of the ID, enter **utm_remote.com** as the local ID for the VPN client. **Note:** The remote ID on the UTM is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the UTM and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the UTM configuration. As the value of the ID, enter **utm_local.com** as the remote ID for the UTM. **Note:** The local ID on the UTM is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the UTM and then enter router.com as the remote ID on the VPN client.

7. Configure the global parameters:

    a. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.
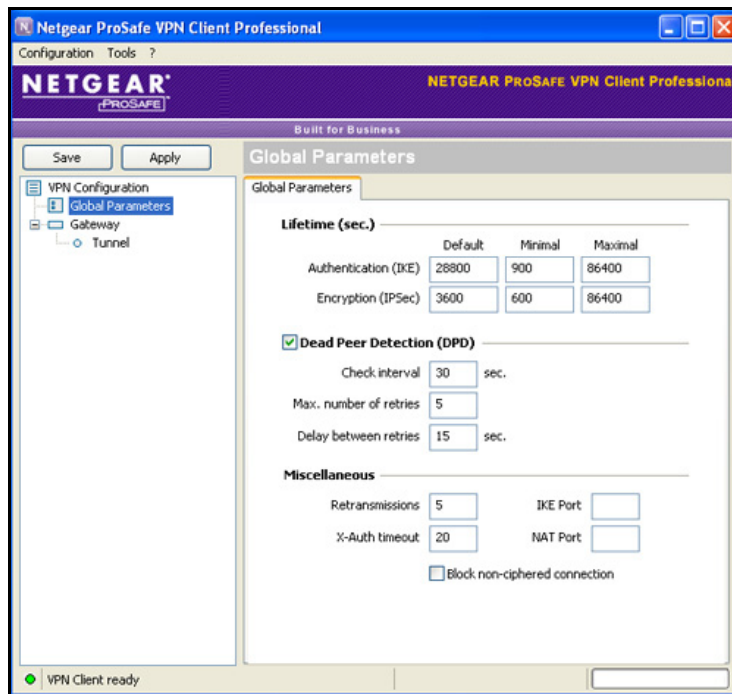
Figure 149.

b. Specify the default lifetimes in seconds:

- **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the UTM.

- **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the UTM.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN client configuration is now complete.

Instead of using the wizard on the VPN client, you can also manually configure the VPN client, which is explained in the following section.

Manually Create a Secure Connection Using the NETGEAR VPN Client

> **Note:** Perform these tasks from a PC that has the NETGEAR ProSafe VPN Client installed.

To manually configure a VPN connection between the VPN client and the UTM, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and then specify the global parameters.

Configure the Authentication Settings (Phase 1 Settings)

➢ **To create new authentication settings:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.
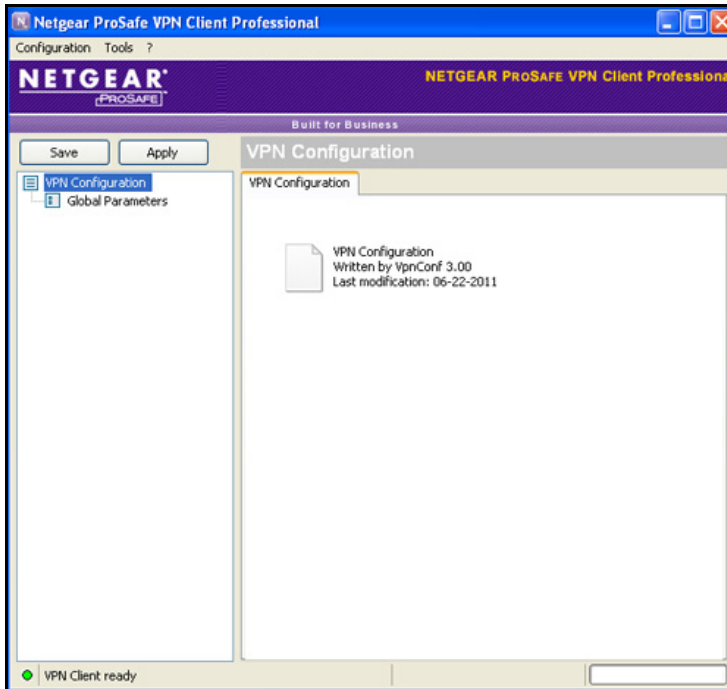
Figure 150.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.

Figure 151.

3. Change the name of the authentication phase (the default is Gateway):

   a. Right-click the authentication phase name.

   b. Select **Rename**.

   c. Type **vpn_client**.

   d. Click anywhere in the tree list pane.

> *Note:* *This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.
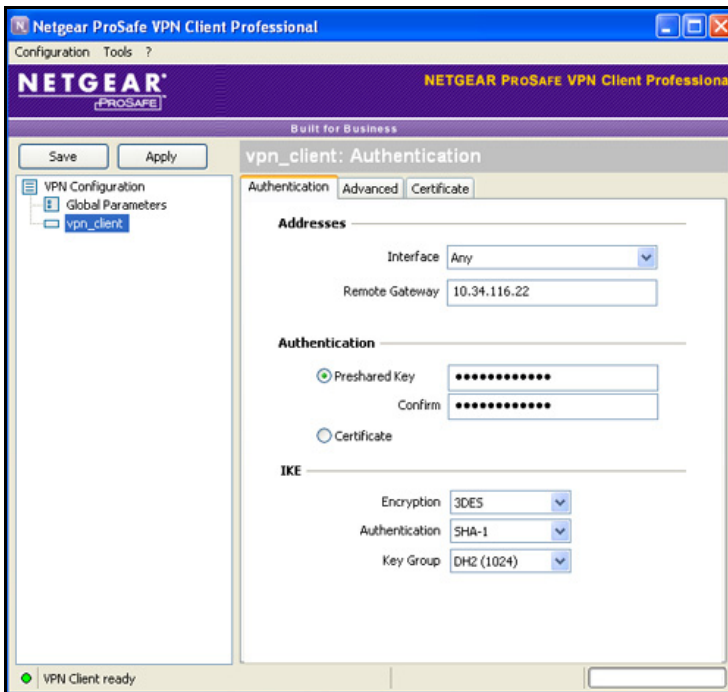
Figure 152.

4. Specify the settings that are explained in the following table.

Table 59. VPN client authentication settings

Setting	Description	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the UTM. For example, enter **10.34.116.22**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the UTM. For example, enter **I7!KL39dFG_8**. Confirm the key in the Confirm field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On the UTM, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

6. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.

Figure 153.

7. Specify the settings that are explained in the following table.

Table 60. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the UTM.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and UTM to negotiate NAT-T.

Table 60. VPN client advanced authentication settings (continued)

Setting	Description
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the UTM configuration. As the value of the ID, enter **utm_remote.com** as the local ID for the VPN client. **Note:** The remote ID on the UTM is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the UTM and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the UTM configuration. As the value of the ID, enter **utm_local.com** as the remote ID for the UTM. **Note:** The local ID on the UTM is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the UTM and then enter router.com as the remote ID on the VPN client.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the IPSec Configuration (Phase 2 Settings)

> **Note:** On the UTM, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **vpn_client** authentication phase name, and then select **New Phase 2**.

2. Change the name of the IPSec configuration (the default is Tunnel):

    a. Right-click the IPSec configuration name.

    b. Select **Rename**.

    c. Type **netgear_platform**.

    d. Click anywhere in the tree list pane.

    Note: This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.
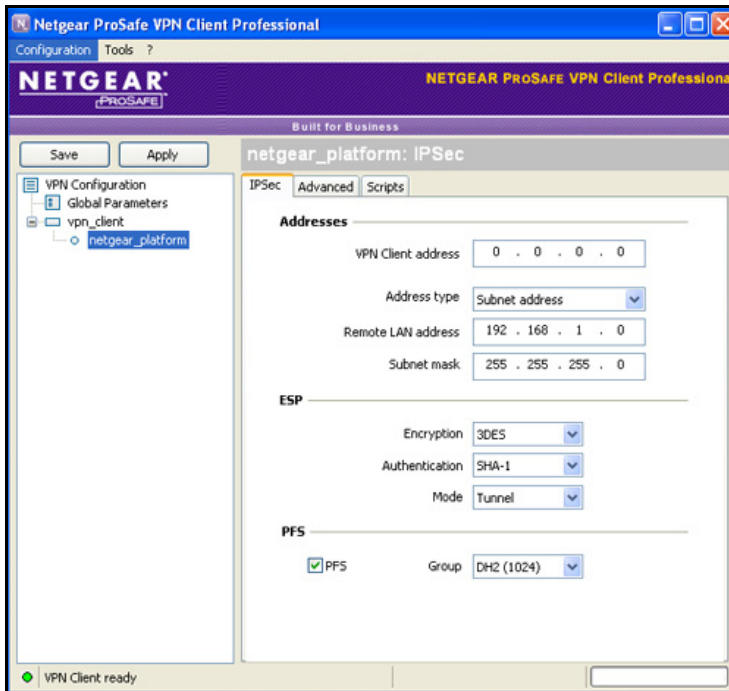
Figure 154.

3. Specify the settings that are explained in the following table.

Table 61. VPN client IPSec configuration settings

Setting	Description
VPN Client address	Either enter **0.0.0.0** as the IP address, or enter a virtual IP address that is used by the VPN client in the UTM's LAN; the computer (for which the VPN client opened a tunnel) appears in the LAN with this IP address.
Address Type	Select **Subnet address** from the drop-down list. This selection defines which addresses the VPN client can communicate with after the VPN tunnel is established.
Remote LAN address	Enter **192.168.1.0** as the remote IP address (that is, LAN network address) of the gateway that opens the VPN tunnel.
Subnet mask	Enter **255.255.255.0** as the remote subnet mask of the gateway that opens the VPN tunnel.

Table 61. VPN client IPSec configuration settings (continued)

Setting	Description	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down list. **Note:** On the UTM, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure the Global Parameters

➢ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.

Figure 155.

2. Specify the default lifetimes in seconds:

   • **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the UTM.

   • **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the UTM.

3. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The UTM configuration is now complete.

Test the Connection and View Connection and Status Information

Both the NETGEAR ProSafe VPN Client and the UTM provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a connection.

Test the NETGEAR VPN Client Connection

There are many ways to establish a connection. The following procedures assume that you use the default authentication phase name *Gateway* and the default IPSec configuration name *Tunnel*. If you manually set up the connection and changed the names, use *vpn_client* (or any other name that you have configured) as the authentication phase name and *netgear_platform* (or any other name that you have configured) as the IPSec configuration name.

➢ **To establish a connection, use one of the following three methods:**

   • **Use the Configuration Panel screen**. In the tree list pane of the Configuration Panel screen, perform *one* of the following tasks:

      - Click the **Tunnel** IPSec configuration name, and press **Ctrl+O.**

      - Right-click the **Tunnel** IPSec configuration name, and select **Open tunnel**.
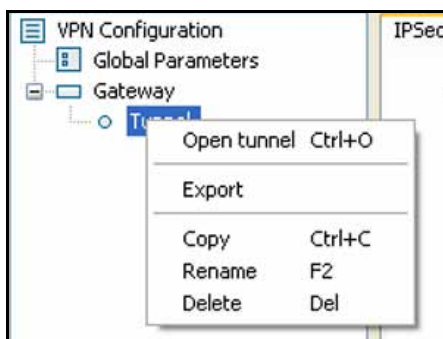
Figure 156.

- **Use the Connection Panel screen**. On the main menu of the Configuration Panel screen, select **Tools > Connection Panel** to open the Connection Panel screen.

  Perform *one* of the following tasks:

  - Double-click **Gateway-Tunnel**.
  - Right-click **Gateway-Tunnel**, and select **Open tunnel**.
  - Click **Gateway-Tunnel**, and press **Ctrl+O**.

Figure 157.

- **Use the system-tray icon**. Right-click the system tray icon, and select **Open tunnel 'Tunnel'**.
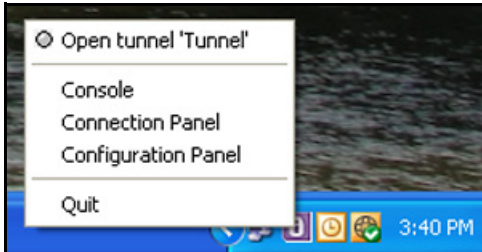
Figure 158.

Whichever way you choose to open the tunnel, when the tunnel opens successfully, the *Tunnel opened* message displays above the system tray:
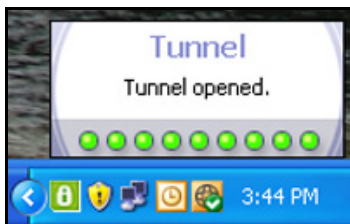
Figure 159.

Once launched, the VPN client displays an icon in the system tray that indicates whether or not a tunnel is opened, using a color code:

 Green icon:
at least one VPN tunnel opened

 Purple icon:
no VPN tunnel opened

Figure 160.

NETGEAR VPN Client Status and Log Information

➢ **To view detailed negotiation and error information on the NETGEAR VPN client:**

Right-click the VPN client icon in the system tray, and select **Console**. The VPN Client Console Active screen displays.

Figure 161.

View the UTM IPSec VPN Connection Status

To review the status of current IPSec VPN tunnels, select **Monitoring > Active Users & VPNs > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays. (The following figure shows an IPSec SA as an example. The UTM9S also shows the PPTP Active Users and L2TP Active Users tabs.)

Figure 162.

The Active IPSec SA(s) table lists each active connection with the information that is described in the following table. The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and then click the **Set Interval** button. To stop polling, click the **Stop** button.

Table 62. IPSec VPN Connection Status screen information

Setting	Description
Policy Name	The name of the VPN policy that is associated with this SA.
Endpoint	The IP address on the remote VPN endpoint.
Tx (KB)	The amount of data that is transmitted over this SA.
Tx (Packets)	The number of IP packets that are transmitted over this SA.
State	The current status of the SA. Phase 1 is the authentication phase, and Phase 2 is key exchange phase. If there is no connection, the status is IPSec SA Not Established.
Action	Click the **Connect** table button to build the connection, or click the **Disconnect** table button to terminate the connection.

View the UTM IPSec VPN Log

> **To query the IPSec VPN log:**

1. Select **Monitoring > Logs & Reports > Logs Query**. The Logs Query screen displays.

2. From the Log Type drop-down list, select **IPSEC VPN**. The IPSec VPN logs display.
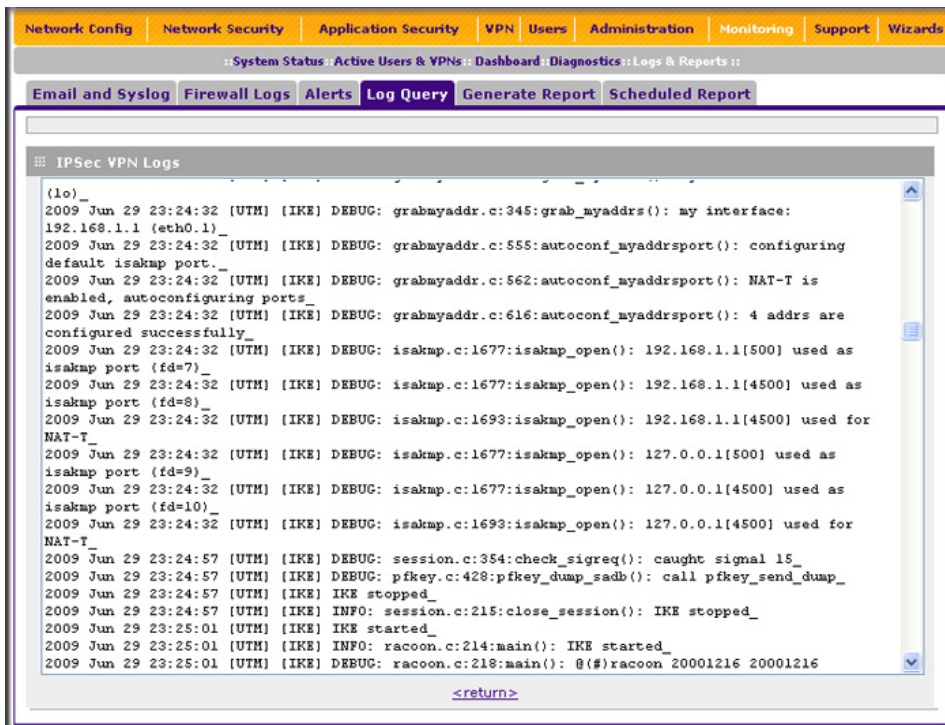
Figure 163.

Manage IPSec VPN Policies

After you have used the VPN Wizard to set up a VPN tunnel, a VPN policy and an IKE policy are stored in separate policy tables. The name that you selected as the VPN tunnel connection name during the VPN Wizard setup identifies both the VPN policy and IKE policy. You can edit existing policies, or manually add new VPN and IKE policies directly in the policy tables.

Manage IKE Policies

The Internet Key Exchange (IKE) protocol performs negotiations between the two VPN gateways and provides automatic management of the keys that are used for IPSec connections. It is important to remember that:

- An automatically generated VPN policy (auto policy) needs to use the IKE negotiation protocol.

- A manually generated VPN policy (manual policy) cannot use the IKE negotiation protocol.

IKE policies are activated when the following situations occur:

1. The VPN policy selector determines that some traffic matches an existing VPN policy:
    - If the VPN policy is of an auto policy type, the IKE policy that is specified in the Auto Policy Parameters section of the Add VPN Policy screen (see *Figure 167* on page 272) is used to start negotiations with the remote VPN gateway.
    - If the VPN policy is of a manual policy type, the settings that are specified in the Manual Policy Parameters section of the Add VPN Policy screen (see *Figure 167* on page 272) are accessed, and the first matching IKE policy is used to start negotiations with the remote VPN gateway:
        - If negotiations fail, the next matching IKE policy is used.
        - If none of the matching IKE policies are acceptable to the remote VPN gateway, then a VPN tunnel cannot be established.

2. An IKE session is established, using the security association (SA) settings that are specified in a matching IKE policy:
    - Keys and other settings are exchanged.
    - An IPSec SA is established, using the settings that are specified in the VPN policy.

The VPN tunnel is then available for data transfer.

When you use the VPN Wizard to set up a VPN tunnel, an IKE policy is established and populated in the List of IKE Policies, and is given the same name as the new VPN connection name. You can also edit exiting policies or add new IKE policies from the IKE Policies screen.

IKE Policies Screen

➢ **To access the IKE Policies screen:**

Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view. (The following figure shows some examples.)
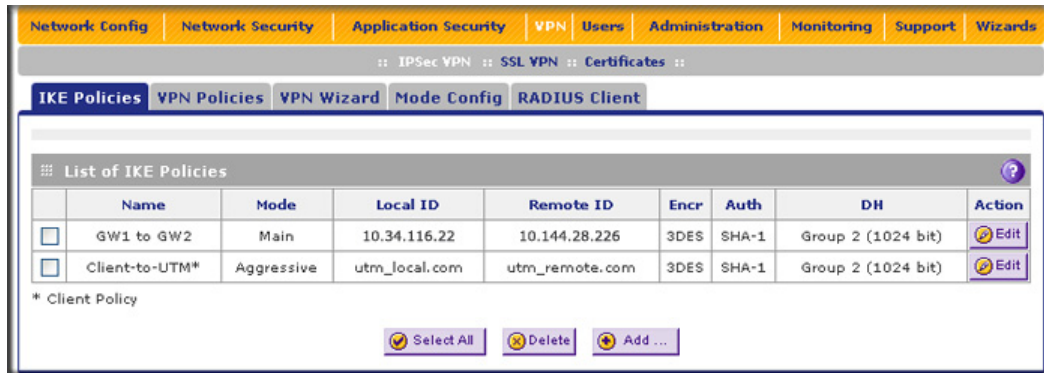
Figure 164.

Each policy contains the data that are explained in the following table. These fields are explained in more detail in *Table 64* on page 266.

Table 63. List of IKE Policies table information

Setting	Description
Name	The name that identifies the IKE policy. When you use the VPN Wizard to set up a VPN policy, an accompanying IKE policy is automatically created with the same name that you select for the VPN policy. **Note:** The name is not supplied to the remote VPN endpoint.
Mode	The exchange mode: Main or Aggressive.
Local ID	The IKE/ISAKMP identifier of the UTM. The remote endpoint needs to have this value as its remote ID.
Remote ID	The IKE/ISAKMP identifier of the remote endpoint, which needs to have this value as its local ID.
Encr	The encryption algorithm that is used for the IKE security association (SA). This setting needs to match the setting on the remote endpoint.
Auth	The authentication algorithm that is used for the IKE SA. This setting needs to match the setting on the remote endpoint.
DH	The Diffie-Hellman (DH) group that is used when keys are exchanged. This setting needs to match the setting on the remote endpoint.

➢ **To delete one or more IKE polices:**

1. Select the check box to the left of each policy that you want to delete, or click the **Select All** table button to select all IKE policies.

2. Click the **Delete** table button.

For information about how to add or edit an IKE policy, see *Manually Add or Edit an IKE Policy* on page 264.

> **Note:** You *can* delete or edit an IKE policy for which the VPN policy is
> active without first disabling or deleting the VPN policy. In earlier
> firmware releases of the UTM you first had to disable or delete the
> VPN policy, but this restriction has been removed.

Manually Add or Edit an IKE Policy

➢ **To manually add an IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see the previous figure).

2. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays (see the following figure, which shows a multiple WAN port model screen). The WAN drop-down lists (next to Select Local Gateway) are shown on the Add IKE Policy screen for the multiple WAN port models but not on the Add IKE Policy screen for the single WAN port models.

Figure 165.

3. Complete the fields, select the radio buttons, and make your selections from the drop-down lists as explained in the following table:

Table 64. Add IKE Policy screen settings

Setting	Description	
Mode Config Record		
Do you want to use Mode Config Record?	Specify whether or not the IKE policy uses a Mode Config record. For information about how to define a Mode Config record, see *Mode Config Operation* on page 281. Select one of the following radio buttons: • **Yes**. IP addresses are assigned to remote VPN clients. You need to select a Mode Config record from the drop-down list. Because Mode Config functions only in Aggressive mode, selecting the Yes radio button sets the tunnel exchange mode to Aggressive mode and disables the Main mode. Mode Config also requires that both the local and remote endpoints are defined by their FQDNs. • **No**. Disables Mode Config for this IKE policy.	
	Select Mode Config Record	From the drop-down list, select one of the Mode Config records that you defined on the Add Mode Config Record screen (see *Configure Mode Config Operation on the UTM* on page 281). **Note:** Click the **View Selected** button to open the Selected Mode Config Record Details pop-up screen.
General		
Policy Name	A descriptive name of the IKE policy for identification and management purposes. **Note:** The name is not supplied to the remote VPN endpoint.	
Direction / Type	From the drop-down list, select the connection method for the UTM: • **Initiator**. The UTM initiates the connection to the remote endpoint. • **Responder**. The UTM responds only to an IKE request from the remote endpoint. • **Both**. The UTM can both initiate a connection to the remote endpoint and respond to an IKE request from the remote endpoint.	
Exchange Mode	From the drop-down list, select the mode of exchange between the UTM and the remote VPN endpoint: • **Main**. This mode is slower than the Aggressive mode but more secure. • **Aggressive**. This mode is faster than the Main mode but less secure. **Note:** If you specify either an FQDN or a user FQDN name as the local ID or remote ID (see the Identifier Type sections later in this table), the Aggressive mode is automatically selected.	
Local		
Select Local Gateway (multiple WAN port models only)	Select a WAN interface from the drop-down list to specify the WAN interface for the local gateway.	

Table 64. Add IKE Policy screen settings (continued)

Setting	Description	
Identifier Type	From the drop-down list, select one of the following ISAKMP identifiers to be used by the UTM, and then specify the identifier in the Identifier field: • **Local WAN IP**. The WAN IP address of the UTM. When you select this option, the Identifier field automatically shows the IP address of the selected WAN interface. • **FQDN**. The Internet address for the UTM. • **User FQDN**. The email address for a local VPN client or the UTM. • **DER ASN1 DN**. A distinguished name (DN) that identifies the UTM in the DER encoding and ASN.1 format.	
	Identifier	Depending on the selection of the Identifier Type drop-down list, enter the IP address, email address, FQDN, or distinguished name.
Remote		
Identifier Type	From the drop-down list, select one of the following ISAKMP identifiers to be used by the remote endpoint, and then specify the identifier in the Identifier field: • **Remote WAN IP**. The WAN IP address of the remote endpoint. When you select this option, the Identifier field automatically shows the IP address of the selected WAN interface. • **FQDN**. The FQDN for a remote gateway. • **User FQDN**. The email address for a remote VPN client or gateway. • **DER ASN1 DN**. A distinguished name (DN) that identifies the remote endpoint in the DER encoding and ASN.1 format.	
	Identifier	Depending on the selection of the Identifier Type drop-down list, enter the IP address, email address, FQDN, or distinguished name.
IKE SA Parameters		
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.	
Authentication Algorithm	From the drop-down list, select one of the following algorithms to use in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest. • **AES-256** (UTM9S only). AES with a 256-bit key size. • **AES-512** (UTM9S only). AES with a 512-bit key size.	

Table 64. Add IKE Policy screen settings (continued)

Setting	Description	
Authentication Method	Select one of the following radio buttons to specify the authentication method: • **Pre-shared key**. A secret that is shared between the UTM and the remote endpoint. • **RSA-Signature**. Uses the active self-signed certificate that you uploaded on the Certificates screen (see *Manage Self-Signed Certificates* on page 384). The pre-shared key is masked out when you select RSA-Signature.	
	Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote (") in the key.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**. • **Group 14 (2048 bit)** (UTM9S only). • **Group 15 (3072 bit)** (UTM9S only). • **Group 16 (4096 bit)** (UTM9S only). **Note:** Ensure that the DH Group is configured identically on both sides.	
SA-Lifetime (sec)	The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying occurs. The default is 28800 seconds (8 hours).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 297.	Select a radio button to specify whether or not Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the UTM detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the UTM attempts to reconnect in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle.
	Reconnect after failure count	The maximum number of DPD failures before the UTM tears down the connection and then attempts to reconnect to the peer. The default is 3 failures.

Table 64. Add IKE Policy screen settings (continued)

Setting	Description		
Extended Authentication			
XAUTH Configuration **Note:** For more information about XAUTH and its authentication modes, see *Configure XAUTH for VPN Clients* on page 277.	Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The UTM functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, or RADIUS CHAP. • **IPSec Host**. The UTM functions as a VPN client of the remote gateway. In this configuration the UTM is authenticated by a remote gateway with a user name and password combination.		
	Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the UTM's user database. You can add users on the Add User screen (see *User Database Configuration* on page 278). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the UTM connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 279. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 279.	
	Username	The user name for XAUTH.	
	Password	The password for XAUTH.	

4. Click **Apply** to save your settings. The IKE policy is added to the List of IKE Policies table.

➢ **To edit an IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 164* on page 263).

2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy that you want to edit. The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen (see *Figure 165* on page 265).

3. Modify the settings that you wish to change (see the previous table).

4. Click **Apply** to save your changes. The modified IKE policy is displayed in the List of IKE Policies table.

Manage VPN Policies

You can create two types of VPN policies. When you use the VPN Wizard to create a VPN policy, only the Auto method is available.

- **Manual**. You manually enter all settings (including the keys) for the VPN tunnel on the UTM and on the remote VPN endpoint. No third-party server or organization is involved.

- **Auto**. Some settings for the VPN tunnel are generated automatically through the use of the IKE (Internet Key Exchange) Protocol to perform negotiations between the two VPN endpoints (the local ID endpoint and the remote ID endpoint). You still need to manually enter all settings on the remote VPN endpoint (unless the remote VPN endpoint also has a VPN Wizard).

In addition, a certification authority (CA) can also be used to perform authentication (see *Manage Digital Certificates for VPN Connections* on page 381). For gateways to use a CA, each VPN gateway needs to have a certificate from the CA. For each certificate, there is both a public key and a private key. The public key is freely distributed, and is used by any sender to encrypt data intended for the receiver (the key owner). The receiver then uses its private key to decrypt the data (without the private key, decryption is impossible). The use of certificates for authentication reduces the amount of data entry that is required on each VPN endpoint.

VPN Policies Screen

The VPN Policies screen allows you to add additional policies—either Auto or Manual—and to manage the VPN policies already created. You can edit policies, enable or disable policies, or delete them entirely. These are the rules for VPN policy use:

- Traffic covered by a policy is automatically sent through a VPN tunnel.

- When traffic is covered by two or more policies, the first matching policy is used. (In this situation, the order of the policies is important. However, if you have only one policy for each remote VPN endpoint, then the policy order is not important.)

- The VPN tunnel is created according to the settings in the security association (SA).

- The remote VPN endpoint needs to have a matching SA; otherwise, it refuses the connection.

To access the VPN Policies screen, select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays. (The following figure shows some examples.)
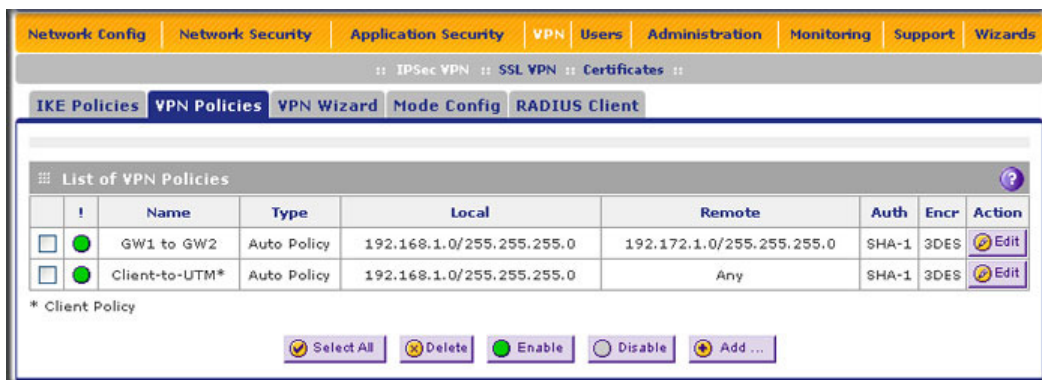
Figure 166.

Each policy contains the data that are explained in the following table. These fields are explained in more detail in *Table 66* on page 273.

Table 65. List of VPN Policies table information

Setting	Description
! (Status)	Indicates whether the policy is enabled (green circle) or disabled (gray circle). To enable or disable a policy, select the check box adjacent to the circle, and click the **Enable** or **Disable** table button, as appropriate.
Name	The name that identifies the VPN policy. When you use the VPN Wizard to create a VPN policy, the name of the VPN policy (and of the automatically created accompanying IKE policy) is the connection name.
Type	Auto or Manual as described previously (Auto is used during VPN Wizard configuration).
Local	IP address (either a single address, range of address, or subnet address) on your LAN. Traffic needs to be from (or to) these addresses to be covered by this policy. (The subnet address is supplied as the default IP address when you are using the VPN Wizard.)
Remote	IP address or address range of the remote network. Traffic needs to be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask.)
Auth	The authentication algorithm that is used for the VPN tunnel. This setting needs to match the setting on the remote endpoint.
Encr	The encryption algorithm that is used for the VPN tunnel. This setting needs to match the setting on the remote endpoint.

➢ **To delete one or more VPN polices:**

1. Select the check box to the left of each policy that you want to delete, or click the **Select All** table button to select all VPN policies.
2. Click the **Delete** table button.

➢ **To enable or disable one or more VPN policies:**

1. Select the check box to the left of each policy that you want to enable or disable, or click the **Select All** table button to select all VPN policies.
2. Click the **Enable** or **Disable** table button.

For information about how to add or edit a VPN policy, see *Manually Add or Edit a VPN Policy* on this page.

> **Note:** You *can* delete or edit an IKE policy for which the VPN policy is active without first disabling or deleting the VPN policy. In earlier firmware releases of the UTM you first had to disable or delete the VPN policy, but this restriction has been removed.

Manually Add or Edit a VPN Policy

➢ **To manually add a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 166* on page 270).

2. Under the List of VPN Policies table, click the **Add** table button. The Add VPN Policy screen displays (see the following figure, which shows the UTM50 screen). The WAN drop-down list (next to Select Local Gateway) is shown on the Add VPN Policy screen for the multiple WAN port models but not on the Add VPN Policy screen for the single WAN port models.

Figure 167.

3. Complete the fields, select the radio buttons and check boxes, and make your selections from the drop-down lists as explained in the following table:

Table 66. Add New VPN Policy screen settings

Setting	Description
General	
Policy Name	A descriptive name of the VPN policy for identification and management purposes. **Note:** The name is not supplied to the remote VPN endpoint.
Policy Type	From the drop-down list, select one of the following policy types: • **Auto Policy**. Some settings (the ones in the Manual Policy Parameters section of the screen) for the VPN tunnel are generated automatically. • **Manual Policy**. All settings need to be specified manually, including the ones in the Manual Policy Parameters section of the screen.
Select Local Gateway (multiple WAN port models only)	Select a WAN interface from the drop-down list to specify the WAN interface for the local gateway.
Remote Endpoint	Select a radio button to specify how the remote endpoint is defined: • **IP Address**. Enter the IP address of the remote endpoint in the fields to the right of the radio button. • **FQDN**. Enter the FQDN of the remote endpoint in the field to the right of the radio button.
Enable NetBIOS?	Select this check box to allow NetBIOS broadcasts to travel over the VPN tunnel. For more information about NetBIOS, see *Configure NetBIOS Bridging with IPSec VPN* on page 299. This feature is disabled by default.
Enable RollOver?	Select this check box to allow the VPN tunnel to roll over to the other WAN interface when the WAN mode is set to Auto-Rollover and an actual rollover occurs. This feature is disabled by default. For the multiple WAN port models only: Select a WAN interface from the drop-down list.

Table 66. Add New VPN Policy screen settings (continued)

Setting	Description	
Enable Keepalive **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 297.	Select a radio button to specify if keep-alive is enabled: • **Yes**. This feature is enabled: Periodically, the UTM sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You need to specify the ping IP address in the Ping IP Address field, the detection period in the Detection Period field, and the maximum number of keep-alive requests that the UTM sends in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Ping IP Address	The IP address that the UTM pings. The address needs to be of a host that can respond to ICMP ping requests.
	Detection Period	The period in seconds between the keep-alive requests. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of keep-alive requests before the UTM tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is 3 keep-alive requests.
Traffic Selection		
Local IP	From the drop-down list, select the address or addresses that are part of the VPN tunnel on the UTM: • **Any**. All PCs and devices on the network. • **Single**. A single IP address on the network. Enter the IP address in the Start IP Address field. • **Range**. A range of IP addresses on the network. Enter the starting IP address in the Start IP Address field and the ending IP address in the End IP Address field. • **Subnet**. A subnet on the network. Enter the starting IP address in the Start IP Address field and the subnet mask in the Subnet Mask field. **Note:** You cannot select Any for both the UTM and the remote endpoint.	
Remote IP	From the drop-down list, select the address or addresses that are part of the VPN tunnel on the remote endpoint. The selections are the same as for the Local IP drop-down list.	
Manual Policy Parameters **Note:** These fields apply only when you select Manual Policy as the policy type. When you specify the settings for the fields in this section, a security association (SA) is created.		
SPI-Incoming	The Security Parameters Index (SPI) for the inbound policy. Enter a hexadecimal value between 3 and 8 characters (for example, 0x1234).	

Table 66. Add New VPN Policy screen settings (continued)

Setting	Description
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.
Key-In	The encryption key for the inbound policy. The length of the key depends on the selected encryption algorithm: • **DES**. Enter 8 characters. • **3DES**. Enter 24 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.
Key-Out	The encryption key for the outbound policy. The length of the key depends on the selected encryption algorithm: • **DES**. Enter 8 characters. • **3DES**. Enter 24 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.
SPI-Outgoing	The Security Parameters Index (SPI) for the outbound policy. Enter a hexadecimal value between 3 and 8 characters (for example, 0x1234).
Integrity Algorithm	From the drop-down list, select one of the following algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest. • **SHA-256** (UTM9S only). Hash algorithm that produces a 256-bit key size. • **SHA-512** (UTM9S only). Hash algorithm that produces a 512-bit key size.
Key-In	The integrity key for the inbound policy. The length of the key depends on the selected integrity algorithm: • **MD5**. Enter 16 characters. • **SHA-1**. Enter 20 characters. • **SHA-256** (UTM9S only). Enter 32 characters. • **SHA-512** (UTM9S only). Enter 64 characters.
Key-Out	The integrity key for the outbound policy. The length of the key depends on the selected integrity algorithm: • **MD5**. Enter 16 characters. • **SHA-1**. Enter 20 characters. • **SHA-256** (UTM9S only). Enter 32 characters. • **SHA-512** (UTM9S only). Enter 64 characters.

Table 66. Add New VPN Policy screen settings (continued)

Setting	Description
Auto Policy Parameters	
Note: These fields apply only when you select Auto Policy as the policy type.	
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. From the drop-down list, select how the SA lifetime is specified: • **Seconds**. In the SA Lifetime field, enter a period in seconds. The minimum value is 300 seconds. The default value is 3600 seconds. • **KBytes**. In the SA Lifetime field, enter a number of kilobytes. The minimum value is 1920000 KB.
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.
Integrity Algorithm	From the drop-down list, select one of the following algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest. • **AES-256** (UTM9S only). Hash algorithm that produces a 256-bit digest. • **AES-512** (UTM9S only). Hash algorithm that produces a 512-bit digest.
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and then select a Diffie-Hellman (DH) group from the drop-down list. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**. • **Group 14 (2048 bit)** (UTM9S only). • **Group 15 (3072 bit)** (UTM9S only). • **Group 16 (4096 bit)** (UTM9S only).
Select IKE Policy	Select an existing IKE policy that defines the characteristics of the Phase-1 negotiation. To display the selected IKE policy, click the **View Selected** button.

4. Click **Apply** to save your settings. The VPN policy is added to the List of VPN Policies table.

➢ **To edit a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 166* on page 270).

2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. This screen shows the same fields as the Add VPN Policy screen (see *Figure 167* on page 272).

3. Modify the settings that you wish to change (see the previous table).

4. Click **Apply** to save your changes. The modified VPN policy is displayed in the List of VPN Policies table.

Configure Extended Authentication (XAUTH)

When many VPN clients connect to a UTM, you might want to use a unique user authentication method beyond relying on a single common pre-shared key for all clients. Although you could configure a unique VPN policy for each user, it is more efficient to authenticate users from a stored list of user accounts. XAUTH provides the mechanism for requesting individual authentication information from the user. A local user database or an external authentication server, such as a RADIUS server, provides a method for storing the authentication information centrally in the local network.

You can enable XAUTH when you manually add or edit an IKE policy. Two types of XAUTH are available:

- **Edge Device**. The UTM is used as a VPN concentrator on which one or more gateway tunnels terminate. You need to specify the authentication type that should be used during verification of the credentials of the remote VPN gateways: the user database, RADIUS-PAP, or RADIUS-CHAP.

- **IPSec Host**. Authentication by the remote gateway through a user name and password that are associated with the IKE policy. The user name and password that are used to authenticate the UTM need to be specified on the remote gateway.

> **Note:** If a RADIUS-PAP server is enabled for authentication, XAUTH first checks the local user database for the user credentials. If the user account is not present, the UTM then connects to a RADIUS server.

Configure XAUTH for VPN Clients

Once the XAUTH has been enabled, you need to establish user accounts in the user database to be authenticated against XAUTH, or you need to enable a RADIUS-CHAP or RADIUS-PAP server.

> **Note:** You cannot modify an existing IKE policy to add XAUTH while the IKE policy is in use by a VPN policy. The VPN policy needs to be disabled before you can modify the IKE policy.

➢ **To enable and configure XAUTH:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 164* on page 263).

2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy for which you want to enable and configure XAUTH. The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen (see *Figure 165* on page 265).

3. In the Extended Authentication section on the screen, complete the fields, select the radio buttons, and make your selections from the drop-down lists as explained in the following table:

Table 67. Extended authentication settings

Setting	Description
Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The UTM functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The UTM functions as a VPN client of the remote gateway. In this configuration the UTM is authenticated by a remote gateway with a user name and password combination.	
Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the UTM's user database. You can add users on the Add User screen (see *User Database Configuration* on page 278). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the UTM connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 279. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 279.
Username	The user name for XAUTH.
Password	The password for XAUTH.

4. Click **Apply** to save your settings.

User Database Configuration

When XAUTH is enabled in an Edge Device configuration, users need to be authenticated either by a local user database account or by an external RADIUS server. Whether or not you use a RADIUS server, you might want some users to be authenticated locally. These users need to be added to the List of Users table on the Users screen, as described in *Configure User Accounts* on page 362.

RADIUS Client Configuration

Remote Authentication Dial In User Service (RADIUS, RFC 2865) is a protocol for managing authentication, authorization, and accounting (AAA) of multiple users in a network. A RADIUS server stores a database of user information and can validate a user at the request of a gateway or server in the network when a user requests access to network resources. During the establishment of a VPN connection, the VPN gateway can interrupt the process with an XAUTH request. At that point, the remote user needs to provide authentication information such as a user name and password or some encrypted response using his or her user name and password information. The gateway then attempts to verify this information first against a local user database (if RADIUS-PAP is enabled) and then by relaying the information to a central authentication server such as a RADIUS server.

> **To configure primary and backup RADIUS servers:**

1. Select **VPN > IPSec VPN > RADIUS Client**. The RADIUS Client screen displays:

Figure 168.

2. Complete the fields and select the radio buttons as explained in the following table:

Table 68. RADIUS Client screen settings

Setting	Description
Primary RADIUS Server	
To enable and configure the primary RADIUS server, select the **Yes** radio button, and then enter the settings for the three fields to the right. The default setting is that the No radio button is selected.	
Primary Server IP Address	The IP address of the primary RADIUS server.

Table 68. RADIUS Client screen settings (continued)

Setting	Description
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the primary RADIUS server. The same secret phrase needs to be configured on both the client and the server.
Primary Server NAS Identifier	The primary Network Access Server (NAS) identifier that needs to be present in a RADIUS request. **Note:** The UTM functions as an NAS, allowing network access to external users after verification of their authentication information. In a RADIUS transaction, the NAS needs to provide some NAS identifier information to the RADIUS server. Depending on the configuration of the RADIUS server, the UTM's IP address might be sufficient as an identifier, or the server might require a name, which you need to enter in this field.
Backup RADIUS Server	
To enable and configure the backup RADIUS server, select the **Yes** radio button, and then enter the settings for the three fields to the right. The default setting is that the No radio button is selected.	
Backup Server IP Address	The IP address of the backup RADIUS server.
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the backup RADIUS server. The same secret phrase needs to be configured on both the client and the server.
Backup Server NAS Identifier	The backup Network Access Server (NAS) identifier that needs to be present in a RADIUS request. **Note:** See the note earlier in this table for the Primary Server NAS Identifier.
Connection Configuration	
Time out period	The period in seconds that the UTM waits for a response from a RADIUS server.
Maximum Retry Counts	The maximum number of times that the UTM attempts to connect to a RADIUS server.

3. Click **Apply** to save your settings.

> **Note:** You can select the RADIUS authentication protocol (PAP or CHAP) on the Edit IKE Policy screen or Add IKE Policy screen (see *Configure XAUTH for VPN Clients* on page 277).

Assign IP Addresses to Remote Users (Mode Config)

To simplify the process of connecting remote VPN clients to the UTM, use the Mode Config feature to automatically assign IP addresses to remote users, including a network access IP address, subnet mask, WINS server, and DNS address. Remote users are given IP addresses available in a secured network space so that remote users appear as seamless extensions of the network.

Mode Config Operation

After the IKE Phase 1 negotiation is complete, the VPN connection initiator (which is the remote user with a VPN client) requests the IP configuration settings such as the IP address, subnet mask, WINS server, and DNS address from the UTM. The Mode Config feature allocates an IP address from the configured IP address pool and activates a temporary IPSec policy, using the information that is specified in the Traffic Tunnel Security Level section of the Mode Config record (on the Add Mode Config Record screen that is shown in *Figure 170* on page 283).

> **Note:** After configuring a Mode Config record, you need to manually configure an IKE policy and select the newly created Mode Config record from the Select Mode Config Record drop-down list (see *Configure Mode Config Operation on the UTM* on page 281). You do not need to make changes to any VPN policy.

> **Note:** An IP address that is allocated to a VPN client is released only after the VPN client has gracefully disconnected or after the SA lifetime for the connection has timed out.

Configure Mode Config Operation on the UTM

To configure Mode Config on the UTM, first create a Mode Config record, and then select the Mode Config record for an IKE policy.

➢ **To configure Mode Config on the UTM:**

1. Select **VPN > IPSec VPN > Mode Config**. The Mode Config screen displays:
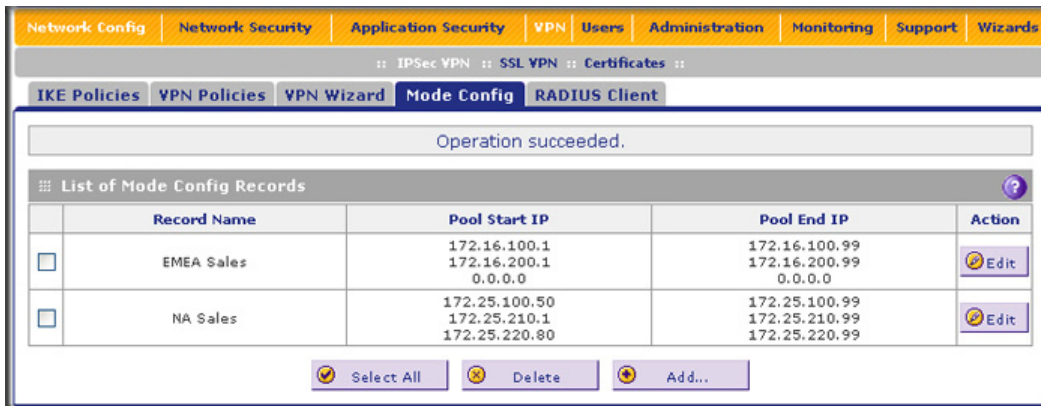
Figure 169.

As an example, the screen shows two Mode Config records with the names EMEA Sales and NA Sales:

- For EMEA Sales, a first pool (172.16.100.1 through 172.16.100.99) and second pool (172.16.200.1 through 172.16.200.99) are shown.

- For NA Sales, a first pool (172.25.100.50 through 172.25.100.99), a second pool (172.25.210.1 through 172.25.210.99), and a third pool (172.25.220.80 through 172.25.220.99) are shown.

2. Under the List of Mode Config Records table, click the **Add** table button. The Add Mode Config Record screen displays:
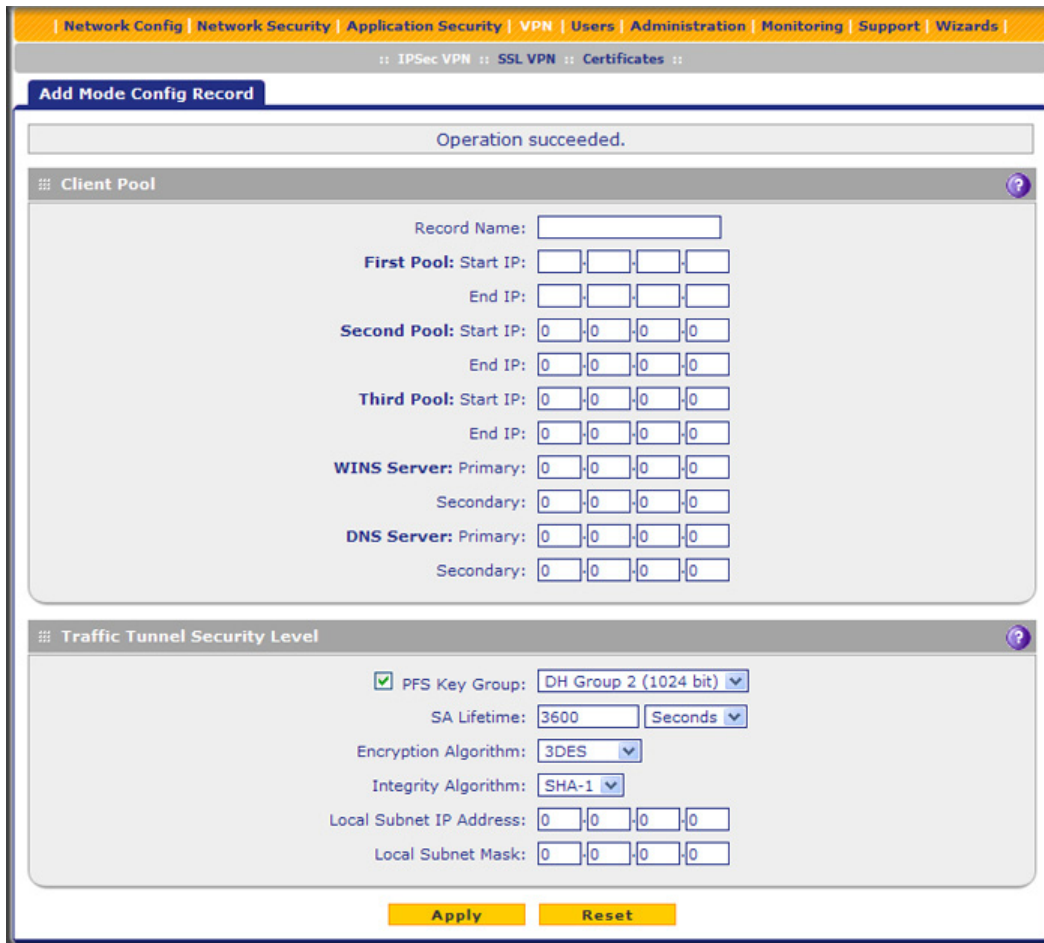
Figure 170.

3. Complete the fields, select the check box, and make your selections from the drop-down lists as explained in the following table:

Table 69. Add Mode Config Record screen settings

Setting	Description
Client Pool	
Record Name	A descriptive name of the Mode Config record for identification and management purposes.
First Pool	Assign at least one range of IP pool addresses in the First Pool fields to enable the UTM to allocate these to remote VPN clients. The Second Pool and Third Pool fields are optional. To specify any client pool, enter the starting IP address for the pool in the Starting IP field, and enter the ending IP address for the pool in the Ending IP field.
Second Pool	
Third Pool	
	Note: No IP pool should be within the range of the local network IP addresses. Use a different range of private IP addresses such as 172.173.xxx.xx.

Table 69. Add Mode Config Record screen settings (continued)

Setting	Description
WINS Server	If there is a WINS server on the local network, enter its IP address in the Primary field. You can enter the IP address of a second WINS server in the Secondary field.
DNS Server	Enter the IP address of the DNS server that is used by remote VPN clients in the Primary field. You can enter the IP address of a second DNS server in the Secondary field.
Traffic Tunnel Security Level	
Note: Generally, the default settings work well for a Mode Config configuration.	
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and then select a Diffie-Hellman (DH) group from the drop-down list. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)** • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. From the drop-down list, select how the SA lifetime is specified: • **Seconds**. In the SA Lifetime field, enter a period in seconds. The minimum value is 300 seconds. The default value is 3600 seconds. • **KBytes**. In the SA Lifetime field, enter a number of kilobytes. The minimum value is 1920000 KB.
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.
Local IP Address	The local IP address to which remote VPN clients have access. If you do not specify a local IP address, the UTM's default LAN IP address is used (by default, 192.168.1.1).
Local Subnet Mask	The local subnet mask. Typically, this is 255.255.255.0.

4. Click **Apply** to save your settings. The new Mode Config record is added to the List of Mode Config Records table.

   Continue the Mode Config configuration procedure by configuring an IKE policy.

5. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 164* on page 263).

6. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays. (The following figure shows the upper part only of a multiple WAN port model screen.) The WAN drop-down list (next to Select Local Gateway) is shown on the Add IKE Policy screen for the multiple WAN port models but not on the Add IKE Policy screen for the single WAN port models.

Figure 171.

7. On the Add IKE Policy screen, complete the fields, select the radio buttons, and make your selections from the drop-down lists as explained in the following table.

> **Note:** The IKE policy settings that are explained in the following table are specifically for a Mode Config configuration. *Table 64* on page 266 explains the general IKE policy settings.

Table 70. IKE policy settings for a Mode Config configuration

Setting	Description	
Mode Config Record		
Do you want to use Mode Config Record?	Select the **Yes** radio button. **Note:** Because Mode Config functions only in Aggressive mode, selecting the Yes radio button sets the tunnel exchange mode to Aggressive mode. Mode Config also requires that both the local and remote endpoints are defined by their FQDNs.	
	Select Mode Config Record	From the drop-down list, select the Mode Config record that you created in *step 4* on page 284. This example uses NA Sales.
General		
Policy Name	A descriptive name of the IKE policy for identification and management purposes. This example uses ModeConfigNA_Sales. **Note:** The name is not supplied to the remote VPN endpoint.	
Direction / Type	Responder is automatically selected when you select the Mode Config record in the Mode Config Record section of the screen. This ensures that the UTM responds to an IKE request from the remote endpoint but does not initiate one.	
Exchange Mode	Aggressive mode is automatically selected when you select the Mode Config record in the Mode Config Record section of the screen.	
Local		
Select Local Gateway (multiple WAN port models only)	Select a WAN interface from the drop-down list to specify the WAN interface for the local gateway.	
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the UTM (that is, the local endpoint) is defined by an FQDN.	
	Identifier	Enter an FQDN for the UTM. This example uses router.com.

Table 70. IKE policy settings for a Mode Config configuration (continued)

Setting	Description	
Remote		
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the remote endpoint is defined by an FQDN.	
	Identifier	Enter the FQDN for the remote endpoint. This needs to be an FQDN that is not used in any other IKE policy. This example uses client.com.
IKE SA Parameters		
Note: Generally, the default settings work well for a Mode Config configuration.		
Encryption Algorithm	To negotiate the security association (SA), from the drop-down list, select the **3DES** algorithm.	
Authentication Algorithm	From the drop-down list, select the **SHA-1** algorithm to be used in the VPN header for the authentication process.	
Authentication Method	Select **Pre-shared key** as the authentication method, and enter a key in the Pre-shared key field.	
	Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote (") in the key. This example uses H8!spsf3#JYK2!.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. From the drop-down list, select **Group 2 (1024 bit)**.	
SA-Lifetime (sec)	The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying occurs. The default setting is 28800 seconds (8 hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (1 hour).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 297.	Select a radio button to specify whether or not Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the UTM detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the UTM attempts to reconnect in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds. This example uses 30 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the UTM tears down the connection and then attempts to reconnect to the peer. The default setting is 3 failures.

Table 70. IKE policy settings for a Mode Config configuration (continued)

Setting	Description	
Extended Authentication		
XAUTH Configuration **Note:** For more information about XAUTH and its authentication modes, see *Configure XAUTH for VPN Clients* on page 277.	Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The UTM functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The UTM functions as a VPN client of the remote gateway. In this configuration the UTM is authenticated by a remote gateway with a user name and password combination.	
	Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the UTM's user database. You can add users on the Add User screen (see *User Database Configuration* on page 278). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the UTM connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 279. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 279.
	Username	The user name for XAUTH.
	Password	The password for XAUTH.

8. Click **Apply** to save your settings. The IKE policy is added to the List of IKE Policies table.

Configure the ProSafe VPN Client for Mode Config Operation

When the Mode Config feature is enabled, the following information is negotiated between the VPN client and the UTM during the authentication phase:

- Virtual IP address of the VPN client
- DNS server address (optional)
- WINS server address (optional)

The virtual IP address that is issued by the UTM is displayed in the VPN Client Address field on the VPN client's IPSec pane.

Note: Perform these tasks from a PC that has the NETGEAR ProSafe
VPN Client installed.

To configure the VPN client for Mode Config operation, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and then specify the global parameters.

Configure the Mode Config Authentication Settings (Phase 1 Settings)

➢ **To create new authentication settings:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.
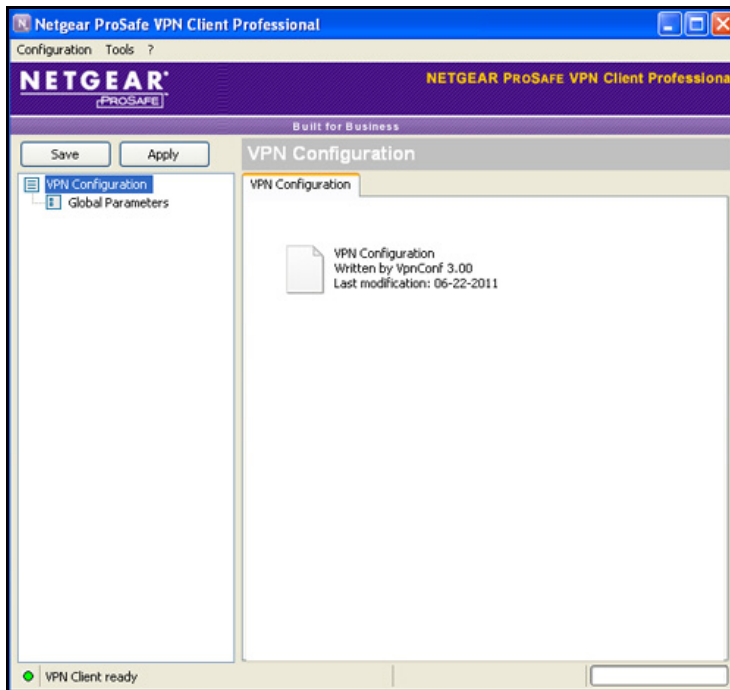
Figure 172.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.
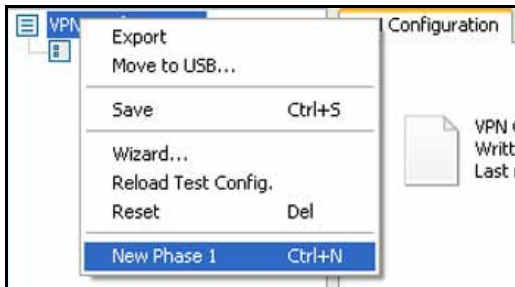
Figure 173.

3. Change the name of the authentication phase (the default is Gateway):

   a. Right-click the authentication phase name.

   b. Select **Rename**.

   c. Type **GW_ModeConfig**.

   d. Click anywhere in the tree list pane.

   Note: *This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.
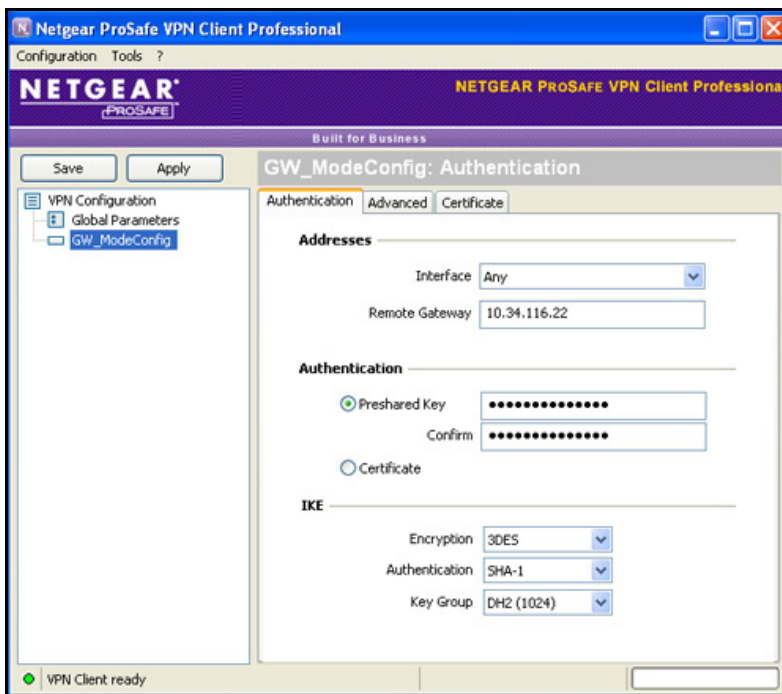
Figure 174.

4. Specify the settings that are explained in the following table.

Table 71. VPN client authentication settings (Mode Config)

Setting	Description	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the UTM. For example, enter **10.34.116.22**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the UTM. For example, enter **H8!spsf3#JYK2!**. Confirm the key in the Confirm field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On the UTM, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

6. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.

Figure 175.

7. Specify the settings that are explained in the following table.

Table 72. VPN client advanced authentication settings (Mode Config)

Setting	Description
Advanced features	
Mode Config	Select this check box to enable Mode Config.
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the UTM.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and UTM to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the UTM configuration. As the value of the ID, enter **client.com** as the local ID for the VPN client. **Note:** The remote ID on the UTM is the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the UTM configuration. As the value of the ID, enter **router.com** as the remote ID for the UTM. **Note:** The local ID on the UTM is the remote ID on the VPN client.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the Mode Config IPSec Configuration (Phase 2 Settings)

> **Note:** On the UTM, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **GW_ModeConfig** authentication phase name, and then select **New Phase 2**.

2. Change the name of the IPSec configuration (the default is Tunnel):

  a. Right-click the IPSec configuration name.

  b. Select **Rename**.

  c. Type **Tunnel_ModeConfig**.

  d. Click anywhere in the tree list pane.

> *Note:* *This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.
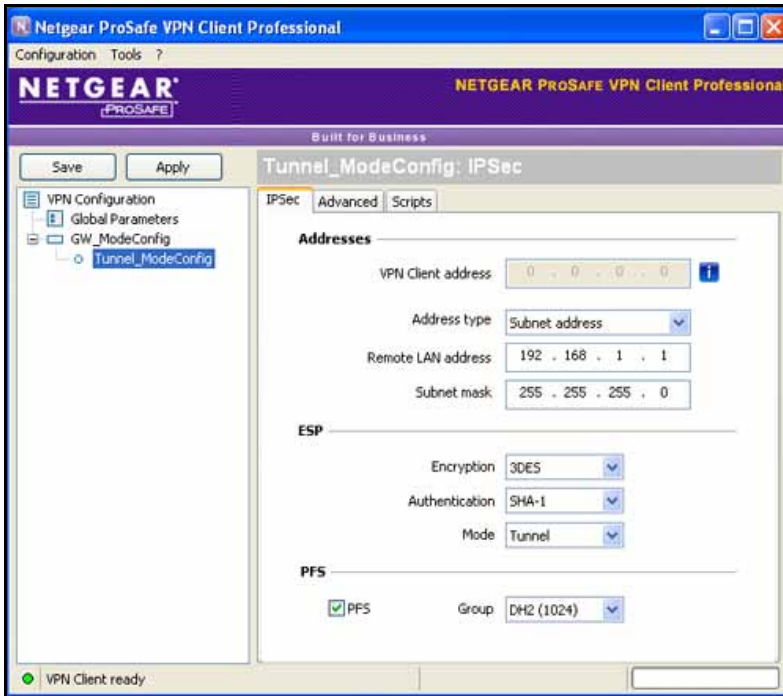
Figure 176.

3. Specify the settings that are explained in the following table.

Table 73. VPN client IPSec configuration settings (Mode Config)

Setting	Description
VPN Client address	This field is masked out because Mode Config is selected. After an IPSec connection is established, the IP address that is issued by the UTM displays in this field (see *Figure 181* on page 297).
Address Type	Select **Subnet address** from the drop-down list.
Remote host address	The address that you need to enter depends on whether or not you have specified a LAN IP network address in the Local IP Address field on the Add Mode Config Record screen of the UTM: • If you left the Local IP Address field blank, enter the UTM's default LAN IP address as the remote host address that opens the VPN tunnel. For example, enter **192.168.1.1**. • If you specified a LAN IP network address in the Local IP Address field, enter the address that you specified as the remote host address that opens the VPN tunnel.

Table 73. VPN client IPSec configuration settings (Mode Config) (continued)

Setting	Description	
Subnet mask	Enter **255.255.255.0** as the remote subnet mask of the UTM that opens the VPN tunnel. This is the LAN IP subnet mask that you specified in the Local Subnet Mask field on the Add Mode Config Record screen of the UTM. If you left the Local Subnet Mask field blank, enter the UTM's default IP subnet mask.	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down list. **Note:** On the UTM, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure the Mode Config Global Parameters

➢ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.
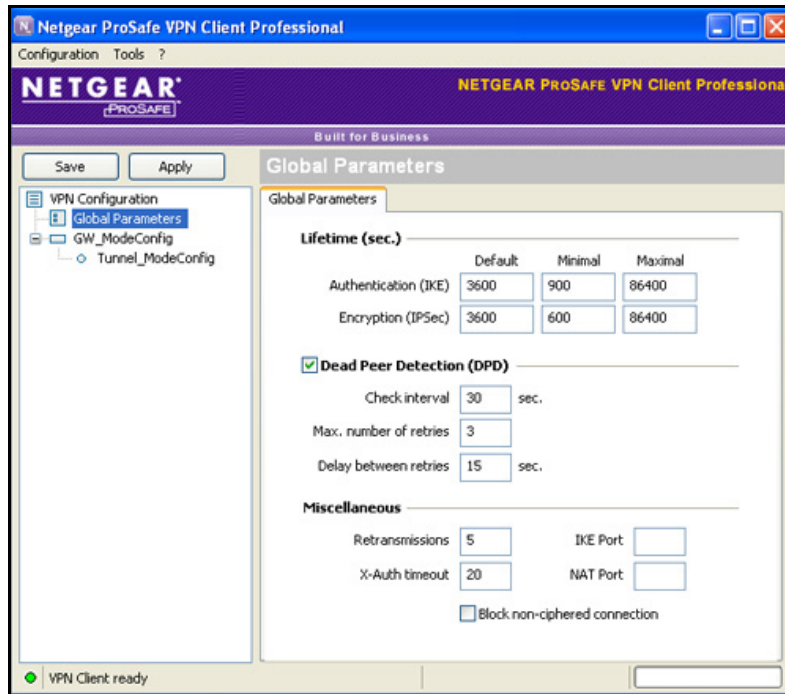
Figure 177.

2. Specify the following default lifetimes in seconds to match the configuration on the UTM:

   • **Authentication (IKE)**, **Default**. Enter **3600** seconds.

   • **Encryption (IPSec)**, **Default**. Enter **3600** seconds.

3. Select the **Dead Peer Detection (DPD)** check box, and configure the following DPD settings to match the configuration on the UTM:

   • **Check Interval**. Enter **30** seconds.

   • **Max. number of entries**. Enter **3** retries.

   • **Delay between entries**. Leave the default delay setting of 15 seconds.

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The Mode Config configuration of the VPN client is now complete.

Test the Mode Config Connection

➢ **To test the Mode Config connection from the VPN client to the UTM:**

1. Right-click the system tray icon, and select **Open tunnel 'Tunnel_ModeConfig'**.
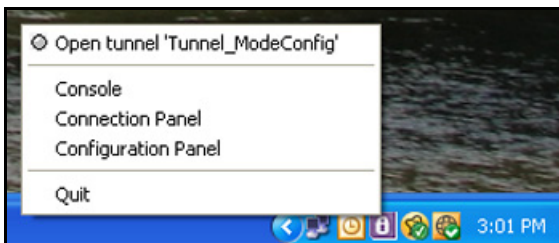
Figure 178.

When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray, and the VPN client displays a green icon in the system tray.
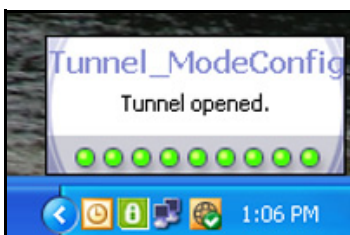
Figure 179.

2. Verify that the UTM issued an IP address to the VPN client. This IP address displays in the VPN Client address field on the IPSec pane of the VPN client. (The following figure shows the upper part of the IPSec pane only.)
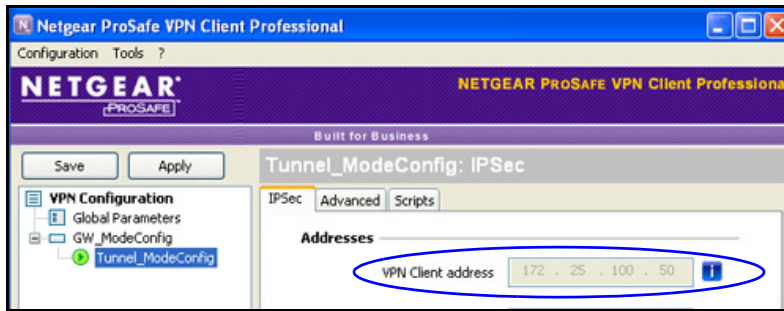
Figure 180.

3. From the client PC, ping a computer on the UTM LAN.

Modify or Delete a Mode Config Record

> **Note:** Before you modify or delete a Mode Config record, make sure it is not used in an IKE policy.

> ➢ **To edit a Mode Config record:**

1. On the Mode Config screen (see *Figure 169* on page 282), click the **Edit** button in the Action column for the record that you want to modify. The Edit Mode Config Record screen displays. This screen is identical to the Add Mode Config Record screen (see *Figure 170* on page 283).

2. Modify the settings as explained in *Table 69* on page 283.

3. Click **Apply** to save your settings.

> ➢ **To delete one or more Mode Config records:**

1. On the Mode Config screen (see *Figure 169* on page 282), Select the check box to the left of each record that you want to delete, or click the **Select All** table button to select all records.

2. Click the **Delete** table button.

Configure Keep-Alives and Dead Peer Detection

In some cases, you might not want a VPN tunnel to be disconnected when traffic is idle, for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require a VPN tunnel to remain connected, you can use the keep-alive and Dead Peer Detection (DPD) features to prevent the tunnel from being disconnected and to force a reconnection if the tunnel disconnects for any reason.

For DPD to function, the peer VPN device on the other end of the tunnel also needs to support DPD. Keep-alive, though less reliable than DPD, does not require any support from the peer device.

Configure Keep-Alives

The keep-alive feature maintains the IPSec SA by sending periodic ping requests to a host across the tunnel and monitoring the replies.

➢ **To configure the keep-alive feature on a configured VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 166* on page 270).

2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. (The following figure shows only the top part of a UTM50 screen with the General section).

Figure 181.

3. Enter the settings as explained in the following table:

Table 74. Keep-alive settings

Setting	Description		
General			
Enable Keepalive	Select the **Yes** radio button to enable the keep-alive feature. Periodically, the UTM sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You need to specify the ping IP address in the Ping IP Address field, the detection period in the Detection Period field, and the maximum number of keep-alive requests that the UTM sends in the Reconnect after failure count field.		
	Ping IP Address	The IP address that the UTM pings. The address should be of a host that can respond to ICMP ping requests.	
	Detection Period	The period in seconds between the keep-alive requests. The default setting is 10 seconds.	
	Reconnect after failure count	The maximum number of keep-alive requests before the UTM tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is 3 keep-alive requests.	

4. Click **Apply** to save your settings.

Configure Dead Peer Detection

The Dead Peer Detection (DPD) feature lets the UTM maintain the IKE SA by exchanging periodic messages with the remote VPN peer.

➤ **To configure DPD on a configured IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 164* on page 263).

2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy that you want to edit. The Edit IKE Policy screen displays. (The following figure shows only the IKE SA Parameters section of the screen).
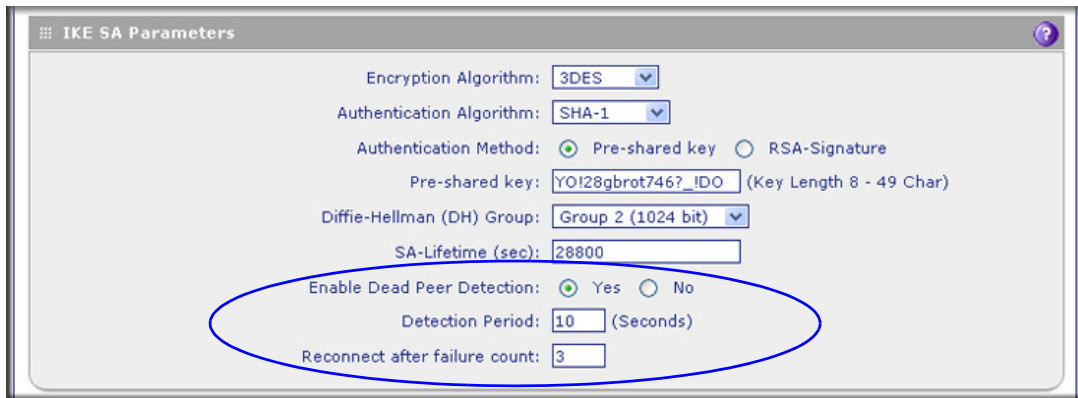
Figure 182.

3. In the IKE SA Parameters section of the screen, locate the DPD fields, and complete the fields as explained the following table:

Table 75. Dead peer Detection settings

Setting	Description	
IKE SA Parameters		
Enable Dead Peer Detection	Select the **Yes** radio button to enable DPD. When the UTM detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the UTM attempts to reconnect in the Reconnect after failure count field.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the UTM tears down the connection and then attempts to reconnect to the peer. The default setting is 3 failures.

4. Click **Apply** to save your settings.

Configure NetBIOS Bridging with IPSec VPN

Windows networks use the Network Basic Input/Output System (NetBIOS) for several basic network services such as naming and neighborhood device discovery. Because VPN routers do not usually pass NetBIOS traffic, these network services do not function for hosts on opposite ends of a VPN connection. To solve this problem, you can configure the UTM to bridge NetBIOS traffic over the VPN tunnel.

➢ **To enable NetBIOS bridging on a configured VPN tunnel:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 166* on page 270).

---

2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. (The following figure shows only the top part of a UTM50 screen with the General section).

Figure 183.

3. Select the **Enable NetBIOS** check box.

4. Click **Apply** to save your settings.

Configure the PPTP Server (UTM9S Only)

As an alternate solution to IPSec VPN and L2TP tunnels, you can configure a Point-to-Point Tunnel Protocol (PPTP) server on the UTM9S to allow users to access PPTP clients over PPTP tunnels.

A PPTP user typically initiates a tunnel request; the PPTP server accommodates the tunnel request and assigns an IP address to the user. After a PPTP tunnel is established, the user can connect to a PPTP client that is located behind the UTM9S.

You need to enable the PPTP server on the UTM9S, specify a PPTP server address pool, and create PPTP user accounts. For information about how to create PPTP user accounts, see *Configure User Accounts* on page 362.

➢ **To enable the PPTP server and configure the PPTP server pool, authentication, and encryption:**

1. Select **VPN > PPTP Server**. The PPTP Server screen displays:
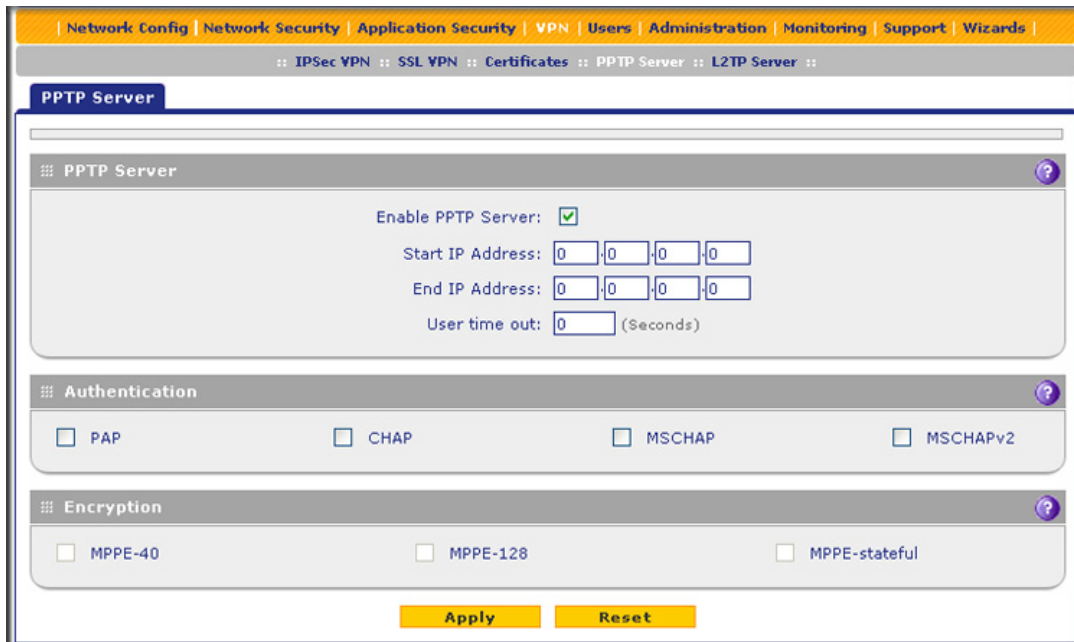
Figure 184.

2. Enter the settings as explained in the following table:

Table 76. PPTP Server screen settings

Setting	Description	
PPTP Server		
Enable PPTP Server	To enable the PPTP server, select the **Enable** check box. Complete the following fields:	
	Start IP Address	Type the first IP address of the address pool.
	End IP Address	Type the last IP address of the address pool.
	User time out	Enter the time-out period in seconds. If there is no traffic from a user, the connection is disconnected after the specified period.
Authentication		
Select one or more of the following authentication methods to authenticate PPTP users: • **PAP**. RADIUS-Password Authentication Protocol (PAP). • **CHAP**. RADIUS-Challenge Handshake Authentication Protocol (CHAP). • **MSCHAP**. RADIUS-Microsoft CHAP (MSCHAP). • **MSCHAPv2**. RADIUS-Microsoft CHAP version 2 (MSCHAPv2). **Note:** For *each* authentication method that you want to use for PPTP users, you need to have created a domain that supports the authentication method (see *Configure Domains* on page 353) and have added the PPTP users to the domain (see *Configure User Accounts* on page 362).		

Table 76. PPTP Server screen settings (continued)

Setting	Description
Encryption	
If the authentication is MSCHAP or MSCHAPv2, the PPTP server can support Microsoft Point-to-Point Encryption (MPPE). Select one or more of the following types of MPPE: • **MPPE-40**. MPPE 40-bit encryption. • **MPPE-128**. MPPE 128-bit encryption. This is the most secure type of MPPE encryption. • **MPPE-stateful**. Stateful MPPE encryption. This is the least secure type of MPPE encryption.	

3. Click **Apply** to save your settings.

View the Active PPTP Users

➢ **To view the active PPTP tunnel users:**

Select **Monitoring > Active Users & VPNs > PPTP Active Users**. The PPTP Active Users screen displays:
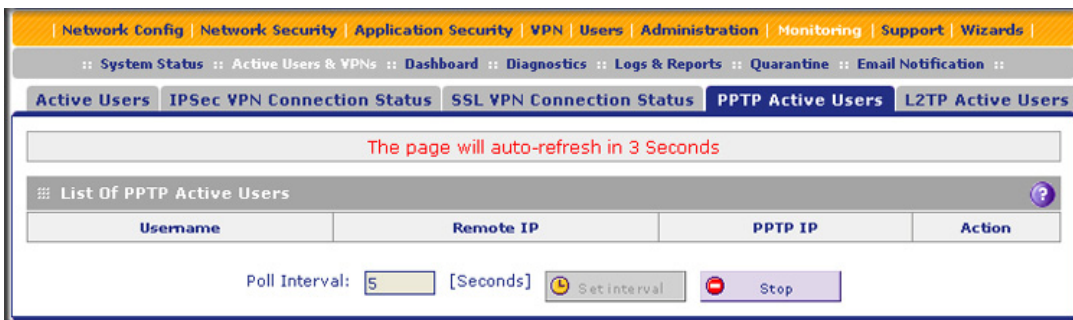
Figure 185.

The List of PPTP Active Users table lists each active connection with the information that is described in the following table.

Table 77. PPTP Active Users screen information

Item	Description
Username	The name of the PPTP user that you have defined (see *Configure User Accounts* on page 362).
Remote IP	The remote client's IP address.
L2TP IP	The IP address that is assigned by the PPTP server on the UTM9S.
Action	This column is not applicable to PPTP.

The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and then click the **Set Interval** button. To stop polling, click the **Stop** button.

Configure the L2TP Server (UTM9S Only)

As an alternate solution to IPSec VPN and PPTP tunnels, you can configure a Layer 2 Tunneling Protocol (L2TP) server on the UTM9S to allow users to access L2TP clients over L2TP tunnels.

An L2TP Access Concentrator (LAC) typically initiates a tunnel to fullfil a connection request from an L2TP user; the L2TP server accommodates the tunnel request and assigns an IP address to the user. After an L2TP tunnel is established, the user can connect to an L2TP client that is located behind the UTM9S.

> **Note:** IPSec VPN and PPTP provide stronger authentication and encryption than L2TP. (Packets that traverse the L2TP tunnel are not encapsulated by IPSec or MPPE.)

You need to enable the L2TP server on the UTM9S, specify an L2TP server address pool, and create L2TP user accounts. For information about how to create L2TP user accounts, see *Configure User Accounts* on page 362.

> **To enable the L2TP server and configure the L2TP server pool and authentication:**

1. Select **VPN > L2TP Server**. The L2TP Server screen displays:

Figure 186.

2. Enter the settings as explained in the following table:

Table 78. L2TP Server screen settings

Setting	Description	
L2TP Server		
Enable L2TP Server	To enable the L2TP server, select the **Enable** check box. Complete the following fields:	
	Start IP Address	Type the first IP address of the address pool.
	End IP Address	Type the last IP address of the address pool.
	User time out	Enter the time-out period in seconds. If there is no traffic from a user, the connection is disconnected after the specified period.
Authentication		
Select one or more of the following authentication methods to authenticate L2TP users: • **PAP**. RADIUS-Password Authentication Protocol (PAP). • **CHAP**. RADIUS-Challenge Handshake Authentication Protocol (CHAP). • **MSCHAP**. RADIUS-Microsoft CHAP (MSCHAP). • **MSCHAPv2**. RADIUS-Microsoft CHAP version 2 (MSCHAPv2). **Note:** For *each* authentication method that you want to use for L2TP users, you need to have created a domain that supports the authentication method (see *Configure Domains* on page 353) and have added the L2TP users to the domain (see *Configure User Accounts* on page 362).		

3. Click **Apply** to save your settings.

View the Active L2TP Users

➤ **To view the active L2TP tunnel users:**

Select **Monitoring > Active Users & VPNs > L2TP Active Users**. The L2TP Active Users screen displays:
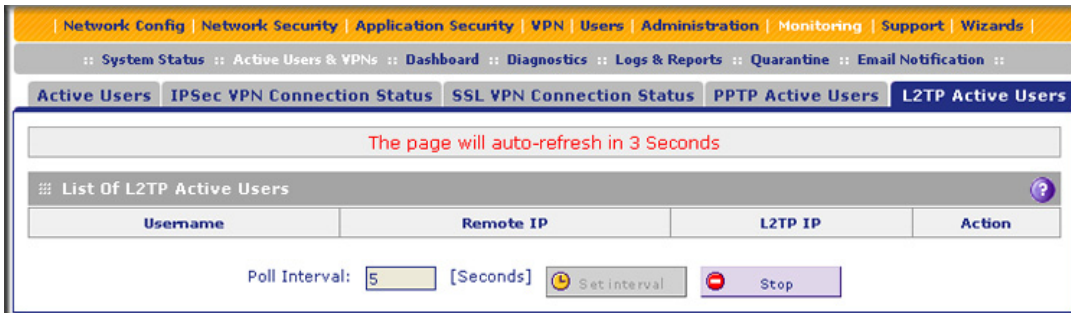
Figure 187.

The List of L2TP Active Users table lists each active connection with the information that is described in the following table.

Table 79. L2TP Active Users screen information

Item	Description
Username	The name of the L2TP user that you have defined (see *Configure User Accounts* on page 362).
Remote IP	The client's IP address on the remote LAC.
L2TP IP	The IP address that is assigned by the L2TP server on the UTM9S.
Action	This column is not applicable to L2TP.

The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and then click the **Set Interval** button. To stop polling, click the **Stop** button.

Virtual Private Networking Using SSL Connections

8

The UTM provides a hardware-based SSL VPN solution designed specifically to provide remote access for mobile users to their corporate resources, bypassing the need for a preinstalled VPN client on their computers. Using the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, the UTM can authenticate itself to an SSL-enabled client, such as a standard web browser. Once the authentication and negotiation of encryption information are completed, the server and client can establish an encrypted connection. With support for up to 13 dedicated SSL VPN tunnels, the UTM allows users to easily access the remote network for a customizable, secure, user portal experience from virtually any available platform.

This chapter contains the following sections:

- *SSL VPN Portal Options*
- *Use the SSL VPN Wizard for Client Configurations*
- *Manually Configure and Edit SSL Connections*

SSL VPN Portal Options

The UTM's SSL VPN portal can provide two levels of SSL service to the remote user:

- **SSL VPN tunnel**. The UTM can provide the full network connectivity of a VPN tunnel using the remote user's browser instead of a traditional IPSec VPN client. The SSL capability of the user's browser provides authentication and encryption, establishing a secure connection to the UTM. Upon successful connection, an ActiveX-based SSL VPN client is downloaded to the remote PC to allow the remote user to virtually join the corporate network.

  The SSL VPN client provides a point-to-point (PPP) connection between the client and the UTM, and a virtual network interface is created on the user's PC. The UTM assigns the PC an IP address and DNS server IP addresses, allowing the remote PC to access network resources in the same manner as if it were connected directly to the corporate network, subject to any policy restrictions that you configure.

- **SSL port forwarding**. Like an SSL VPN tunnel, port forwarding is a web-based client that is installed transparently and then creates a virtual, encrypted tunnel to the remote network. However, port forwarding differs from an SSL VPN tunnel in several ways:

  - Port forwarding supports only TCP connections, not UDP connections or connections using other IP protocols.

  - Port forwarding detects and reroutes individual data streams on the user's PC to the port-forwarding connection rather than opening up a full tunnel to the corporate network.

  - Port forwarding offers more fine-grained management than an SSL VPN tunnel. You define individual applications and resources that are available to remote users.

The SSL VPN portal can present the remote user with one or both of these SSL service levels, depending on how you set up the configuration.

Use the SSL VPN Wizard for Client Configurations

The SSL VPN Wizard facilitates the configuration of the SSL VPN client connections by taking you through six screens, the last of which allows you to save the SSL VPN policy. For information about how to edit policies or to manually configure policies, see *Manually Configure and Edit SSL Connections* on page 323.

➢ **To start the SSL VPN Wizard:**

1. Select **Wizards** from the main navigation menu. The Welcome to the Netgear Configuration Wizard screen displays:
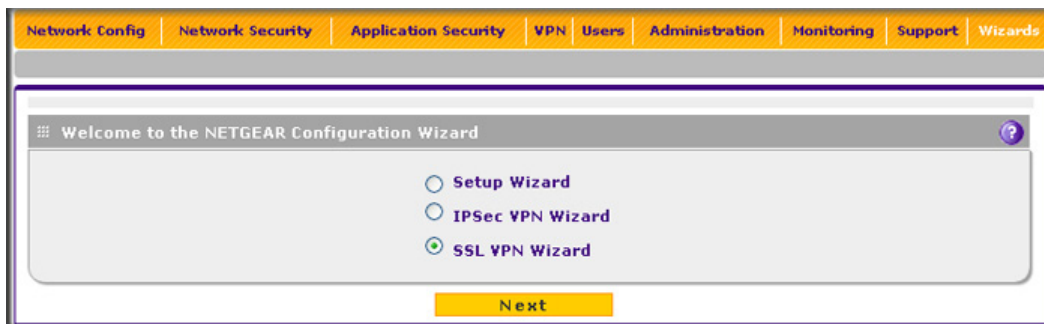
Figure 188.

2. Select the **SSL VPN Wizard** radio button.

3. Click **Next**. The first SSL VPN Wizard screen displays.

The following sections explain the five configuration screens of the SSL VPN Wizard. On the sixth screen, you can save your SSL VPN policy.

The tables in the following sections explain the buttons and fields of the SSL VPN Wizard screens. Additional information about the settings in the SSL VPN Wizard screens is provided in *Manually Configure and Edit SSL Connections* on page 323 or in other chapters. Each of the following sections provides a specific link to a section in *Manually Configure and Edit SSL Connections* on page 323 or to a section in another chapter.

SSL VPN Wizard Step 1 of 6 (Portal Settings)

Figure 189.

Note that the previous figure contains a layout example. Enter the settings as explained in the following table, and then click **Next** to go the following screen.

> **Note:** If you leave the Portal Layout Name field blank, the SSL VPN Wizard uses the default portal layout. You need to enter a name other than SSL VPN in the Portal Layout Name field to enable the SSL VPN Wizard to create a new portal layout. Do not enter an existing portal layout name in the Portal Layout Name field; otherwise, the SSL VPN Wizard will fail (although the UTM will not reboot in this situation).

Table 80. SSL VPN Wizard Step 1 of 6 screen settings (portal settings)

Setting	Description
Portal Layout and Theme Name	
Portal Layout Name	A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL. **Note:** Custom portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at https://vpn.company.com, and you create a portal layout named CustomerSupport, then users access the subsite at https://vpn.company.com/portal/CustomerSupport. **Note:** Only alphanumeric characters, hyphens (-), and underscores (_) are accepted in the Portal Layout Name field. If you enter other types of characters or spaces, the layout name is truncated before the first nonalphanumeric character. **Note:** Unlike most other URLs, this name is case-sensitive.
Portal Site Title	The title that displays at the top of the user's web browser window, for example, *Company Customer Support*.
Banner Title	The banner title of a banner message that users see before they log in to the portal, for example, *Welcome to Customer Support*.
Banner Message	The text of a banner message that users see before they log in to the portal, for example, *In case of login difficulty, call 123-456-7890*. Enter a plain text message, or include HTML and JavaScript tags. The maximum length of the login screen message is 4096 characters.
Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen as shown in *Figure 195* on page 320.
HTTP meta tags for cache control (recommended)	Select this check box to apply HTTP meta tag cache control directives to this portal layout. Cache control directives include: <meta http-equiv="pragma" content="no-cache"> <meta http-equiv="cache-control" content="no-cache"> <meta http-equiv="cache-control" content="must-revalidate"> **Note:** NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user's web browser cache.
ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to delete all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. The ActiveX web cache control is ignored by web browsers that do not support ActiveX.

Table 80. SSL VPN Wizard Step 1 of 6 screen settings (portal settings) (continued)

Setting	Description
SSL VPN Portal Pages to Display	
VPN Tunnel page	To provide full network connectivity, select this check box.
Port Forwarding	To provide access to specific defined network services, select this check box. **Note:** Any pages that are not selected are not visible from the SSL VPN portal; however, users can still access the hidden pages unless you create SSL VPN access policies to prevent access to these pages.

After you have completed the steps in the SSL VPN Wizard, you can make changes to the portal settings by selecting **VPN > SSL VPN > Portal Layout**. For more information about portal settings, see *Create the Portal Layout* on page 324.

SSL VPN Wizard Step 2 of 6 (Domain Settings)

Figure 190.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Note: If you leave the Domain Name field blank, the SSL VPN Wizard uses the default domain name geardomain. You need to enter a name other than geardomain in the Domain Name field to enable the SSL VPN Wizard to create a new domain. Do not enter an existing domain name in the Domain Name field; otherwise, the SSL VPN Wizard will fail and the UTM will reboot to recover its configuration.

Table 81. SSL VPN Wizard Step 2 of 6 screen settings (domain settings)

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type **Note:** If you select any type of RADIUS authentication, make sure that one or more RADIUS servers are configured (see *RADIUS Client Configuration* on page 279).	From the drop-down list, select the authentication method that the UTM applies: • **Local User Database (default)**. Users are authenticated locally on the UTM. This is the default setting. You do not need to complete any other fields on this screen. • **Radius-PAP**. RADIUS Password Authentication Protocol (PAP). Complete the following fields: 　- Authentication Server 　- Authentication Secret 　- Radius Port 　- Repeat 　- Timeout • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the following fields: 　- Authentication Server 　- Authentication Secret 　- Radius Port 　- Repeat 　- Timeout • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the following fields: 　- Authentication Server 　- Authentication Secret • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the following fields: 　- Authentication Server 　- Authentication Secret • **WIKID-PAP**. WiKID Systems PAP. Complete the following fields: 　- Authentication Server 　- Authentication Secret 　- Radius Port 　- Repeat 　- Timeout

Table 81. SSL VPN Wizard Step 2 of 6 screen settings (domain settings) (continued)

Setting	Description

Authentication Type (continued)	• **WIKID-CHAP**. WiKID Systems CHAP. Complete the following fields:
	   - Authentication Server
	   - Authentication Secret
	   - Radius Port
	   - Repeat
	   - Timeout
	• **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the following fields:
	   - Authentication Server
	   - Authentication Secret
	   - Radius Port
	   - Repeat
	   - Timeout
	• **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the following fields:
	   - Authentication Server
	   - Authentication Secret
	   - Radius Port
	   - Repeat
	   - Timeout
	• **NT Domain**. Microsoft Windows NT Domain. Complete the following fields:
	   - Authentication Server
	   - Workgroup
	• **Active Directory**. Microsoft Active Directory. Complete the following fields, and make a selection from the LDAP Encryption drop-down list:
	   - Authentication Server
	   - Active Directory Domain
	   - LDAP Port
	   - Bind DN
	   - Bind Password
	   - Search Base
	   - Additional Filter (optional)
	• **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the following fields, and make a selection from the LDAP Encryption drop-down list:
	   - Authentication Server
	   - LDAP Base DN
	   - LDAP Port
	   - Bind DN
	   - Bind Password
	   - Search Base
	   - UID Attribute
	   - Member Groups Attribute (optional)
	   - Group Members Attribute (optional)
	   - Additional Filter (optional)

Table 81. SSL VPN Wizard Step 2 of 6 screen settings (domain settings) (continued)

Setting	Description
Portal	The portal that you selected on the first SSL VPN Wizard screen. You cannot change the portal on this screen; the portal is displayed for information only.
Authentication Server	The server IP address or server name of the authentication server for any type of authentication other than authentication through the local user database.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WiKID, or MIAS authentication.
Workgroup	The workgroup that is required for Microsoft NT Domain authentication.
LDAP Base DN	The LDAP base distinguished name (DN) that is required for LDAP authentication.
Active Directory Domain	The active directory domain name that is required for Microsoft Active Directory authentication.
LDAP Port	The port number for the LDAP or Active Directory authentication server. The default port for the LDAP server is 389, which is generally the default port for TLS encryption or no encryption. When the encryption is SSL, the default port is generally 636.
Bind DN	The LDAP or Active Directory DN that is required to access the LDAP or Active Directory authentication server. This should be a user in the LDAP or Active Directory who has read access to all the users that you would like to import into the UTM. The Bind DN field accepts two formats: • **A display name in the dn format**. For example: cn=Jamie Hanson,cn=users,dc=test,dc=com. • **A Windows login account name in email format**. For example: jhanson@testAD.com. This last type of bind DN can be used only for a Windows Active Directory server.
Bind Password	The authentication secret or password that is required to access the LDAP or Active Directory authentication server.
LDAP Encryption	From the drop-down list, select the encryption type for the connection between the UTM and the LDAP or Active Directory server: • **None**. The connection is not encrypted. This is the default setting. • **TLS**. The connection uses Transport Layer Security (TLS) encryption. • **SSL**. The connection uses Secure Socket Layer (SSL) encryption.
Search Base	The DN at which to start the search, specified as a sequence of relative distinguished names (RDNs), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany.com, your search base DN might be as follows: dc=yourcompany,dc=com.
UID Attribute	The attribute in the LDAP directory that contains the user's identifier (UID). For an Active Directory, enter **sAMAccountName**. For an OpenLDAP directory, enter **uid**.
Member Groups Attribute	This field is optional. The attribute that is used to identify the groups that an entry belongs to. For an Active Directory, enter **memberOf**. For OpenLDAP, you can enter a customized attribute to identify the groups of an entry.

Table 81. SSL VPN Wizard Step 2 of 6 screen settings (domain settings) (continued)

Setting	Description
Group Members Attribute	This field is optional. The attribute that is used to identify the members of a group. For an Active Directory, enter **member**. For OpenLDAP, you can enter a customized attribute to identify the members of a group.
Additional Filter	This field is optional. A filter that is used when the UTM is searching the LDAP server for matching entries while excluding others. (Use the format described by RFC 2254.) The following search term examples match users only: Active Directory. objectClass=user Open LDAP. objectClass=posixAccount
Radius Port	The port number for the RADIUS server. You can enter a value between 1 and 65535. The default port number is 1812.
Repeat	The period in seconds that the UTM waits for a response from a RADIUS server. You can enter a value between 1 and 10. The default is 3 seconds.
Timeout	The maximum number of times that the UTM attempts to connect to a RADIUS server. You can enter a value between 3 and 30. The default is 5 times.

After you have completed the steps in the SSL VPN Wizard, you can make changes to the domain settings by selecting **Users > Domains**. For more information about domain settings, see *Configure Domains* on page 353.

SSL VPN Wizard Step 3 of 6 (User Settings)

Figure 191.

Note that the previous figure contains an example. Enter the settings as explained in the following table, and then click **Next** to go the following screen.

> **Note:** Do not enter an existing user name in the **User Name** field;
> otherwise, the SSL VPN Wizard will fail and the UTM will reboot to
> recover its configuration.

Table 82. SSL VPN Wizard Step 3 of 6 screen settings (user settings)

Setting	Description
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	When you use the SSL VPN Wizard, the user type is always SSL VPN User. You cannot change the user type on this screen; the user type is displayed for information only.
Group	When you create a new domain on the second SSL VPN Wizard screen, a group with the same name is automatically created. (A user belongs to a group, and a group belongs to a domain.) You cannot change the group on this screen; the group is displayed for information only.
Password	The password that needs to be entered by the user to gain access to the UTM. The password needs to contain alphanumeric, hyphen (-), or underscore (_) characters.
Confirm Password	This field needs to be identical to the password that you entered in the Password field.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes.

After you have completed the steps in the SSL VPN Wizard, you can make changes to the user settings by selecting **Users > Users**. For more information about user settings, see *Configure User Accounts* on page 362.

SSL VPN Wizard Step 4 of 6 (Client Addresses and Routes)

Figure 192.

Note that the previous figure contains an example. Enter the settings as explained in the following table, and then click **Next** to go the following screen.

Note: Do not enter an existing route for a VPN tunnel client in the Destination Network and Subnet Mask fields; otherwise, the SSL VPN Wizard will fail and the UTM will reboot to recover its configuration.

Table 83. SSL VPN Wizard Step 4 of 6 screen settings (client addresses and routes)

Setting	Description
Client IP Address Range	
Enable Full Tunnel Support	Select this check box to enable full-tunnel support. If you leave this check box cleared (which is the default setting), full-tunnel support is disabled but split-tunnel support is enabled, and you need to add a client route by completing the Destination Network and Subnet Mask fields. **Note:** When full-tunnel support is enabled, client routes are not operable.
DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This setting is optional.

Table 83. SSL VPN Wizard Step 4 of 6 screen settings (client addresses and routes) (continued)

Setting	Description
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel has been established.
Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.
Client Address Range Begin	The first IP address of the IP address range that you want to assign to the VPN tunnel clients.
Client Address Range End	The last IP address of the IP address range that you want to assign to the VPN tunnel clients.
Add Routes for VPN Tunnel Clients	
Destination Network	Leave this field blank, or specify a destination network IP address of a local network or subnet that has not yet been used.
Subnet Mask	Leave this field blank to specify the address of the appropriate subnet mask.

After you have completed the steps in the SSL VPN Wizard, you can make changes to the client IP address range and routes by selecting **VPN > SSL VPN > SSL VPN Client**. For more information about client IP address range and routes settings, see *Configure the SSL VPN Client* on page 331.

SSL VPN Wizard Step 5 of 6 (Port Forwarding)

Figure 193.

Note that the previous figure contains an example. Enter the settings as explained in the following table, and then click **Next** to go the following screen.

> **Note:** Do not enter an IP address that is already in use in the upper Local
> Server IP Address field or a port number that is already in use in the
> TCP Port Number field; otherwise, the SSL VPN Wizard will fail and
> the UTM will reboot to recover its configuration.

Table 84. SSL VPN Wizard Step 5 of 6 screen settings (port-forwarding settings)

Setting	Description	
Add New Application for Port Forwarding		
Local Server IP Address	The IP address of an internal server or host computer that remote users have access to.	
TCP Port Number	The TCP port number of the application that is accessed through the SSL VPN tunnel. Following are some commonly used TCP applications and port numbers.	
	FTP Data (usually not needed)	20
	FTP Control Protocol	21
	SSH	22[a]
	Telnet	23[a]
	SMTP (send mail)	25
	HTTP (web)	80
	POP3 (receive mail)	110
TCP Port Number (continued)	NTP (Network Time Protocol)	123
	Citrix	1494
	Terminal Services	3389
	VNC (virtual network computing)	5900 or 5800
Add New Host Name for Port Forwarding		
Local Server IP Address	The IP address of an internal server or host computer that you want to name. **Note:** Both the upper and lower Local Server IP Address fields on this screen (that is, the field in the Add New Application for Port Forwarding section and the field in the Add New Host Name for Port Forwarding section) need to contain the same IP address.	
Fully Qualified Domain Name	The full server name, that is, the host name-to-IP address-resolution for the network server as a convenience for remote users.	

a. Users can specify the port number together with the host name or IP address.

After you have completed the steps in the SSL VPN Wizard, you can make changes to the client IP address range and routes by selecting **VPN** > **SSL VPN** > **Port Forwarding**.

For more information about port-forwarding settings, see *Configure Applications for Port Forwarding* on page 328.

SSL VPN Wizard Step 6 of 6 (Verify and Save Your Settings)

Verify your settings; if you need to make any changes, click the **Back** action button (if necessary several times) to return to the screen on which you want to make changes.

Figure 194.

Click **Apply** to save your settings. If the settings are accepted by the UTM, a message *Operation Succeeded* displays at the top of the screen, and the Welcome to the Netgear Configuration Wizard screen displays again (see *Figure 188* on page 307).

Access the New SSL Portal Login Screen

All screens that you can access from the SSL VPN configuration menu of the web management interface display a user portal link in the right upper corner, above the menu bars (**User Portal**).

When you click the **User Portal** link, the SSL VPN default portal opens (see *Figure 196* on page 321 and *Figure 197* on page 321). This user portal is not the same as the new SSL portal login screen that you defined with the help of the SSL VPN Wizard.

➢ **To open the new SSL portal login screen:**

1. Select **VPN > SSL VPN > Portal Layouts**. The Portal Layouts screen displays (see *Figure 200* on page 325).

2. In the Portal URL field of the List of Layouts table, select the URL that ends with the portal layout name that you defined with the help of the SSL VPN Wizard. The new SSL portal login screen displays. (The following figure shows a SSL portal login screen on the UTM10.)
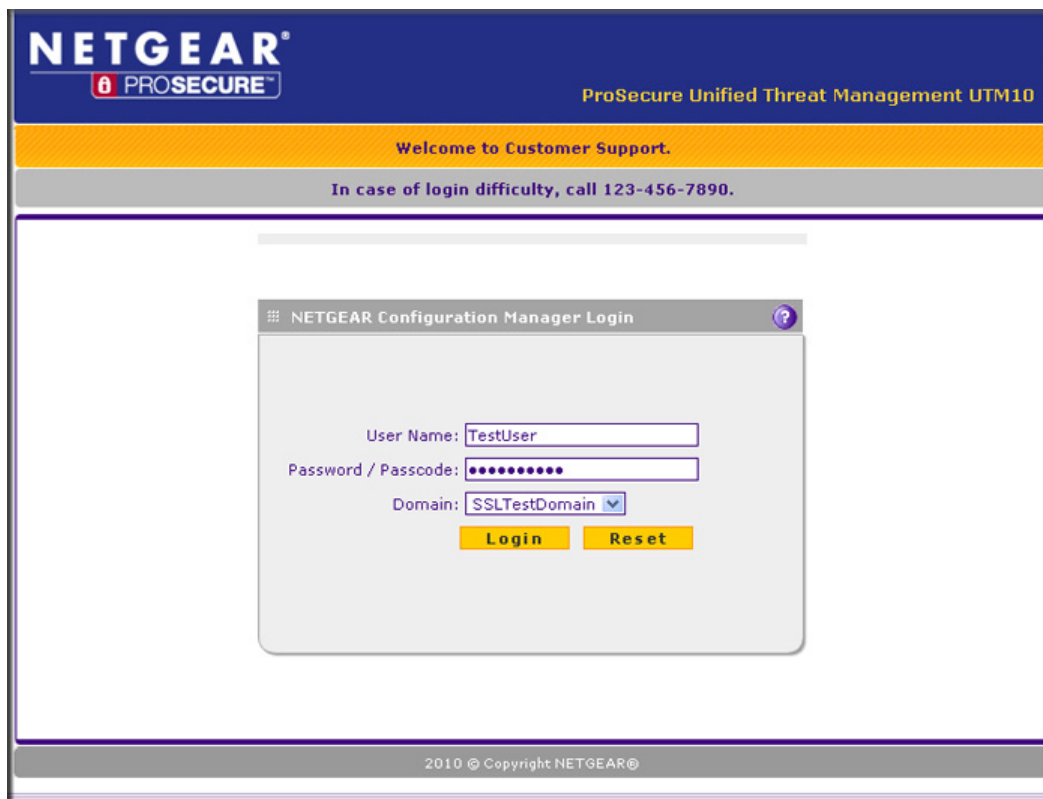
Figure 195.

3. Enter the user name and password that you just created with the help of the SSL VPN Wizard.

---

4. Click **Login**. The default User Portal screen displays. The format of the User Portal screen depends on the settings that you selected on the first screen of the SSL VPN Wizard (see *SSL VPN Wizard Step 1 of 6 (Portal Settings)* on page 308):

   - *Figure 196* shows the User Portal screen with both a VPN Tunnel and a Port Forwarding menu option.

   - *Figure 197* shows the User Portal screen with a Port Forwarding menu option only. The VPN Tunnel menu option is not displayed.
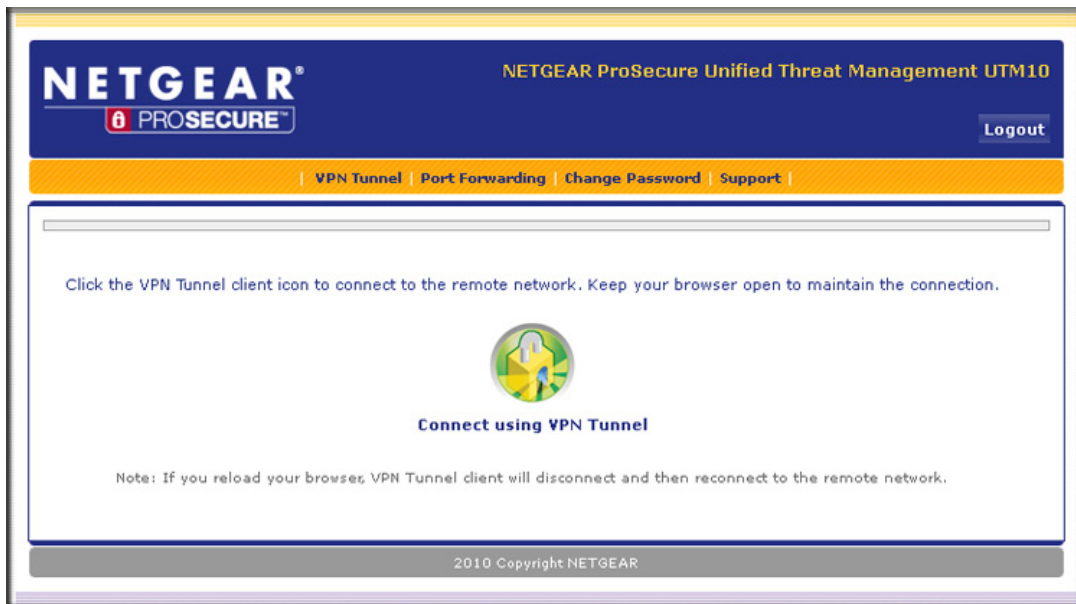
Figure 196.

Figure 197.

The default User Portal screen displays a simple menu that provides the SSL user with the following menu selections:

- **VPN Tunnel**. Provides full network connectivity.
- **Port Forwarding**. Provides access to the network services that you defined as described in *SSL VPN Wizard Step 5 of 6 (Port Forwarding)* on page 317.
- **Change Password**. Allows the user to change his or her password.
- **Support**. Provides access to the NETGEAR website.

Note: The first time that a user attempts to connect through the VPN tunnel, the NETGEAR SSL VPN tunnel adapter is installed; the first time that a user attempts to connect through the port-forwarding tunnel, the NETGEAR port-forwarding engine is installed.

View the UTM SSL VPN Connection Status

To review the status of current SSL VPN tunnels, select **Monitoring > Active Users & VPNs > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:

Figure 198.

The active user's user name, group, and IP address are listed in the table with a time stamp indicating the time and date that the user connected.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

View the UTM SSL VPN Log

➢ **To query the SSL VPN log:**

1. Select **Monitoring > Logs & Reports > Logs Query**. The Logs Query screen displays.
2. From the Log Type drop-down, select **SSL VPN**. The SSL VPN logs display.
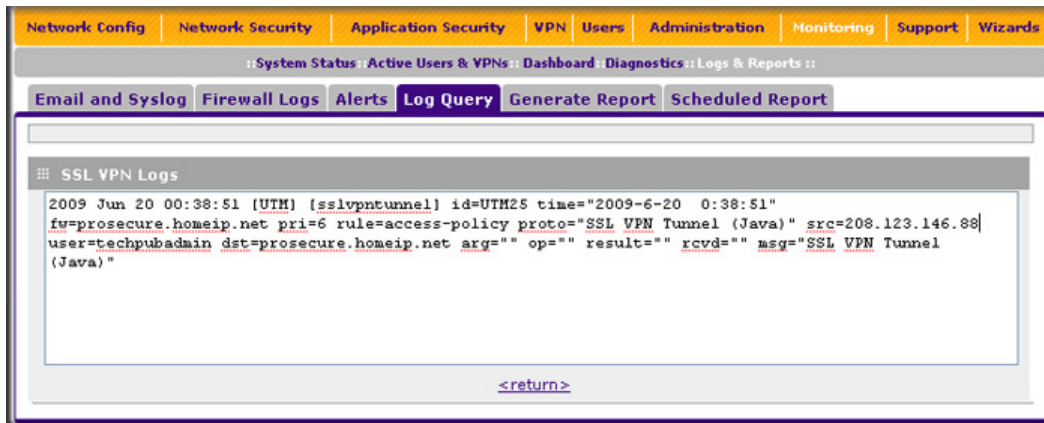
Figure 199.

Manually Configure and Edit SSL Connections

To manually configure and activate SSL connections, perform the following six basic steps in the order that they are presented:

1. Edit the existing SSL portal or create a new one (see *Create the Portal Layout* on page 324).

When remote users log in to the UTM, they see a portal page that you can customize to present the resources and functions that you choose to make available.

2. Create authentication domains, user groups, and user accounts (see *Configure Domains, Groups, and Users* on page 328).)

a. Create one or more authentication domains for authentication of SSL VPN users.

When remote users log in to the UTM, they need to specify a domain to which their login account belongs. The domain determines the authentication method that is used and the portal layout that is presented, which in turn determines the network resources to which the users are granted access. Because you need to assign a portal layout when creating a domain, the domain is created after you have created the portal layout.

b. Create one or more groups for your SSL VPN users.

When you define the SSL VPN policies that determine network resource access for your SSL VPN users, you can define global policies, group policies, or individual policies. Because you need to assign an authentication domain when creating a group, the group is created after you have created the domain.

c. Create one or more SSL VPN user accounts.

Because you need to assign a group when creating a SSL VPN user account, the user account is created after you have created the group.

3. For port forwarding, define the servers and services (see *Configure Applications for Port Forwarding* on page 328).

Create a list of servers and services that can be made available through user, group, or global policies. You can also associate fully qualified domain names (FQDNs) with these servers. The UTM resolves the names to the servers using the list you have created.

4. For SSL VPN tunnel service, configure the virtual network adapter (see *Configure the SSL VPN Client* on page 331).

For the SSL VPN tunnel option, the UTM creates a virtual network adapter on the remote PC that then functions as if it were on the local network. Configure the portal's SSL VPN client to define a pool of local IP addresses to be issued to remote clients, as well as DNS addresses. Declare static routes or grant full access to the local network, subject to additional policies.

5. To simplify policies, define network resource objects (see *Use Network Resource Objects to Simplify Policies* on page 334).

Network resource objects are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies.

6. Configure the SSL VPN policies (see *Configure User, Group, and Global Policies* on page 336).

Policies determine access to network resources and addresses for individual users, groups, or everyone.

Create the Portal Layout

The Portal Layouts screen that you can access from the SSL VPN configuration menu allows you to create a custom page that remote users see when they log in to the portal. Because the page is completely customizable, it provides an ideal way to communicate remote access instructions, support information, technical contact information, or VPN-related news updates to remote users. The page is also well suited as a starting page for restricted users; if mobile users or business partners are permitted to access only a few resources, the page that you create presents only the resources that are relevant to these users.

You apply portal layouts by selecting one from the available portal layouts in the configuration of a domain. When you have completed your portal layout, you can apply the portal layout to one or more authentication domains (see *Configure Domains* on page 353). You can also make the new portal the default portal for the SSL VPN gateway by selecting the default radio button adjacent to the portal layout name.

> **Note:** The UTM's default portal address is https://<IP_Address>/portal/SSL-VPN. The default domain geardomain is attached to the SSL-VPN portal.

You can define individual layouts for the SSL VPN portal. The layout configuration includes the menu layout, theme, portal pages to display, and web cache control options. The default portal layout is the SSL-VPN portal. You can add additional portal layouts. You can also make

any portal the default portal for the UTM by clicking the **Default** button in the Action column of the List of Layouts table, to the right of the desired portal layout.

➢ **To create a new SSL VPN portal layout:**

1. Select **VPN > SSL VPN > Portal Layouts**. The Portal Layouts screen displays. (The following figure shows layouts in the List of Layouts table as an example. The IP addresses that are shown in this figure do not relate to other figures and examples in this manual. The portal URL normally includes the WAN IP address of the UTM.)
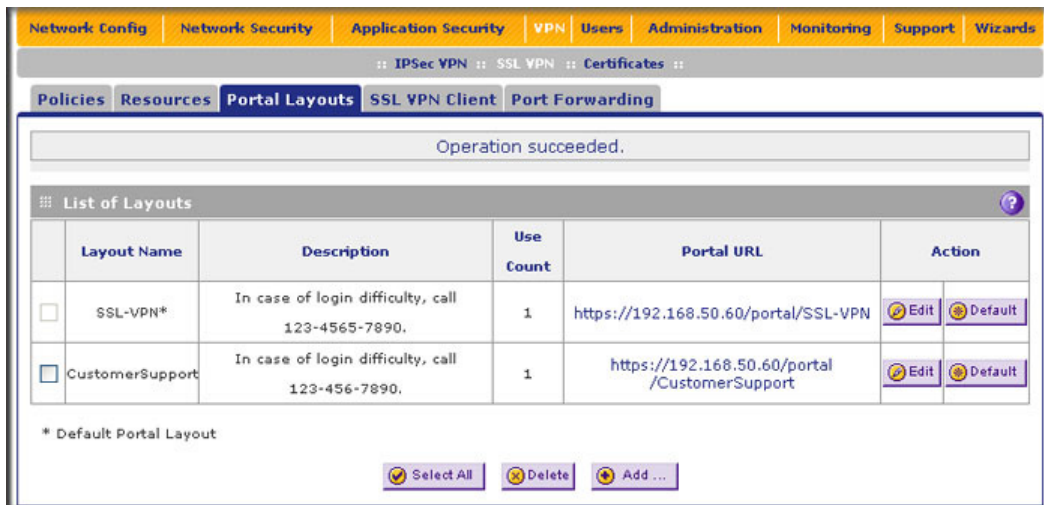
Figure 200.

The List of Layouts table displays the following fields:

- **Layout Name**. The descriptive name of the portal.
- **Description**. The banner message that is displayed at the top of the portal (see *Figure 195* on page 320).
- **Use Count**. The number of remote users that are currently using the portal.
- **Portal URL**. The URL at which the portal can be accessed.
- **Action**. The table buttons, which allow you to edit the portal layout or set it as the default.

2. Under the List of Layouts table, click the **Add** table button. The Add Portal Layout screen displays. (The following figure shows an example.)
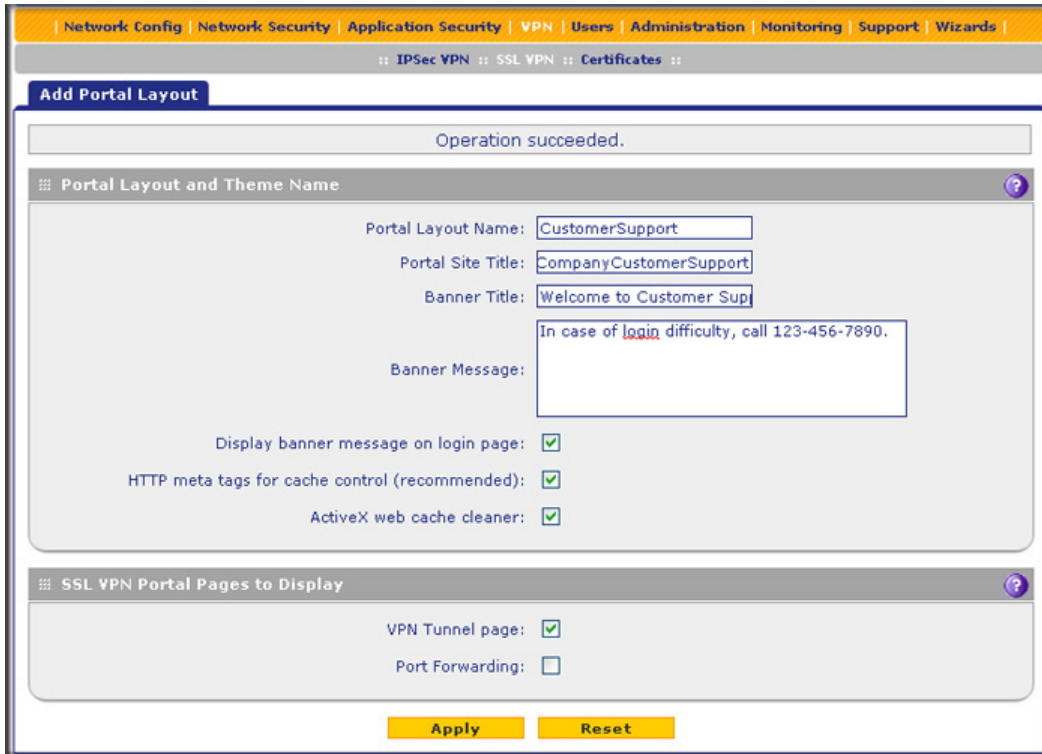
Figure 201.

3. Complete the fields and select the check boxes as explained in the following table:

Table 85. Add Portal Layout screen settings

Setting	Description
Portal Layout and Theme Name	
Portal Layout Name	A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL. **Note:** Custom portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at https://vpn.company.com, and you create a portal layout named CustomerSupport, then users access the website at https://vpn.company.com/portal/CustomerSupport. **Note:** Only alphanumeric characters, hyphens (-), and underscores (_) are accepted in the Portal Layout Name field. If you enter other types of characters or spaces, the layout name is truncated before the first nonalphanumeric character. **Note:** Unlike most other URLs, this name is case-sensitive.
Portal Site Title	The title that displays at the top of the user's web browser window, for example, *Company Customer Support*.

Table 85. Add Portal Layout screen settings (continued)

Setting	Description
Banner Title	The banner title of a banner message that users see before they log in to the portal, for example, *Welcome to Customer Support*. **Note:** For an example, see *Figure 195* on page 320. The banner title text is displayed in the orange header bar.
Banner Message	The text of a banner message that users see before they log in to the portal, for example, *In case of login difficulty, call 123-456-7890*. Enter a plain text message, or include HTML and JavaScript tags. The maximum length of the login screen message is 4096 characters. **Note:** For an example, see *Figure 195* on page 320. The banner message text is displayed in the gray header bar.
Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen as shown in *Figure 195* on page 320.
HTTP meta tags for cache control (recommended)	Select this check box to apply cache control directives for the HTTP meta tags to this portal layout. Cache control directives include: <meta http-equiv="pragma" content="no-cache"> <meta http-equiv="cache-control" content="no-cache"> <meta http-equiv="cache-control" content="must-revalidate"> **Note:** NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user's web browser cache.
ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to delete all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. The ActiveX web cache control is ignored by web browsers that do not support ActiveX.
SSL VPN Portal Pages to Display	
VPN Tunnel page	To provide full network connectivity, select this check box.
Port Forwarding	To provide access to specific defined network services, select this check box. **Note:** Any pages that are not selected are not visible from the SSL VPN portal; however, users can still access the hidden pages unless you create SSL VPN access policies to prevent access to these pages.

4. Click **Apply** to save your settings. The new portal layout is added to the List of Layouts table. For information about how to display the new portal layout, see *Access the New SSL Portal Login Screen* on page 320.

➢ **To edit a portal layout:**

1. On the Portal Layouts screen (see *Figure 200* on page 325), click the **Edit** button in the Action column for the portal layout that you want to modify. The Edit Portal Layout screen displays. This screen is identical to the Add Portal Layout screen (see the previous figure).

2. Modify the settings as explained in the previous table.

3. Click **Apply** to save your settings.

➢ **To delete one or more portal layouts:**

1. On the Portal Layouts screen (see *Figure 200* on page 325), select the check box to the left of each portal layout that you want to delete, or click the **Select All** table button to select all layouts. (You cannot delete the SSL-VPN default portal layout.)

2. Click the **Delete** table button.

Configure Domains, Groups, and Users

Remote users connecting to the UTM through an SSL VPN portal need to be authenticated before they are granted access to the network. The login screen that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines both the authentication method and the portal layout that are used.

You need to create name and password accounts for the SSL VPN users. When you create a user account, you need to specify a group. Groups are used to simplify the application of access policies. When you create a group, you need to specify a domain. Therefore, you should create any domains first, then groups, and then user accounts.

For information about how to configure domains, groups, and users, see *Configure Authentication Domains, Groups, and Users* on page 345.

Configure Applications for Port Forwarding

Port forwarding provides access to specific defined network services. To define these services, you need to specify the internal server addresses and port numbers for TCP applications that are intercepted by the port-forwarding client on the user's PC. This client reroutes the traffic to the UTM.

Add Servers and Port Numbers

To configure port forwarding, you need to define the IP addresses of the internal servers and the port number for TCP applications that are available to remote users.

➢ **To add a server and a port number:**

1. Select **VPN > SSL VPN > Port Forwarding**. The Port Forwarding screen displays. (The following figure shows an example.)
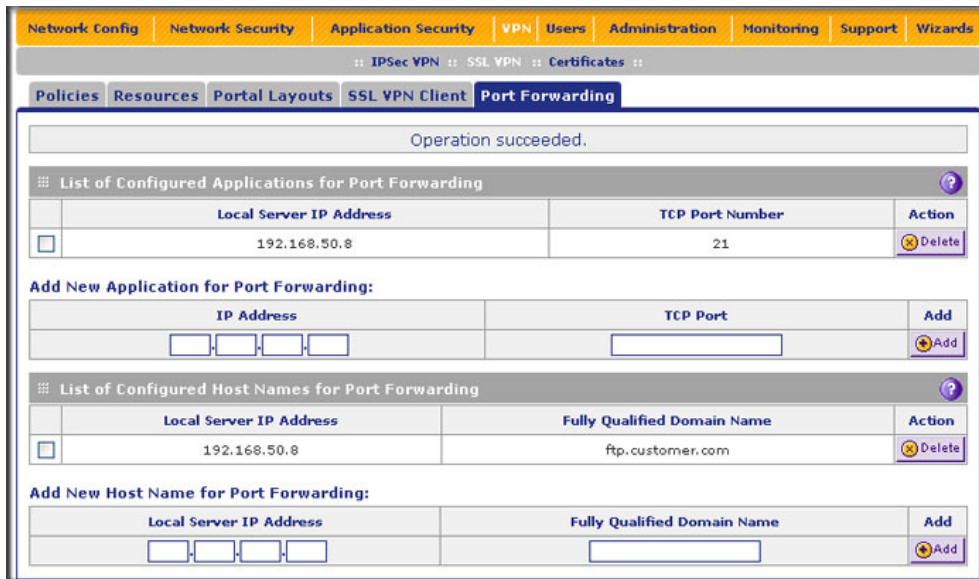
Figure 202.

2. In the Add New Application for Port Forwarding section of the screen, specify information in the following fields:

- **IP Address**. The IP address of an internal server or host computer that a remote user has access to.

- **TCP Port**. The TCP port number of the application that is accessed through the SSL VPN tunnel. The following table lists some commonly used TCP applications and port numbers.

Table 86. Port-forwarding applications/TCP port numbers

TCP application	Port number
FTP data (usually not needed)	20
FTP Control Protocol	21
SSH	22[a]
Telnet	23[a]
SMTP (send mail)	25
HTTP (web)	80
POP3 (receive mail)	110
NTP (Network Time Protocol)	123
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

> *a. Users can specify the port number together with the host name or IP address.*

3. Click the **Add** table button. The new application entry is added to the List of Configured Applications for Port Forwarding table. Remote users can now securely access network applications once they have logged in to the SSL VPN portal and launched port forwarding.

➤ **To delete an application from the List of Configured Applications for Port Forwarding table:**

1. Select the check box to the left of the application that you want to delete.

2. Click the **Delete** table button in the Action column.

Add a New Host Name

After you have configured port forwarding by defining the IP addresses of the internal servers and the port number for TCP applications that are available to remote users, you then can also specify host-name-to-IP-address resolution for the network servers as a convenience for users. Host name resolution allows users to access TCP applications at familiar addresses such as mail.*example*.com or ftp.*customer*.com rather than by IP addresses.

➤ **To add servers and host names for client name resolution:**

1. Select **VPN > SSL VPN > Port Forwarding**. The Port Forwarding screen displays (see *Figure 202* on page 329).

2. In the Add New Host Name for Port Forwarding section of the screen, specify information in the following fields:

- **Local Server IP Address**. The IP address of an internal server or host computer that you want to name.

- **Fully Qualified Domain Name**. The full server name.

> **Note:** If the server or host computer that you want to name does not display in the List of Configured Applications for Port Forwarding table, you need to add it before you can rename it.

3. Click the **Add** table button. The new application entry is added to the List of Configured Host Names for Port Forwarding table.

➤ **To delete a name from the List of Configured Host Names for Port Forwarding table:**

1. Select the check box to the left of the name that you want to delete.

2. Click the **Delete** table button in the Action column.

Configure the SSL VPN Client

The SSL VPN client on the UTM assigns IP addresses to remote VPN tunnel clients. Because the VPN tunnel connection is a point-to-point connection, you can assign IP addresses from the local subnet to the remote VPN tunnel clients.

The following are some additional considerations:

- So that the virtual (PPP) interface address of a VPN tunnel client does not conflict with addresses on the local network, configure an IP address range that does not directly overlap with addresses on your local network. For example, if 192.168.1.1 through 192.168.1.100 are currently assigned to devices on the local network, then start the client address range at 192.168.1.101, or choose an entirely different subnet altogether.

- The VPN tunnel client cannot contact a server on the local network if the VPN tunnel client's Ethernet interface shares the same IP address as the server or the UTM. (For example, if your PC has a network interface IP address of 10.0.0.45, then you cannot contact a server on the remote network that also has the IP address 10.0.0.45.)

- Select whether you want to enable full-tunnel or split-tunnel support based on your bandwidth:
  - A full tunnel sends all of the client's traffic across the VPN tunnel.
  - A split tunnel sends only traffic that is destined for the local network based on the specified client routes. All other traffic is sent to the Internet. A split tunnel allows you to manage bandwidth by reserving the VPN tunnel for local traffic only.

- If you enable split-tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you need to add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel.

Configure the Client IP Address Range

First determine the address range to be assigned to VPN tunnel clients, and then define the address range.

➢ **To define the client IP address range:**

1. Select **VPN > SSL VPN > SSL VPN Client**. The SSL VPN Client screen displays:
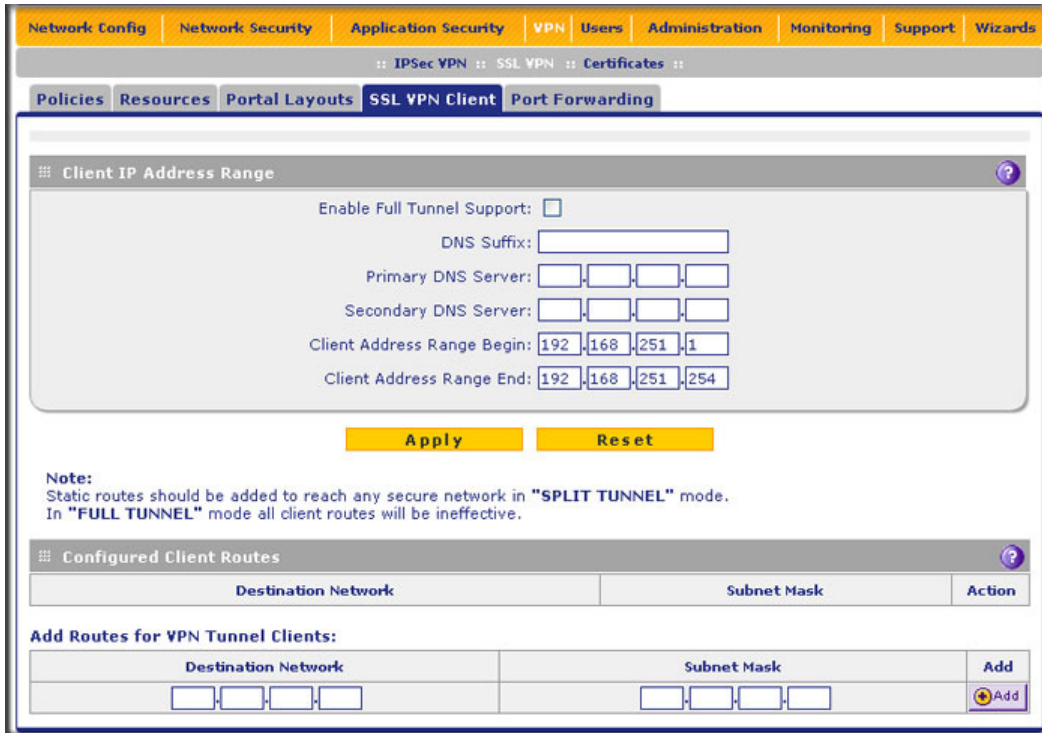
Figure 203.

2. Select the check box and complete the fields as explained in the following table:

Table 87. SSL VPN Client screen settings

Setting	Description
Client IP Address Range	
Enable Full Tunnel Support	Select this check box to enable full-tunnel support. If you leave this check box cleared (which is the default setting), full-tunnel support is disabled but split-tunnel support is enabled, and you need to add client routes (see *Add Routes for VPN Tunnel Clients* on page 333). **Note:** When full-tunnel support is enabled, client routes are not operable.
DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel has been established.
Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.

Table 87. SSL VPN Client screen settings (continued)

Setting	Description
Client Address Range Begin	The first IP address of the IP address range that you want to assign to the VPN tunnel clients.
Client Address Range End	The last IP address of the IP address range that you want to assign to the VPN tunnel clients.

3. Click **Apply** to save your settings. VPN tunnel clients are now able to connect to the UTM and receive a virtual IP address in the client address range.

Add Routes for VPN Tunnel Clients

The VPN tunnel clients assume that the following networks are located across the VPN-over-SSL tunnel:

- The subnet that contains the client IP address (that is, PPP interface), as determined by the class of the address (Class A, B, or C).

- Subnets that are specified in the Configured Client Routes table on the SSL VPN Client screen.

If the assigned client IP address range is in a different subnet from the local network, or if the local network has multiple subnets, or if you select split-mode tunnel operation, you need to define client routes.

➢ **To add an SSL VPN tunnel client route:**

1. Select **VPN > SSL VPN > SSL VPN Client**. The SSL VPN Client screen displays (see *Figure 203* on page 332).

2. In the Add Routes for VPN Tunnel Clients section of the screen, specify information in the following fields:

- **Destination Network**. The destination network IP address of a local network or subnet. For example, enter 192.168.1.60.

- **Subnet Mask**. The address of the appropriate subnet mask.

3. Click the **Add** table button. The new client route is added to the Configured Client Routes table.

If VPN tunnel clients are already connected, restart the UTM. Restarting forces clients to reconnect and receive new addresses and routes.

➢ **To change the specifications of an existing route and to delete an old route:**

1. Add a new route to the Configured Client Routes table.

2. In the Configured Client Routes table, to the right of the route that is out-of-date, click the **Delete** table button.

If an existing route is no longer needed for any reason, you can delete it.

Use Network Resource Objects to Simplify Policies

Network resources are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies. You do not need to redefine the same set of IP addresses or address ranges when you configure the same access policies for multiple users.

Defining network resources is optional; smaller organizations can choose to create access policies using individual IP addresses or IP networks rather than predefined network resources. But for most organizations, NETGEAR recommends that you use network resources. If your server or network configuration changes, you can perform an update quickly by using network resources instead of individually updating all of the user and group policies.

Add New Network Resources

➢ **To define a network resource:**

1. Select **VPN > SSL VPN > Resources**. The Resources screen displays. (The following figure shows some resources in the List of Resources table as an example.)
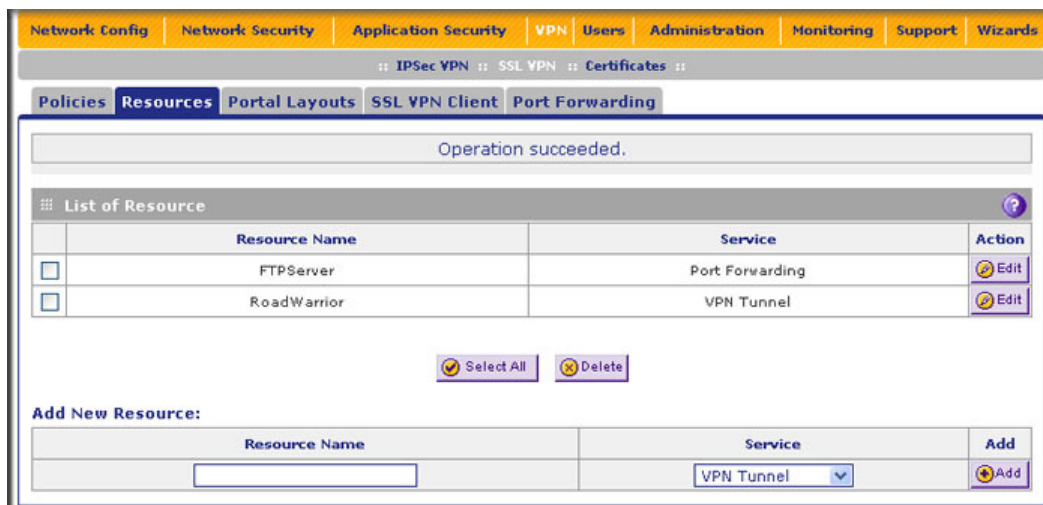
Figure 204.

2. In the Add New Resource section of the screen, specify information in the following fields:

   • **Resource Name**. A descriptive name of the resource for identification and management purposes.

   • **Service**. From the Service drop-down list, select the type of service to which the resource applies:

     - **VPN Tunnel**. The resource applies only to a VPN tunnel.

     - **Port Forwarding**. The resource applies only to port forwarding.

     - **All**. The resource applies both to a VPN tunnel and to port forwarding.

3. Click the **Add** table button. The new resource is added to the List of Resources table.

➢ **To delete one or more network resources:**

1. Select the check box to the left of each network resource that you want to delete, or click the **Select All** table button to select all network resources.

2. Click the **Delete** table button.

Edit Network Resources to Specify Addresses

➢ **To edit network resources:**

1. Select **VPN > SSL VPN > Resources**. The Resources screen displays (see the previous figure, which shows some examples).

2. In the List of Resources table, to the right of the new resource in the Action column, click the **Edit** table button. A new screen displays. (The following figure shows an example.)
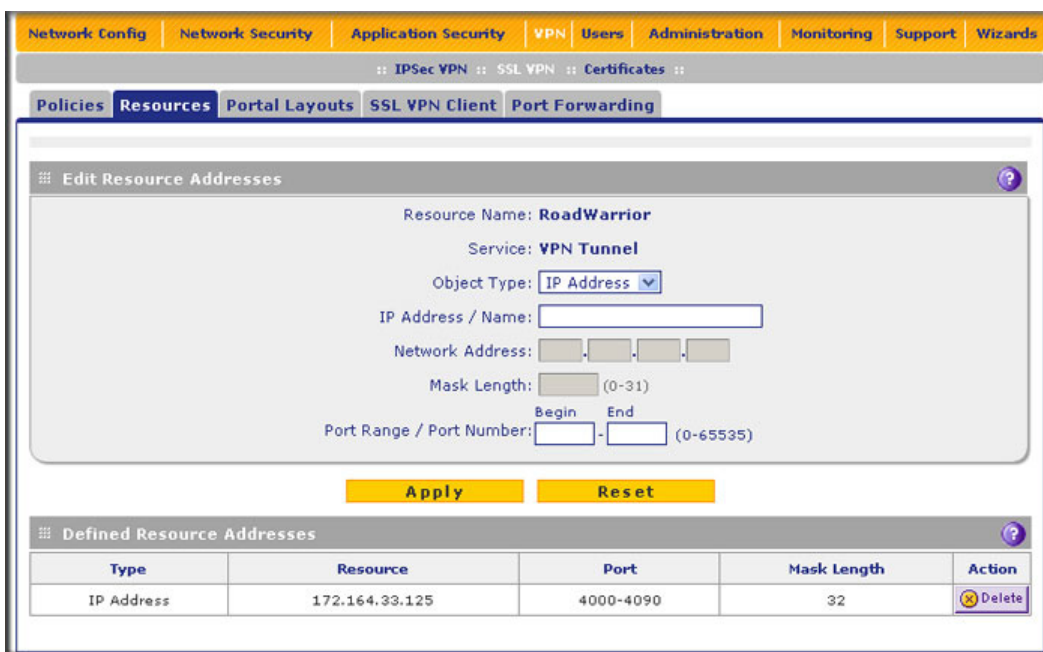
Figure 205.

3. Complete the fields and make your selection from the drop-down list as explained in the following table:

Table 88. Resources screen settings to edit a resource

Setting	Description
Add Resource Addresses	
Resource Name	The unique identifier for the resource. You cannot modify the resource name after you have created it on the first Resources screen.

Table 88. Resources screen settings to edit a resource (continued)

Setting	Description	
Service	The SSL service that is assigned to the resource. You cannot modify the service after you have assigned it to the resource on the first Resources screen.	
Object Type	From the drop-down list, select one of the following options: • **IP Address**. The object is an IP address. You need to enter the IP address or the FQDN in the IP Address / Name field. • **IP Network**. The object is an IP network. You need to enter the network IP address in the Network Address field and the network mask length in the Mask Length field.	
	IP Address / Name	Applicable only when you select IP Address as the object type. Enter the IP address or FQDN for the location that is permitted to use this resource.
	Network Address	Applicable only when you select IP Network as the object type. Enter the network IP address for the locations that are permitted to use this resource.
Object Type (continued)	Mask Length	Applicable only when you select IP Network as the object type. As an option, enter the network mask (0–31) for the locations that are permitted to use this resource.
Port Range / Port Number	A port or a range of ports (0–65535) to apply the policy to. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.	

4. Click **Apply** to save your settings. The new configuration is added to the Defined Resource Addresses table.

To delete a configuration from the Defined Resource Addresses table, click the **Delete** table button to the right of the configuration that you want to delete.

Configure User, Group, and Global Policies

You can define and apply user, group, and global policies to predefined network resource objects, IP addresses, address ranges, or all IP addresses, and to different SSL VPN services. A specific hierarchy is invoked over which policies take precedence. The UTM policy hierarchy is defined as follows:

- User policies take precedence over all group policies.
- Group policies take precedence over all global policies.
- If two or more user, group, or global policies are configured, the *most specific* policy takes precedence.

For example, a policy that is configured for a single IP address takes precedence over a policy that is configured for a range of addresses. And a policy that applies to a range of IP addresses takes precedence over a policy that is applied to all IP addresses. If two or more

IP address ranges are configured, then the smallest address range takes precedence. Host names are treated the same as individual IP addresses.

Network resources are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire network resource.

For example, assume the following global policy configuration:

- Policy 1. A Deny rule has been configured to block all services to the IP address range 10.0.0.0–10.0.0.255.
- Policy 2. A Deny rule has been configured to block FTP access to 10.0.1.2–10.0.1.10.
- Policy 3. A Permit rule has been configured to allow FTP access to the predefined network resource with the name FTP Servers. The FTP Servers network resource includes the following addresses: 10.0.0.5–10.0.0.20 and the FQDN ftp.*company*.com, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies have been configured, if a user attempted to access FTP servers at the following addresses, the actions listed would occur:

- 10.0.0.1. The user would be blocked by Policy 1.
- 10.0.1.5. The user would be blocked by Policy 2.
- 10.0.0.10. The user would be granted access by Policy 3. The IP address range 10.0.0.5–10.0.0.20 is more specific than the IP address range that is defined in Policy 1.
- ftp.*company*.com. The user would be granted access by Policy 3. A single host name is more specific than the IP address range that is configured in Policy 2.

> **Note:** The user would not be able to access ftp.*company*.com using its IP address 10.0.1.3. The UTM's policy engine does not perform reverse DNS lookups.

View Policies

➤ **To view the existing policies:**

1. Select **VPN > SSL VPN**. The SSL VPN submenu tabs display, with the Policies screen in view. (The following figure shows some examples.)
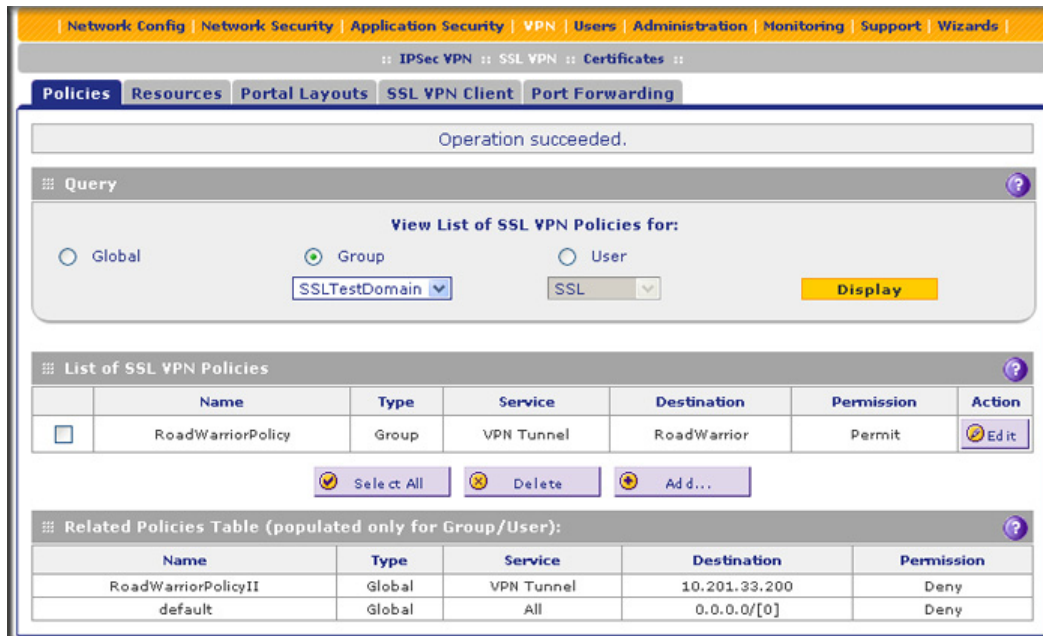
Figure 206.

2. Make your selection from the following Query options:
   - To view all global policies, select the **Global** radio button.
   - To view group policies, select the **Group** radio button, and select the relevant group's name from the drop-down list.
   - To view user policies, select the **User** radio button, and select the relevant user's name from the drop-down list.
3. Click the **Display** action button. The List of SSL VPN Policies table displays the list for your selected Query option.

Add a Policy

➢ **To add an SSL VPN policy:**

1. Select **VPN > SSL VPN**. The SSL VPN submenu tabs display, with the Policies screen in view (see the previous figure).
2. Under the List of SSL VPN Policies table, click the **Add** table button. The Add SSL VPN Policy screen displays:
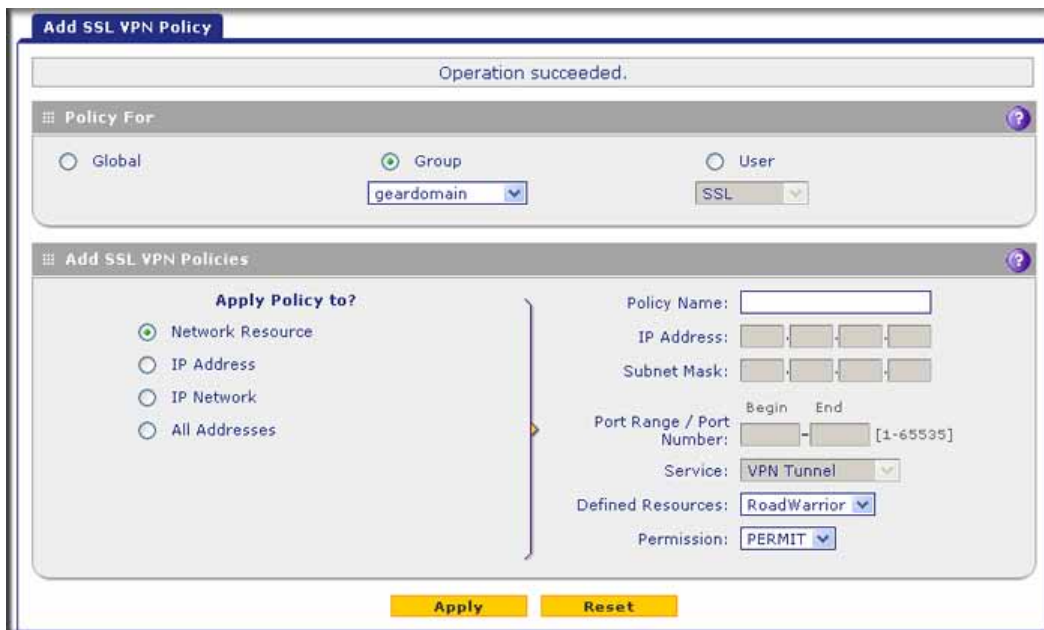
Figure 207.

3. Select the radio buttons, complete the fields, and make your selection from the drop-down lists as explained in the following table:

Table 89. Add SSL VPN Policy screen settings

Setting	Description
Policy For	
Select one of the following radio buttons to specify the type of SSL VPN policy: • **Global**. The new policy is global and includes all groups and users. • **Group**. The new policy needs to be limited to a single group. From the drop-down list, select a group name. For information about how to create groups, see *Configure Groups* on page 359. • **User**. The new policy needs to be limited to a single user. From the drop-down list, select a user name. For information about how to create user accounts, see *Configure User Accounts* on page 362.	
Add SSL VPN Policies	
Apply Policy For	Select one of the following radio buttons to specify how the policy is applied. When you select a radio button, the fields and drop-down lists that apply to your selection (see explanations later in this table) unmask onscreen. • **Network Resource**. The policy is applied to a network resource that you have defined on the Resources screen (see *Use Network Resource Objects to Simplify Policies* on page 334). • **IP Address**. The policy is applied to a single IP address. • **IP Network**. The policy is applied to a network address. • **All Addresses**. The policy is applied to all addresses.

Table 89. Add SSL VPN Policy screen settings (continued)

Setting	Description		
Apply Policy For (continued)	Network Resource	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		Defined Resources	From the drop-down list, select a network resource that you have defined on the Resources screen (see *Use Network Resource Objects to Simplify Policies* on page 334).
		Permission	From the drop-down list, select **PERMIT** or **DENY** to specify whether the policy permits or denies access.
	IP Address	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		IP Address	The IP address to which the SSL VPN policy is applied.
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select **PERMIT** or **DENY** to specify whether the policy permits or denies access.
	IP Network	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		IP Address	The network IP address to which the SSL VPN policy is applied.
		Subnet Mask	The network subnet mask to which the SSL VPN policy is applied.
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.

Table 89. Add SSL VPN Policy screen settings (continued)

Setting	Description			
Apply Policy For (continued)	IP Network (continued)	Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.	
		Permission	From the drop-down list, select **PERMIT** or **DENY** to specify whether the policy permits or denies access.	
	All Addresses	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.	
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.	
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.	
		Permission	From the drop-down list, select **PERMIT** or **DENY** to specify whether the policy permits or denies access.	

4. Click **Apply** to save your settings. The policy is added to the List of SSL VPN Policies table on the Policies screen. The new policy goes into effect immediately.

Note: If you have configured SSL VPN user policies, ensure that HTTPS remote management is enabled (see *Configure Remote Management Access* on page 399). If HTTPS remote management is not enabled, all SSL VPN user connections are disabled.

➢ **To edit an SSL VPN policy:**

1. On the Policies screen (see *Figure 206* on page 338), click the **Edit** button in the Action column for the SSL VPN policy that you want to modify. The Edit SSL VPN Policy screen displays. This screen is identical to the Add SSL VPN Policy screen (see previous screen).

2. Modify the settings as explained in the previous table.

3. Click **Apply** to save your settings.

➢ **To delete one or more SSL VPN policies:**

1. On the Policies screen (see *Figure 206* on page 338), select the check box to the left of each SSL VPN policy that you want to delete, or click the **Select All** table button to select all policies.

2. Click the **Delete** table button.

Managing Users, Authentication, and VPN Certificates 9

This chapter describes how to manage users, authentication, and security certificates for IPSec VPN and SSL VPN. This chapter contains the following sections:

- *Authentication Process and Options*
- *Configure Authentication Domains, Groups, and Users*
- *Manage Digital Certificates for VPN Connections*

Authentication Process and Options

Users are assigned to a group, and a group is assigned to a domain. Therefore, you should first create any domains, then groups, then user accounts.

Note: Do not confuse the authentication groups with the LAN groups that are discussed in *Manage Groups and Hosts (LAN Groups)* on page 106.

You need to create name and password accounts for all users who need to be able to connect to the UTM. This includes administrators, guests, and SSL VPN clients. Accounts for IPSec VPN clients are required only if you have enabled Extended Authentication (XAUTH) in your IPSec VPN configuration.

Users connecting to the UTM need to be authenticated before being allowed to access the UTM or the VPN-protected network. The login screen that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines the authentication method that is used and, for SSL connections, the portal layout that is presented.

Note: IPSec VPN users always belong to the default domain (geardomain) and are not assigned to groups.

Except in the case of IPSec VPN users, when you create a user account, you need to specify a group. When you create a group, you need to specify a domain.

The UTM support security policies that are based on an Active Directory with single sign-on (SSO) through the use of the DC agent and additional Lightweight Directory Access Protocol (LDAP) configuration options (see *Configure Authentication Domains, Groups, and Users* on page 345).

The following table summarizes the external authentication protocols and methods that the UTM supports.

Table 90. External authentication protocols and methods

Authentication protocol or method	Description
PAP	Password Authentication Protocol (PAP) is a simple protocol in which the client sends a password in clear text.
CHAP	Challenge Handshake Authentication Protocol (CHAP) executes a three-way handshake in which the client and server trade challenge messages, each responding with a hash of the other's challenge message that is calculated using a shared secret value.
RADIUS	A network-validated PAP, CHAP, MSCHAP, or MSCHAPv2 password-based authentication method that functions with Remote Authentication Dial In User Service (RADIUS).
MIAS	A network-validated PAP or CHAP password-based authentication method that functions with Microsoft Internet Authentication Service (MIAS), which is a component of Microsoft Windows 2003 Server.
WiKID	WiKID Systems is a PAP or CHAP key-based two-factor authentication method that functions with public key cryptography. The client sends an encrypted PIN to the WiKID server and receives a one-time passcode with a short expiration period. The client logs in with the passcode. See *Appendix E, Two-Factor Authentication*, for more on WiKID authentication.
NT Domain	A network-validated domain-based authentication method that functions with a Microsoft Windows NT Domain authentication server. This authentication method has been superseded by Microsoft Active Directory authentication but is supported to authenticate legacy Windows clients.
Active Directory	A network-validated domain-based authentication method that functions with a Microsoft Active Directory authentication server. Microsoft Active Directory authentication servers support a group and user structure. Because the Active Directory supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on Active Directory attributes. The UTM support single sign-on (SSO) through the use of the DC agent and additional LDAP configuration options. **Note:** A Microsoft Active Directory database uses an LDAP organization schema.

Table 90. External authentication protocols and methods (continued)

Authentication protocol or method	Description
LDAP	A network-validated domain-based authentication method that functions with a Lightweight Directory Access Protocol (LDAP) authentication server. LDAP is a standard for querying and updating a directory. Because LDAP supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on LDAP attributes.
	The UTM support single sign-on (SSO) through the use of the DC agent and additional LDAP configuration options.

Configure Authentication Domains, Groups, and Users

This section contains the following subsections:

- *Login Portals*
- *Active Directories and LDAP Configurations*
- *Configure Domains*
- *Configure Groups*
- *Configure User Accounts*
- *Set User Login Policies*
- *Change Passwords and Other User Settings*
- *DC Agent*
- *Configure RADIUS VLANs*
- *Configure Global User Settings*
- *View and Log Out Active Users*

Login Portals

The login screen and authentication on the UTM depend on the user type. There are two basic user types on the UTM that are explained in the following sections:

- *Administrative Users and Users with Guest Privileges*
- *Users with Special Access Privileges*
- *Unauthenticated or Anonymous Users*

Administrative Users and Users with Guest Privileges

Users with administrative and guest privileges on the UTM need to log in through the NETGEAR Configuration Manager Login screen (see the following figure), where they are authenticated through the UTM's local user database. These users need to provide their user name and password. After they have been authenticated, they then can access the web management interface to view or change the UTM's configuration.

For information about how to configure and modify accounts for administrative users and users with guest privileges, see *Configure User Accounts* on page 362 and *Change Passwords and Other User Settings* on page 369.
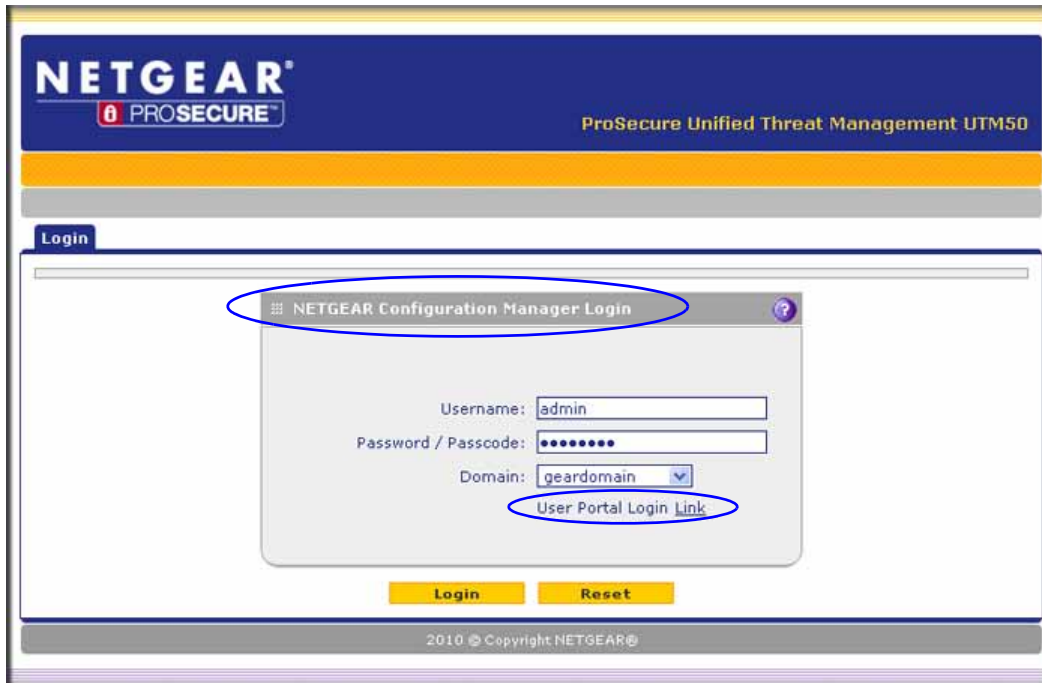
Figure 208.

Users with Special Access Privileges

User who have a computer behind the UTM and who are assigned access policies that differ from the UTM's default email and web access policies (see *Set Web Access Exception Rules* on page 221) need to log in through the User Portal Login screen (see the following figure).

These users need to provide their user name and password, and select the domain to which you have assigned them so they can be authenticated according to the method that you have configured for the domain.

The lower part of the NETGEAR Configuration Manager Login screen (see the previous figure) provides a User Portal Login Link, but you would typically provide users a direct link to the User Portal Login screen instead of letting them pass through the NETGEAR Configuration Manager Login screen. The following figure shows the default User Portal Login screen. For information about how to configure SSL VPN portals, see *Use the SSL VPN Wizard for Client Configurations* on page 307 and *Create the Portal Layout* on page 324.
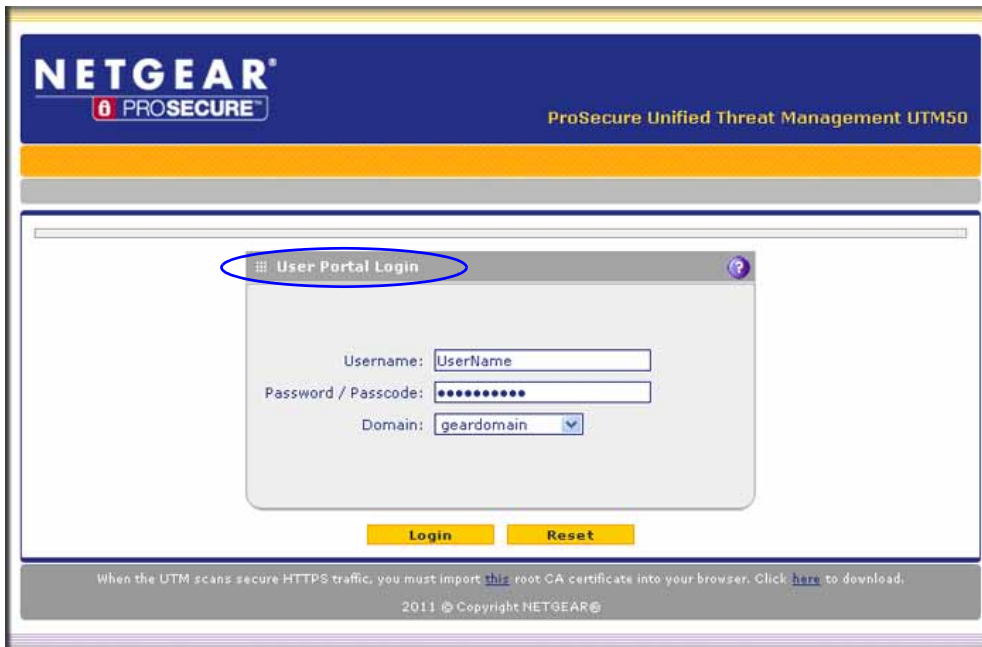
Figure 209.

> **Note:** The first time that a user remotely connects to a UTM with a browser through an SSL connection, he or she might get a warning message about the SSL certificate. The user can follow the directions of his or her browser to accept the SSL certificate, or import the UTM's root certificate by selecting the link at the bottom of the User Portal Login screen.

After a user has logged in through the User Portal Login screen, a confirmation screen displays:

Figure 210.

If you do *not* use the DC agent in your configuration (see *DC Agent* on page 370), after completing a session, a user needs to log out manually by following these steps:

1. Return to the User Portal Login screen (see *Figure 209* on page 347).

> **Note:** The user needs to know how to return to the User Portal Login screen. The administrator needs to provide the User Portal Login URL:
> https://<IP_address>/~common/cgi-bin/user_login.pl or
> https://<FullyQualifiedDomainName>/~common/cgi-bin/user_login.pl
>
> Alternately, the administrator can provide the NETGEAR Configuration Manager Login screen, from which the user can access the User Portal Login screen:
> https://<IP_address> or
> https://<FullyQualifiedDomainName>

---

2. Log in again.
3. On the confirmation screen (see the previous figure), click the **Logout** link.

⚠️ **WARNING!**

If you do *not* use the DC agent in your configuration, make sure that users understand that they need to log out after completing a session in order to prevent subsequent users from inheriting access privileges that were not assigned to them.

For information about how to configure and modify accounts for users with special access privileges, see the following sections:

- *Configure User Accounts*
- *Set User Login Policies*
- *Change Passwords and Other User Settings*

Unauthenticated or Anonymous Users

If you set up an open network, you would want to allow unauthenticated users to surf anonymously until they intend to proceed past a blocked Web activity and would need to provide credentials to the UTM. For a secure network, you would use a more restrictive access policy for unauthenticated users and a less restricted access policy for authenticated users.

The UTM9S has the capability to quarantine emails and spam messages. For information about how end users can send a spam report to an email address, see *Spam Reports for End Users* on page 472.

Active Directories and LDAP Configurations

> **Note:** For an overview of the authentication options that the UTM supports, see *Authentication Process and Options* on page 343.

The UTM supports security policies that are based on an Active Directory with single sign-on (SSO) through the use of the DC agent (see *DC Agent* on page 370) and additional LDAP configuration options.

> **Note:** This manual assumes that you already have some knowledge of Active Directories and LDAP servers.

How an Active Directory Works

Understanding how a typical Active Directory (AD) works might be of help when you are specifying the settings for the LDAP and Active Directory domains on the UTM.

The following applies to a typical AD:

- Organizational unit (OU), common name (CN), and domain controller (DC) can all be used to build a search base in the AD. The following applies to the OU and CN containers:
    - An AD administrator can create an OU but cannot create a CN that was built in the AD server.
    - An AD administrator can apply a global policy object (GPO) to an OU but not to a CN.
- An OU is created in the root node (for example, dc=companyname, dc=com) of the hierarchy. In a company AD, an OU often represents a regional office or department.
- A group is created under cn=users.
- A user is created under each OU so that the user can logically show in a tree of the AD server.
- A relationship between a group and users is built using their attributes (by default: member and memberOf). These show in a lookup result.

The following is an example of how to set the search base:

If a company AD server has cn=users and ou=companyname defined and both are specified under dc=companyname,dc=com, the search base needs to be set as dc=companyname,dc=com in order for the UTM to search both users and groups.

If the size limit is exceeded so that dc=companyname,dc=com misses some entries during the lookup process, a user can still be correctly authenticated. However, to prevent the size limit from being exceeded, an AD administrator needs to set a larger value in the LDAP server configuration so that the entire list of users and groups is returned in the lookup result.

Another workaround is to use a specific search name or a name with a wildcard in the lookup process, so that the subset of the entire list is returned in the lookup result.

How to Bind a DN in an Active Directory Configuration

Understanding how to bind a distinguished name (DN) in an Active Directory (AD) configuration might be of help when you are specifying the settings for the AD domains on the UTM.

In this example, the AD domain name is testAD.com, and the AD server has the IP address 192.168.35.115 on port 389.

➢ **To bind a user with the name Jamie Hanson with the AD server:**

1. On a computer that has access to the AD, open the AD for Users and Computers.

2. Select the user Jamie Hanson.

3. Click the **General** tab. The general properties for Jamie Hanson display.
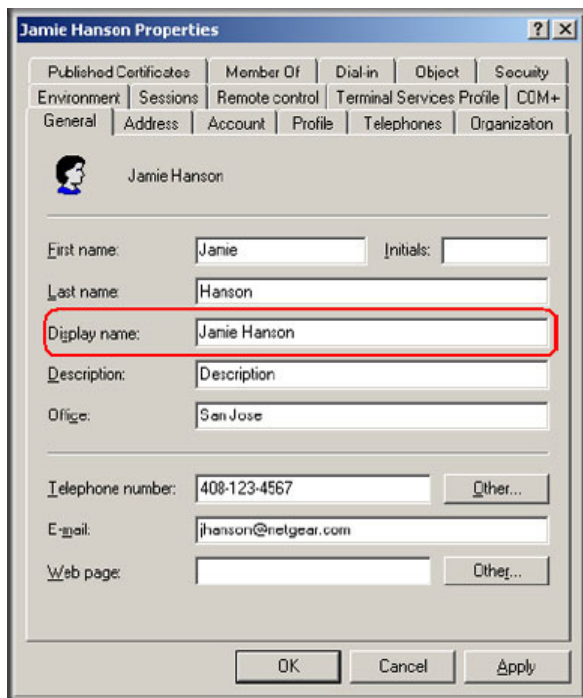
Figure 211.

4. To verify Jamie Hanson's user login name, click the **Account** tab. The account properties for Jamie Hanson display.
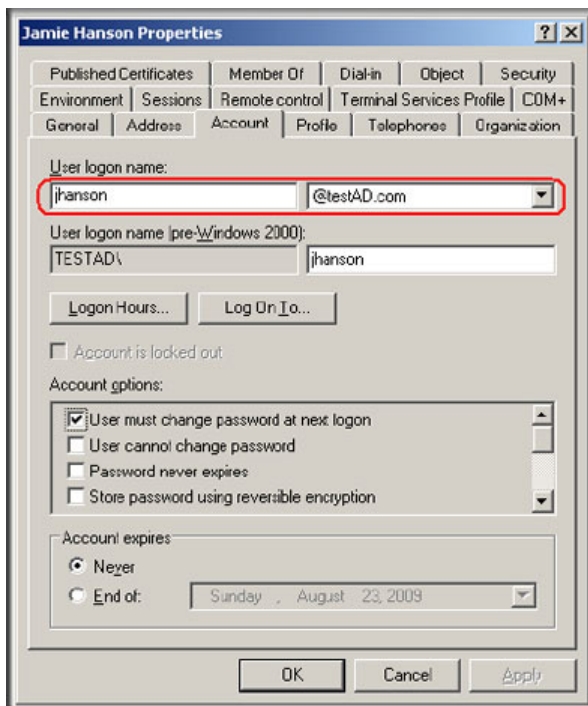
Figure 212.

5. Log in to the UTM.

6. Select **Users > Domains**.

7. Click **Add**. The Add Domain screen displays.

8. Enter **testAD.com** in the Domain Name field.

9. From the Authentication Type drop-down list, select **Active Directory**.

10. Select a previously configured portal from the Select Portal drop-down list.

11. Enter **192.168.35.115** in the Authentication Server field.

12. Enter the company information (for example, **dc=netgear,dc=com**) in the Active Directory Domain field.

13. To bind the user Jamie Hanson to the AD server for authentication on the UTM, use one of the following two formats in the Bind DN field of the Add Domain screen:

    - The display name in dn format:
      cn=Jamie Hanson,cn=users,dc=testAD,dc=com (see the following figure).

Figure 213.

- The Windows account name in email format such as jhanson@testAD.com. (The following figure shows only the Bind DN field.)

Figure 214.

14. Complete the remaining fields and drop-down list as needed.

15. Click **Apply** to save your settings.

Configure Domains

The domain determines the authentication method to be used for associated users. For SSL connections, the domain also determines the portal layout that is presented, which in turn determines the network resources to which the associated users have access. The default domain of the UTM is named geardomain. You cannot delete the default domain.

Create and Delete Domains

> **To create a domain:**

1. Select **Users > Domains**. The Domains screen displays. (The following figure shows the UTM's default domain—geardomain—and, as an example, other domains in the List of Domains table.)
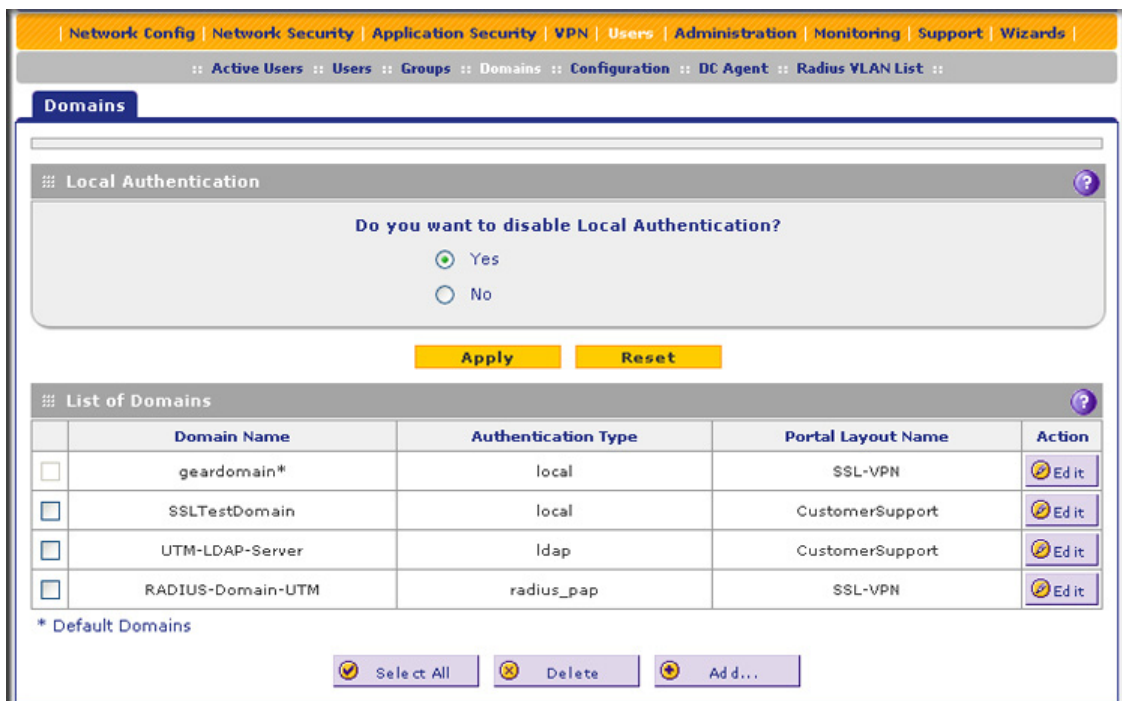
Figure 215.

The List of Domains table displays the domains with the following fields:

- **Check box**. Allows you to select the domain in the table.
- **Domain Name**. The name of the domain. The default domain name (geardomain) is appended by an asterisk.
- **Authentication Type**. The authentication method that is assigned to the domain.
- **Portal Layout Name**. The SSL portal layout that is assigned to the domain.
- **Action**. The Edit table button, which provides access to the Edit Domain screen.

2. Under the List of Domains table, click the **Add** table button. The Add Domain screen displays:
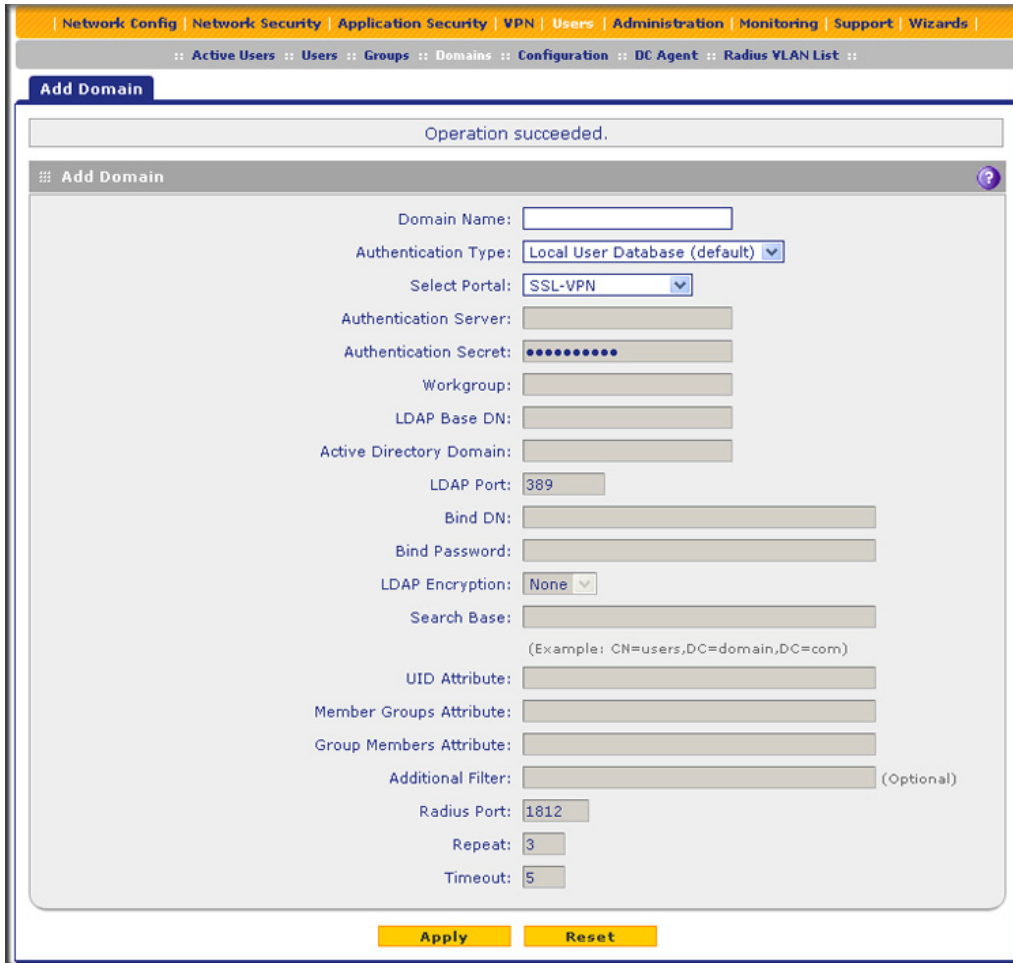
Figure 216.

3. Enter the settings as explained in the following table:

Table 91. Add Domain screen settings

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.

Authentication Type	From the drop-down list, select the authentication method that the UTM applies:
	• **Local User Database (default)**. Users are authenticated locally on the UTM. This is the default setting. You do not need to complete any other fields on this screen.
	• **Radius-PAP**. RADIUS Password Authentication Protocol (PAP). Complete the following fields:
	    - Authentication Server
	    - Authentication Secret
	    - Radius Port
	    - Repeat
	    - Timeout

Table 91. Add Domain screen settings (continued)

Setting	Description

Authentication Type (continued)
 	
Note: If you select any type of RADIUS authentication, make sure that one or more RADIUS servers are configured (see *RADIUS Client Configuration* on page 279).
	• **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the following fields:
	    - Authentication Server
	    - Authentication Secret
	    - Radius Port
	    - Repeat
	    - Timeout
	• **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the following fields:
	    - Authentication Server
	    - Authentication Secret
	• **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the following fields:
	    - Authentication Server
	    - Authentication Secret
	• **WIKID-PAP**. WiKID Systems PAP. Complete the following fields:
	    - Authentication Server
	    - Authentication Secret
	    - Radius Port
	    - Repeat
	    - Timeout
	• **WIKID-CHAP**. WiKID Systems CHAP. Complete the following fields:
	    - Authentication Server
	    - Authentication Secret
	    - Radius Port
	    - Repeat
	    - Timeout
	• **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the following fields:
	    - Authentication Server
	    - Authentication Secret
	    - Radius Port
	    - Repeat
	    - Timeout
	• **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the following fields:
	    - Authentication Server
	    - Authentication Secret
	    - Radius Port
	    - Repeat
	    - Timeout

Table 91. Add Domain screen settings (continued)

Setting	Description

Authentication Type (continued)	• **NT Domain**. Microsoft Windows NT Domain. Complete the following fields:
	   - Authentication Server
	   - Workgroup
	• **Active Directory**. Microsoft Active Directory. Complete the following fields, and make a selection from the LDAP Encryption drop-down list:
	   - Authentication Server
	   - Active Directory Domain
	   - LDAP Port
	   - Bind DN
	   - Bind Password
	   - Search Base
	   - Additional Filter (optional)
	• **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the following fields, and make a selection from the LDAP Encryption drop-down list:
	   - Authentication Server
	   - LDAP Base DN
	   - LDAP Port
	   - Bind DN
	   - Bind Password
	   - Search Base
	   - UID Attribute
	   - Member Groups Attribute (optional)
	   - Group Members Attribute (optional)
	   - Additional Filter (optional)

Portal	The portal that you selected on the first SSL VPN Wizard screen. You cannot change the portal on this screen; the portal is displayed for information only.
Authentication Server	The server IP address or server name of the authentication server for any type of authentication other than authentication through the local user database.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WiKID, or MIAS authentication.
Workgroup	The workgroup that is required for Microsoft NT Domain authentication.
LDAP Base DN	The LDAP base distinguished name (DN) that is required for LDAP authentication.
Active Directory Domain	The Active Directory domain name that is required for Microsoft Active Directory authentication.
LDAP Port	The port number for the LDAP or Active Directory authentication server. The default port for the LDAP server is 389, which is generally the default port for TLS encryption or no encryption. When the encryption is SSL, the default port is generally 636.

Table 91. Add Domain screen settings (continued)

Setting	Description

Bind DN	The LDAP or Active Directory DN that is required to access the LDAP or Active Directory authentication server. This should be a user in the LDAP or Active Directory directory who has read access to all the users that you would like to import into the UTM. The Bind DN field accepts two formats:
	• **A display name in the DN format**. For example:
	  cn=Jamie Hanson,cn=users,dc=test,dc=com.
	• **A Windows login account name in email format**. For example:
	  jhanson@testAD.com. This last type of bind DN can be used only for a Windows Active Directory server.

Bind Password	The authentication secret or password that is required to access the LDAP or Active Directory authentication server.
LDAP Encryption	From the drop-down list, select the encryption type for the connection between the UTM and the LDAP or Active Directory server: • **None**. The connection is not encrypted. This is the default setting. • **TLS**. The connection uses Transport Layer Security (TLS) encryption. • **SSL**. The connection uses Secure Socket Layer (SSL) encryption.
Search Base	The DN at which to start the search, specified as a sequence of relative distinguished names (RDNs), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany.com, your search base DN might be as follows: dc=yourcompany,dc=com.
UID Attribute	The attribute in the LDAP directory that contains the user's identifier (UID). For an Active Directory, enter **sAMAccountName**. For an OpenLDAP directory, enter **uid**.
Member Groups Attribute	This field is optional. The attribute that is used to identify the groups an entry belongs to. For an Active Directory, enter **memberOf**. For OpenLDAP, you can enter a customized attribute to identify the groups of an entry.
Group Members Attribute	This field is optional. The attribute that is used to identify the members of a group. For an Active Directory, enter **member**. For OpenLDAP, you can enter a customized attribute to identify the members of a group.
Additional Filter	This field is optional. A filter that is used when the UTM is searching the LDAP server for matching entries while excluding others. (Use the format described by RFC 2254.) The following search term examples match users only: Active Directory. objectClass=user Open LDAP. objectClass=posixAccount
Radius Port	The port number for the RADIUS server. The default port number is 1812.

Table 91. Add Domain screen settings (continued)

Setting	Description
Repeat	The period in seconds that the UTM waits for a response from a RADIUS server.
Timeout	The maximum number of times that the UTM attempts to connect to a RADIUS server.

4. Click **Apply** to save your settings. The domain is added to the List of Domains table.

5. If you use local authentication, make sure that it is not disabled: in the Local Authentication section of the Domain screen (see *Figure 215* on page 353), select the **No** radio button.

> **Note:** A combination of local and external authentication is supported.

⚠ **WARNING!**

If you disable local authentication, make sure that there is at least one external administrative user; otherwise, access to the UTM is blocked.

6. If you change local authentication, click **Apply** in the Domain screen to save your settings.

➢ **To delete one or more domains:**

1. In the List of Domains table, select the check box to the left of each domain that you want to delete, or click the **Select All** table button to select all domains. You cannot delete a default domain.

2. Click the **Delete** table button.

Edit Domains

➢ **To edit a domain:**

1. Select **Users > Domains**. The Domains screen displays (see *Figure 215* on page 353).

2. In the Action column of the List of Domains table, click the **Edit** table button for the domain that you want to edit. The Edit Domains screen displays. This screen is very similar to the Add Domains screen (see the previous figure).

3. Modify the settings as explained in the previous table. (You cannot modify the Domain Name and Authentication Type fields.)

4. Click **Apply** to save your changes. The modified domain is displayed in the List of Domains table.

Configure Groups

The use of groups simplifies the configuration of VPN policies when different sets of users have different restrictions and access controls. It also simplifies the configuration of web access exception rules. Like the default domain of the UTM, the default group is also named geardomain. The default group geardomain is assigned to the default domain geardomain. You cannot delete the default domain geardomain, nor its associated default group geardomain.

When you create a new domain, for example, on the second SSL VPN Wizard screen (see *SSL VPN Wizard Step 2 of 6 (Domain Settings)* on page 310), a default group with the same name as the new domain is created automatically. You cannot delete this default group either. However, when you delete the domain with which it is associated, the default group is deleted automatically.

> **Note:** IPSec VPN users always belong to the default domain (geardomain) and are not assigned to groups.

> **Note:** Groups that are defined on the Groups screen are used for setting SSL VPN policies. These groups should not be confused with LAN groups that are defined on the LAN Groups screen and that are used to simplify firewall policies. For information about LAN groups, see *Manage Groups and Hosts (LAN Groups)* on page 106.

Create and Delete Groups

> **To create a VPN group:**

1. Select **Users > Groups**. The Groups screen displays. (The following figure shows the UTM's default group—geardomain—and, as an example, several other groups in the List of Groups table.)

   The List of Groups table displays the VPN groups with the following fields:

   - **Check box**. Allows you to select the group in the table.
   - **Name**. The name of the group. If the group name is appended by an asterisk, the group was created by default when you created the domain with the identical name as the default group. You cannot delete a default group; you can delete only the domain with the identical name, which causes the default group to be deleted.
   - **Domain**. The name of the domain to which the group is assigned.
   - **Action**. The Edit table button, which provides access to the Edit Group screen.
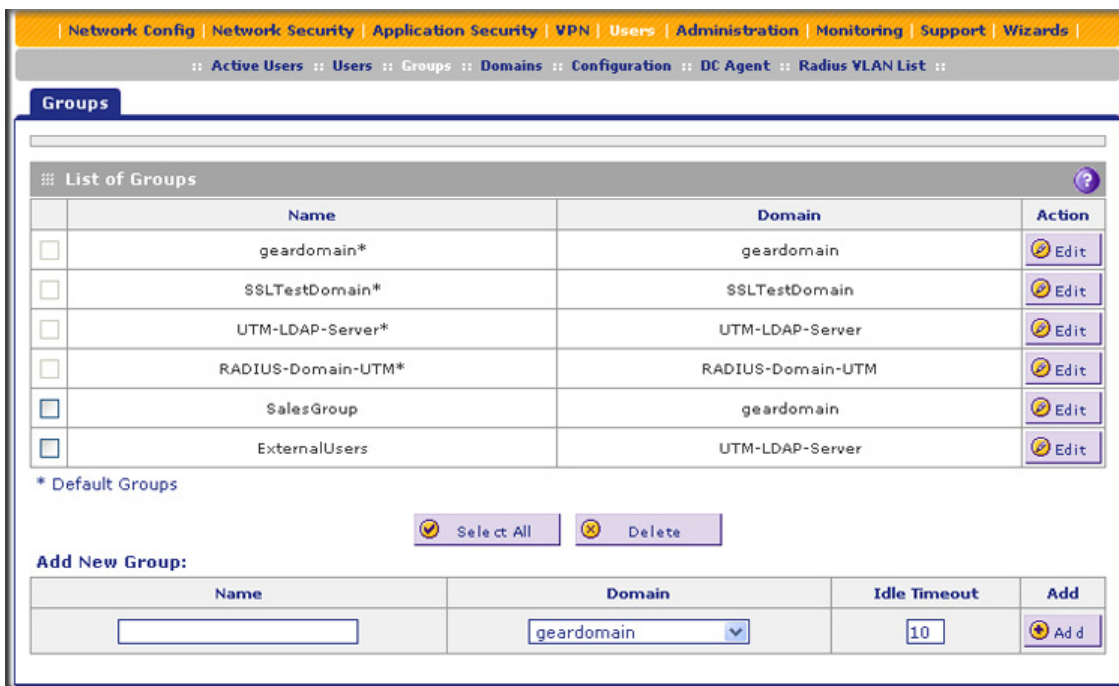
Figure 217.

2. In the Add New Group section of the screen, enter the settings as explained in the following table:

Table 92. Groups screen settings

Setting	Description
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.
Domain	The drop-down list shows the domains that are listed on the Domain screen. From the drop-down list, select the domain with which the group is associated. For information about how to configure domains, see *Configure Domains* on page 353.
Idle Timeout	The period after which an idle user is automatically logged out of the UTM's web management interface. The default idle time-out period is 5 minutes.

3. Click the **Add** table button. The new group is added to the List of Groups table.

➢ **To delete one or more groups:**

1. In the List of Groups table, select the check box to the left of each group that you want to delete, or click the **Select All** table button to select all groups.

2. Click the **Delete** table button.

Note: You cannot delete a default group such as one that was automatically created when you specified a new domain on the second SSL VPN Wizard screen (see *SSL VPN Wizard Step 2 of 6 (Domain Settings)* on page 310). You can delete only the domain with which the default group is associated and that has an identical name as the default group (see *Configure Domains* on page 353). Deleting the domain causes the default group to be removed.

Edit Groups

➢ **To edit a VPN group:**

1. Select **Users > Groups**. The Groups screen displays (see the previous figure).

2. In the Action column of the List of Groups table, click the **Edit** table button for the group that you want to edit. The Edit Groups screen displays:

Figure 218.

With the exception of groups that are associated with domains that use the LDAP authentication method, you can modify only the idle time-out settings. You can never modify the Group Name and Group's Auth Type fields.

3. Modify the idle time-out period in minutes in the Idle Timeout field. For a group that is associated with a domain that uses the LDAP authentication method, configure the LDAP attributes (in fields 1 through 4) as needed.

4. Click **Apply** to save your changes. The modified group is displayed in the List of Groups table.

Configure User Accounts

The UTM supports both unauthenticated and authenticated users:

- **Unauthenticated users**. Anonymous users who do not log in to the UTM and to which the UTM's default email and web access policies apply.

- **Authenticated users**. Users who have a computer behind the UTM, who log in to the UTM with a user name and password, and who are assigned an access policy that usually differs from the UTM's default email and web access policies. Different users or user groups can have different access policies, so there can be multiple access policies on the UTM.

  In addition to being authenticated as individual users, users can be authenticated on the UTM according to group membership or IP address:

  - Group membership. A group is defined in the UTM's local database, an LDAP database, or a RADIUS database. If you use a RADIUS database for authentication, a group can also be defined in a VLAN.

  - IP address. A group is defined by its IP address and subnet.

When you create a user account, you need to assign the user to a user group. When you create a group, you need to assign the group to a domain that specifies the authentication method. Therefore, you should first create any domains, then groups, and then user accounts.

You can create different types of user accounts by applying pre-defined user types:

- **Administrator**. A user who has full access and the capacity to change the UTM configuration (that is, read/write access).

- **SSL VPN User**. A user who can log in only to the SSL VPN portal.

- **IPSEC VPN User**. A user who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 277).

- **Guest user**. A user who can only view the UTM configuration (that is, read-only access).

- **PPTP VPN User**. A user who can make a connection to the PPTP server only.

- **L2TP VPN User**. A user who can make a connection to the L2TP server only.

➢ **To create an individual user account:**

1. Select **Users > Users**. The Users screen displays. (The following figure shows the UTM's default users—admin and guest—and, as an example, several other users in the List of Users table.)
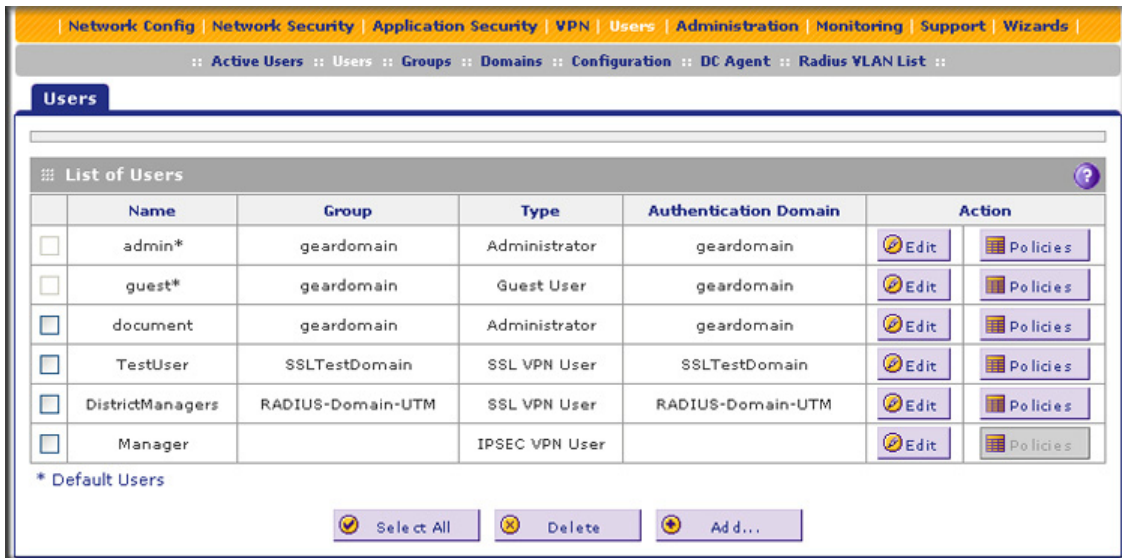
Figure 219.

The List of Users table displays the users and has the following fields:

- **Check box**. Allows you to select the user in the table.
- **Name**. The name of the user. If the user name is appended by an asterisk, the user is a default user that came preconfigured with the UTM and cannot be deleted.
- **Group**. The group to which the user is assigned.
- **Type**. The type of access credentials that are assigned to the user.
- **Authentication Domain**. The authentication domain to which the user is assigned.
- **Action**. The Edit table button, which provides access to the Edit User screen; the Policies table button, which provides access to the policy screens.

2. Click the **Add** table button. The Add User screen displays:
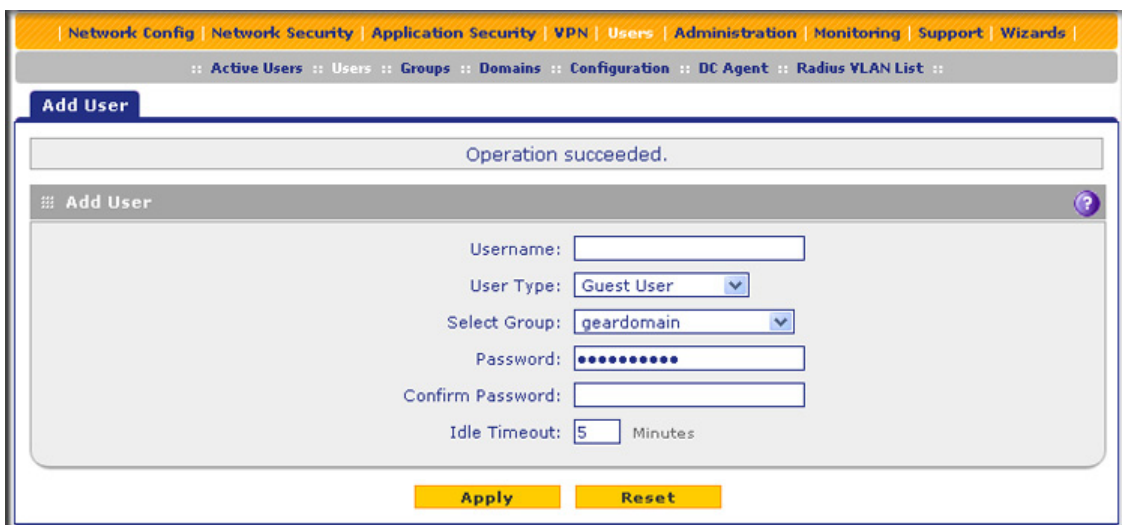
Figure 220.

3. Enter the settings as explained in the following table:

Table 93. Add User screen settings

Setting	Description
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	From the drop-down list, select one of the predefined user types that determines the access credentials: • **Administrator**. User who has full access and the capacity to change the UTM configuration (that is, read/write access). • **SSL VPN User**. User who can log in only to the SSL VPN portal. • **IPSEC VPN User**. User who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 277). • **Guest User**. User who can only view the UTM configuration (that is, read-only access). • **PPTP VPN User**. A user who can make a connection to the PPTP server only. • **L2TP VPN User**. A user who can make a connection to the L2TP server only.
Select Group	The drop-down list shows the groups that are listed on the Group screen. From the drop-down list, select the group to which the user is assigned. For information about how to configure groups, see *Configure Groups* on page 359. **Note:** The user is assigned to the domain that is associated with the selected group.
Password	The password that the user needs to enter to gain access to the UTM. The password needs to contain alphanumeric, hyphen (-), or underscore (_) characters.
Confirm Password	This field needs to be identical to the password that you entered in the Password field.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes. **Note:** The idle time-out is not applicable to PPTP and L2TP users because the user time-out is already specified on the PPTP Server screen (see *Configure the PPTP Server (UTM9S Only)* on page 300) and L2TP Server screen (see *Configure the L2TP Server (UTM9S Only)* on page 303).

4. Click **Apply** to save your settings. The user is added to the List of Users table.

➢ **To delete one or more user accounts:**

1. In the List of Users table, select the check box to the left of each user account that you want to delete, or click the **Select All** table button to select all accounts. You cannot delete a default user account.

2. Click the **Delete** table button.

Note: You cannot delete the default admin or guest user.

Set User Login Policies

You can restrict the ability of defined users to log in to the UTM's web management interface. You can also require or prohibit logging in from certain IP addresses or from particular browsers.

> **Note:** User logon policies are not applicable to PPTP and L2TP users.

Configure Login Policies

> **To configure user login policies:**

1. Select **Users > Users**. The Users screen displays (see *Figure 219* on page 363).

2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view:
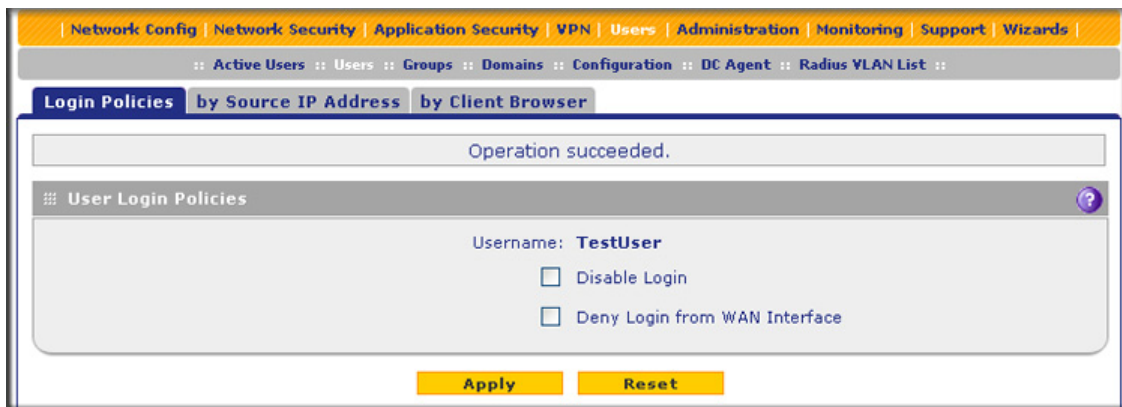
Figure 221.

3. In the User Login Policies section of the screen, make the following selections:

   • To prohibit this user from logging in to the UTM, select the **Disable Login** check box.

   • To prohibit this user from logging in from the WAN interface, select the **Deny Login from WAN Interface** check box. In this case, the user can log in only from the LAN interface.

> **Note:** For security reasons, the Deny Login from WAN Interface check box is selected by default for guests and administrators. The Disable Login check box is disabled (masked out) for administrators.

4. Click **Apply** to save your settings.

Configure Login Restrictions Based on IP Address

➢ **To restrict logging in based on IP address:**

1. Select **Users > Users**. The Users screen displays (see *Figure 219* on page 363).

2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view.

3. Click the **By Source IP Address** submenu tab. The By Source IP Address screen displays. (The following figure shows an IP address in the Defined Addresses table as an example.)
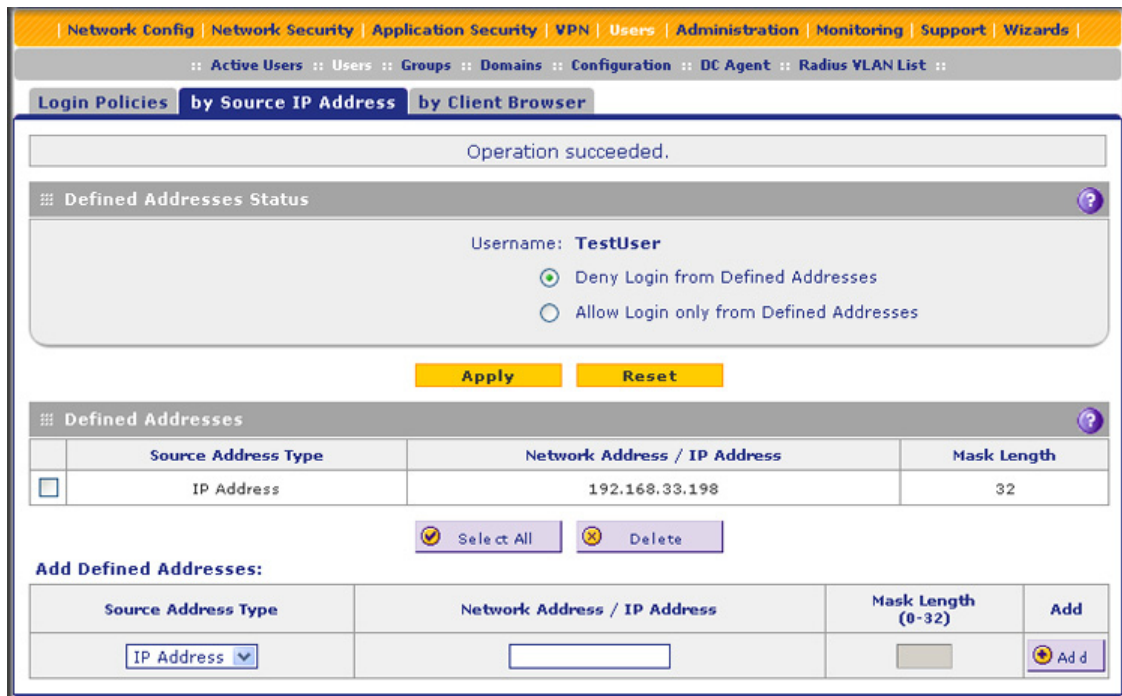
Figure 222.

4. In the Defined Addresses Status section of the screen, select one of the following radio buttons:

   • **Deny Login from Defined Addresses**. Deny logging in from the IP addresses in the Defined Addresses table.

   • **Allow Login only from Defined Addresses**. Allow logging in from the IP addresses in the Defined Addresses table.

5. Click **Apply** to save your settings.

6. In the Add Defined Addresses section of the screen, add an address to the Defined Addresses table by entering the settings as explained in the following table:

Table 94. By Source IP Address screen settings

Setting	Description
Source Address Type	Select the type of address from the drop-down list: • **IP Address**. A single IP address. • **IP Network**. A subnet of IP addresses. You need to enter a netmask length in the Mask Length field.
Network Address / IP Address	Depending on your selection from the Source Address Type drop-down list, enter the IP address or the network address.
Mask Length	For a network address, enter the netmask length (0–32). **Note:** By default, a single IP address is assigned a netmask length of 32.

7. Click the **Add** table button. The address is added to the Defined Addresses table.

8. Repeat *step 6* and *step 7* for any other addresses that you want to add to the Defined Addresses table.

➢ **To delete one or more addresses:**

1. In the Defined Addresses table, select the check box to the left of each address that you want to delete, or click the **Select All** table button to select all addresses.

2. Click the **Delete** table button.

Configure Login Restrictions Based on Web Browser

➢ **To restrict logging in based on the user's browser:**

1. Select **Users > Users**. The Users screen displays (see *Figure 219* on page 363).

2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view.

3. Click the **By Client Browser** submenu tab. The By Client Browser screen displays. (The following figure shows a browser in the Defined Browsers table as an example.)
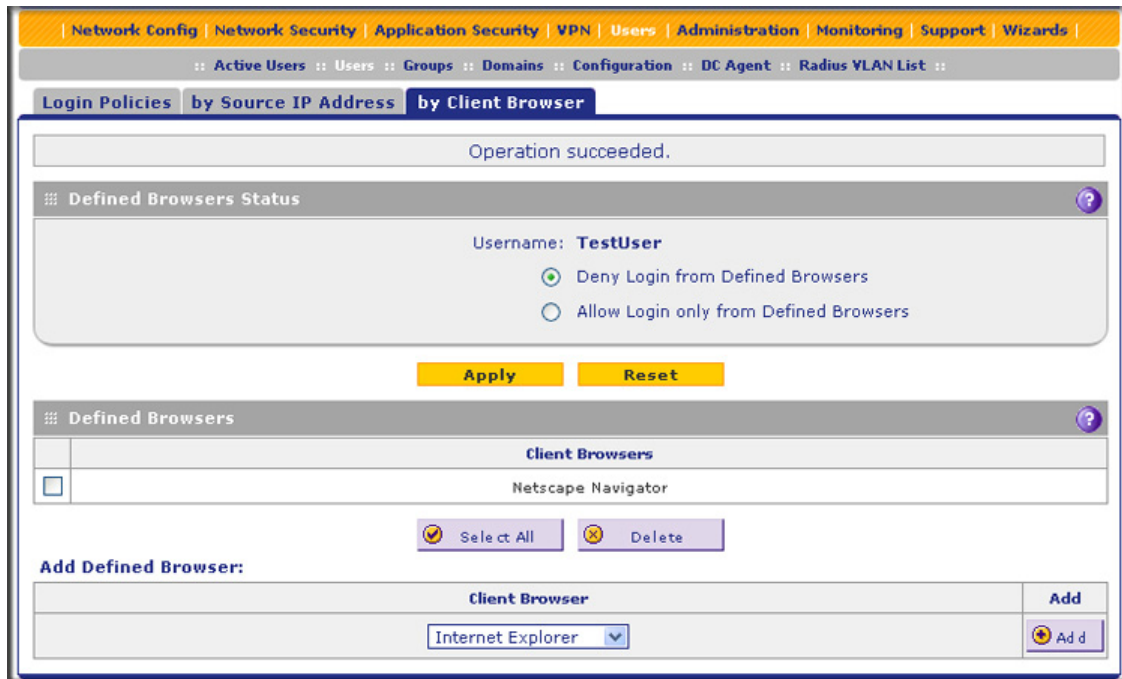
Figure 223.

4. In the Defined Browsers Status section of the screen, select one of the following radio buttons:
   - **Deny Login from Defined Browsers**. Deny logging in from the browsers in the Defined Browsers table.
   - **Allow Login only from Defined Browsers**. Allow logging in from the browsers in the Defined Browsers table.

5. Click **Apply** to save your settings.

6. In the Add Defined Browser section of the screen, add a browser to the Defined Browsers table by selecting one of the following browsers from the drop-down list:
   - **Internet Explorer**.
   - **Opera**.
   - **Netscape Navigator**.
   - **Firefox**. Mozilla Firefox.
   - **Mozilla**. Other Mozilla browsers.

7. Click the **Add** table button. The browser is added to the Defined Browsers table.

8. Repeat *step 6* and *step 7* for any other browsers that you want to add to the Defined Browsers table.

➢ **To delete one or more browsers:**

1. In the Defined Browsers table, select the check box to the left of each browser that you want to delete, or click the **Select All** table button to select all browsers.

2. Click the **Delete** table button.

Change Passwords and Other User Settings

For any user, you can change the password, user type, and idle time-out settings. Only administrators have read/write access. All other users have read-only access.

> **Note:** The default administrator and default guest passwords for the web management interface are both password. NETGEAR recommends that you change the password for the administrator account to a more secure password, and that you configure a separate secure password for the guest account.

> **Note:** The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

> **Note:** After a factory defaults reset, the password and time-out value are changed back to password and 5 minutes, respectively.

> **To modify user settings, including passwords:**

1. Select **Users > Users**. The Users screen displays (see *Figure 219* on page 363).

2. In the Action column of the List of Users table, click the **Edit** table button for the user for which you want to modify the settings. The Edit User screen displays:

Figure 224.

3. Modify the settings as explained in the following table:

Table 95. Edit User screen settings

Setting	Description	
Select User Type	From the drop-down list, select one of the predefined user types that determines the access credentials: • **Administrator**. User who has full access and the capacity to change the UTM configuration (that is, read/write access). • **SSL VPN User**. User who can log in only to the SSL VPN portal. • **IPSEC VPN User**. User who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 277). • **Guest User**. User who can only view the UTM configuration (that is, read-only access). • **PPTP VPN User**. A user who can make a connection to the PPTP server only. • **L2TP VPN User**. A user who can make a connection to the L2TP server only.	
Check to Edit Password	Select this check box to make the password fields accessible to modify the password.	
	Enter Your Password	Enter the old password.
	New Password	Enter the new password.
	Confirm New Password	Reenter the new password for confirmation.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes. **Note:** The idle time-out is not applicable to PPTP and L2TP users because the user time-out is already specified on the PPTP Server screen (see *Configure the PPTP Server (UTM9S Only)* on page 300) and L2TP Server screen (see *Configure the L2TP Server (UTM9S Only)* on page 303).	

4. Click **Apply** to save your settings.

DC Agent

If you set up an open network, you would want to allow unauthenticated users to surf anonymously. For a secure network, you would use a more restrictive access policy for unauthenticated users and a less restricted access policy for authenticated users.

Without the use of the DC agent, any Active Directory (AD) domain user surfs anonymously until providing credentials to the UTM in order to proceed past a blocked web activity. With use of the DC agent, an AD domain user is immediately known to the UTM when he or she is authenticated on a DC server on which the DC agent is installed, allowing a single sign-on (SSO).

If the AD authenticates through a domain controller (DC) server that runs Windows Server 2003 with Service Pack 1 (SP1) or Windows Server 2008, you can use the ProSecure DC Agent software to authenticate AD domain users.

> **Note:** The DC agent does not function with LDAP domain users.

The DC agent monitors all Windows login events (that is, all AD domain user authentications) on the DC server, and provides a mapping of Windows user names and IP addresses to the UTM, enabling the UTM to transparently apply user policies. The DC agent transfers encrypted names, IP addresses, groups, and login times of the users logged in to the UTM, where this information remains securely (that is, it is not transferred out of the UTM).

Requirements for the ProSecure DC Agent Software and DC Agent Server

Note the following requirements for the ProSecure DC agent software and domain controller (DC) servers:

- If the DC server is located behind a firewall or there is a firewall on the DC server, ensure that the firewall does not block the server's listening port. The default port that is used by the DC agent is 5182.

- The DC agent needs to be able to automatically log an account login event when a domain user account is authenticated against the Active Directory on a DC server.

  Verify that the DC server has the following configuration:

  - The Audit Logon Events policy is defined, and the Success check box is selected.
  - The Audit Account Logon Events policy is defined, and the Success check box is selected.
  - The Audit Account Management policy is defined, and the Success check box is selected.

  In addition, if you change the log path of the security log, restart the DC server to bring the change into effect.

- If you use the ProSecure DC Agent software on a DC server that is running Windows Server 2003, ensure that Window's Security Log settings in the Event Viewer are set to the maximum size of 16 MB and to overwrite events as needed.

Download ProSecure DC Agent Software, and Create and Delete DC Agents

When new ProSecure DC Agent software is available, the UTM automatically downloads the software from the update server and notifies administrative users in several ways:

- The UTM sends an email to administrative users.
- The UTM records a syslog entry.
- The UTM generates a notification screen that is presented to administrative users upon login.

➢ **To download ProSecure DC Agent software and add a DC agent:**

1. Select **Users > DC Agent**. The DC Agent screen displays:
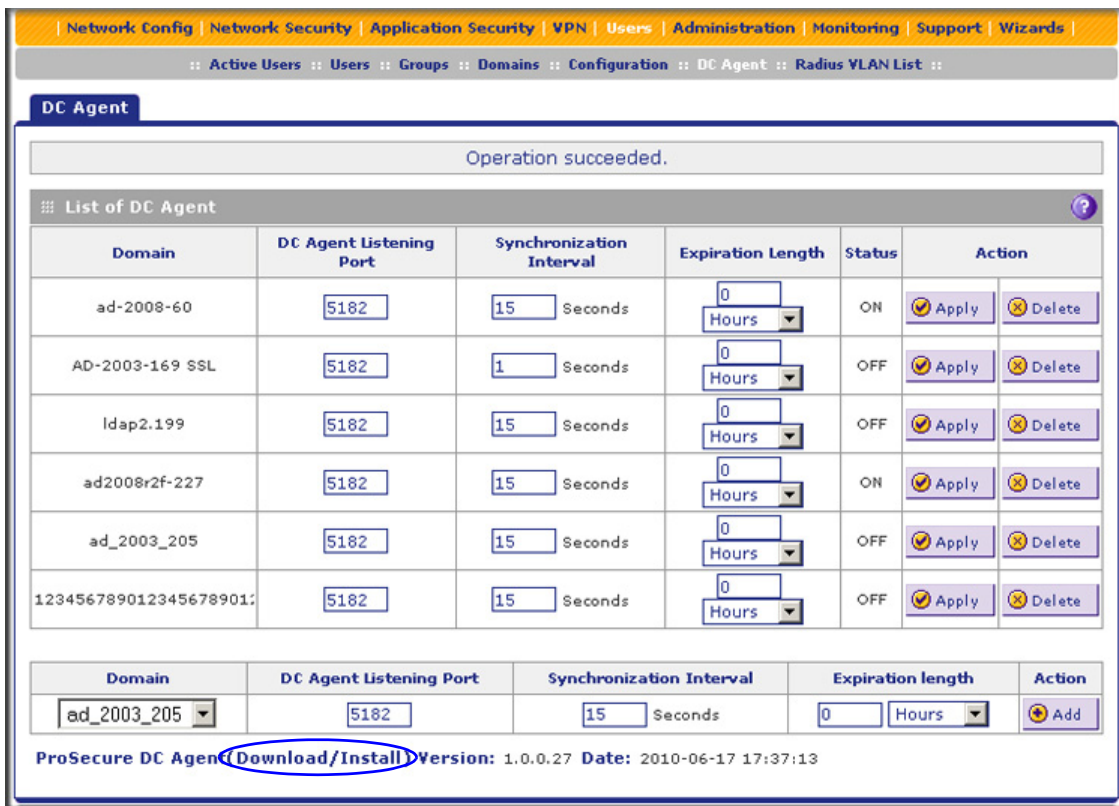
Figure 225.

2. Under the List of DC Agents table, click the **Download/Install** link to download the ProSecure DC Agent software (that is, the dc_agent.mis file). Follow the instructions of your browser to save the software file to your computer.

3. Install the ProSecure DC Agent software on each domain controller (DC) server through which the LDAP directory authenticates users. After installation, the ProSecure DC Agent control panel lets you configure and manage the DC agent. For more information, click the **Help** button on the control panel.
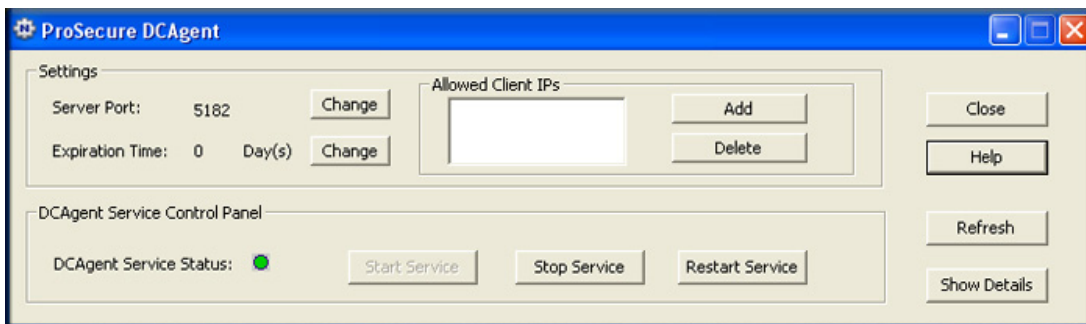
Figure 226.

4. On the DC Agent screen (see *Figure 225* on page 372), complete the fields and make your selections from the drop-down lists as explained in the following table:

Table 96. DC Agent screen settings

Setting	Description
Domain	From the Domain drop-down list, select an Active Directory (AD) domain to bind with the DC agent. For information about configuring AD domains, see *Configure Domains* on page 353.
DC Agent Listening Port	Enter the listening port of the DC agent. The listening port is the port through which the DC agent transfers the list of authenticated users to the UTM. The default port is 5182.
Synchronization Interval	Enter the time interval (in seconds) at which the DC agent updates the list of authenticated users. The default interval is 15 seconds.
Expiration length	Enter time interval in hours or minutes (determined by your selection from the Expiration length drop-down list) that is allowed to elapse before a user login expires. The default setting is 0 (zero), that is, a user login does not expire.
Status	Displays the status of the DC agent: ON indicates that the DC agent is active; OFF indicates that the DC agent is inactive.

5. To add the newly configured DC agent to the List of DC Agent(s) table, click the **Add** table button in the Action column.

The Status column displays ON when a DC agent is available and OFF when a DC agent is not available.

To delete a DC agent from the table, click its **Delete** button in the Action column.

➢ **To edit a DC agent:**

1. In the Domain column, locate the DC agent that you want to edit, and make changes in the columns to the right of the Domain column as explained in the previous table.

2. In the Action column, click the DC agent's **Apply** button to save your changes.

Example: Configure Active Directory Single Sign-On with a DC Agent

In the following example, you configure user authentication through Active Directory (AD) single sign-on (SSO) with the use of a DC agent on a UTM50:

- The domain name is Test_Domain.
- The IP address of the authentication server is 12.18.39.27.
- The AD domain is test_user.com.
- The IP address of the UTM50 is 90.49.145.18.

➢ **To configure AD SSO with a DC agent:**

1. Add a new domain on the UTM50:

   a. Select **Users > Domains**. The Domains screen displays.

b. Click the **Add** table button to add a new domain. The Add Domain screen displays:

Figure 227.

c. Enter the following settings:

- In the Domain Name field, enter **Test_Domain**.
- From the Authentication Type drop-down list, select **Active Directory**.
- From the Select Portal drop-down list, select a portal. (In this example, the default portal is SSL-VPN.)
- In the Authentication Server field, enter **12.18.39.27**.
- In the Active Directory Domain field, enter **test_user.com**.
- In the Bind DN field, enter a bind DN. (In this example, the bind DN is admin22@test_user.com.)
- In the Bind Password field, enter a password.
- In the Search Base field, enter **dc=test_user,dc=com**.

d. Click **Apply** to save your changes.

2. Add a new DC agent on the UTM50:

   a. Select **Users > DC Agent**. The DC Agent screen displays:
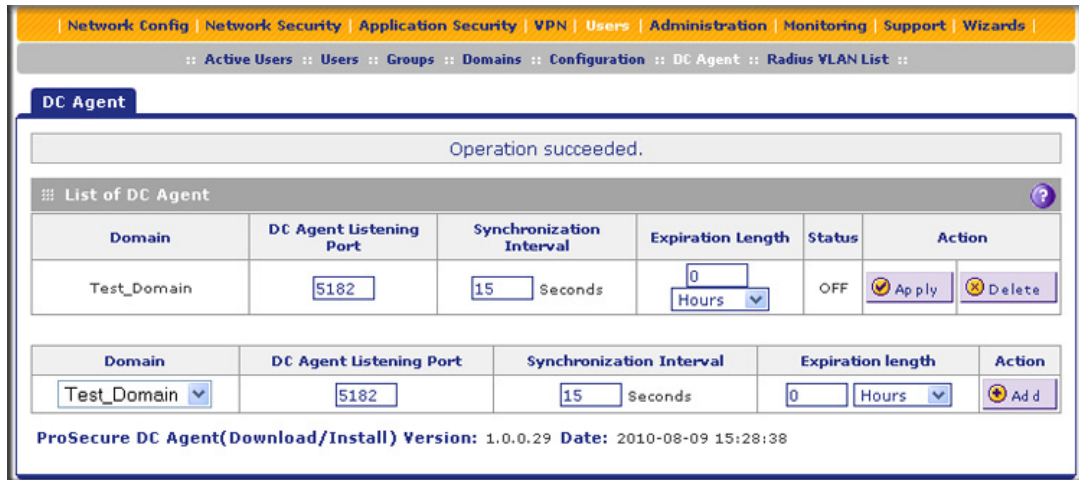
   Figure 228.

   b. In the Domain field, enter **Test_Domain**.

   c. In the Action column, click **Add**.

3. Add the IP address of the UTM50 on the ProSecure DC Agent control panel:

   a. Click **Add**.

   b. In the Add a client pop-up screen, enter **90.49.145.18**.

   c. Click **OK**. The IP address of the UTM50 displays in the Allowed Client IPs field:
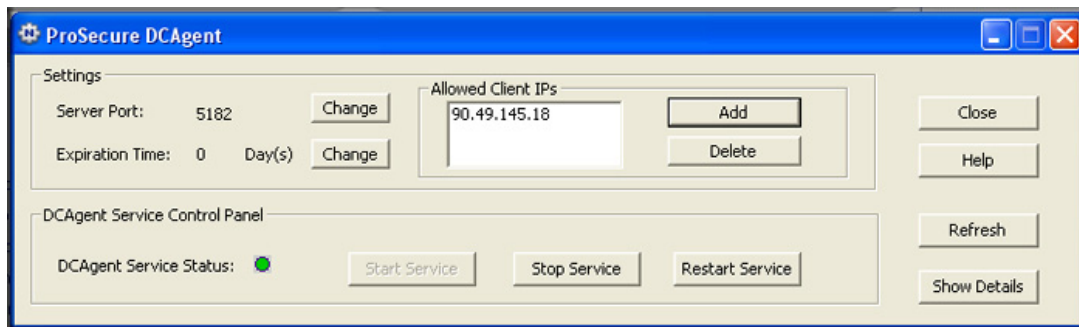
   Figure 229.

4. To verify that the UTM50 functions fine with the DC agent, search for active users that are logged in to the Test_Domain domain on the Active Users screen:

   a. Select **Users > Active Users**. The Active Users screen displays.

   b. Select the **Search Criteria** radio button.

   c. In the Domain field, enter **Test_Domain**.

   d. Click **Search**. If the users that are logged in to the Test_Domain domain display in the search results, the UTM50 functions fine with the DC agent. (For more information about active users, see *View and Log Out Active Users* on page 378.)

Configure RADIUS VLANs

You can use a RADIUS virtual LAN (VLAN) to set web access exceptions and provide an added layer of security.

➢ **To do so, follow this procedure:**

1. Specify a RADIUS server (see *RADIUS Client Configuration* on page 279).

2. Create a RADIUS domain (see *Configure Domains* on page 353).

3. Add a RADIUS virtual LAN (VLAN) (see the information in this section).

Note: The VLAN ID or name should be same as the VLAN ID or name that is configured on the RADIUS server.

---

4. Define web access exceptions for the users that are member of the RADIUS VLAN (see *Set Web Access Exception Rules* on page 221).

➢ **To configure a RADIUS VLAN:**

1. Select **Users > Radius VLAN List**. The List of VLAN screen displays. (The following figure contains one VLAN as an example.)
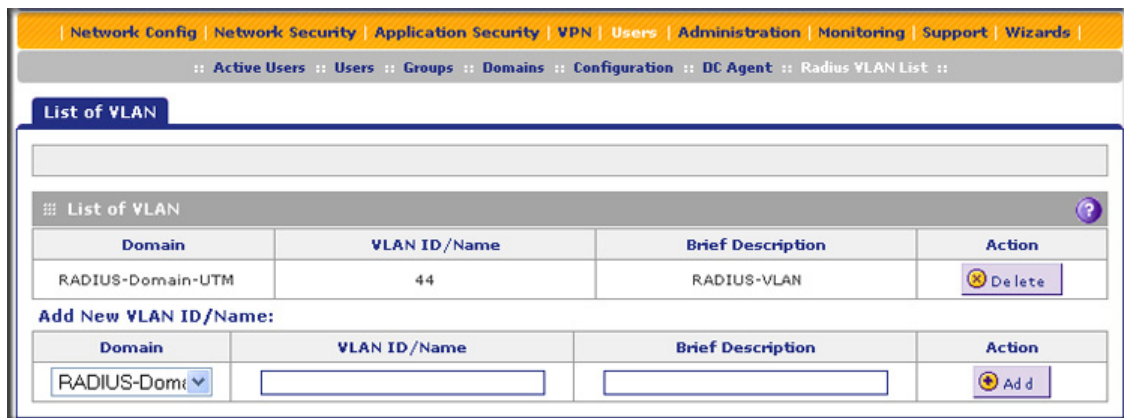
Figure 230.

The List of VLAN table displays the following fields:

- **Domain**. The RADIUS domain.
- **VLAN ID/Name**. The identifier or name for the VLAN.
- **Brief Description**. An optional brief description of the VLAN.
- **Action**. The Delete table button, which allows you to delete the VLAN.

2. Add a VLAN by specifying the VLAN in the Add New VLAN ID/Name section of the screen:

   a. Select a RADIUS VLAN from the Domain drop-down list.

   b. In the VLAN ID/Name field, enter the identifier or the name of the VLAN.

   c. In the Brief Description field, enter a description of the VLAN. This field is optional.

3. Click the **Add** table button. The new VLAN is added to the List of VLAN table.

To delete a user from the List of VLAN table, click the **Delete** table button in the Action column for the VLAN that you want to delete.

Configure Global User Settings

You can globally set the user session settings for authenticated users. These settings include the session expiration period, the allowed session idle time, and the default domain that is presented to the users.

1. To specify the global user configuration settings:

1. Select **Users > Configuration**. The Configuration screen displays:

Figure 231.

2. Locate the Session Parameters section on screen. Specify the session settings:

- **Session Expiration Length**. The period after which a session expires and a user needs to log in again. This setting applies to all users. From the drop-down list, select either **Minutes** or **Hours**. Then, in the field to the left of the drop-down list, enter a number for the minutes or hours. The session expiration length cannot exceed the idle time period. By default, the session expiration length is 24 hours.

   Note: *For information about how to set the time-out period for the web management interface, see* Change Passwords and Administrator and Guest Settings *on page 397.*

- **Idle Time**. The period after which an idle connection is terminated and a user needs to log in again. This setting applies to all users. From the drop-down list, select either **Minutes** or **Hours**. Then, in the field to the left of the drop-down list, enter a number

for the minutes or hours. The idle time period cannot exceed the session expiration length. By default, the idle time period is 8 hours.

3. Click **Apply** to save the session settings.

4. Locate the Users Portal Login Settings section on screen. Specify the default domain settings:

   - From the Default Domain drop-down list, select a domain that you previously configured on the Domain screen (see *Configure Domains* on page 353). This domain is presented on the User Portal Login screen (see *Figure 209* on page 347). By default, the domain that is presented is geardomain.

   - Select the **Authenticate User with User Selected Domain** check box to limit the authentication on the User Portal Login screen to the domain that you select from the Default Domain drop-down list. If you do not select this check box, the UTM attempts to authenticate users through all the domains that are listed in the drop-down list on the User Portal Login screen. When authentication through one domain fails, the UTM attempts authentication through another domain.

5. Click **Apply** to save the default domain settings.

View and Log Out Active Users

A user with administrative privileges can view the active users and log out selected or all active users.

➢ **To log out all active users:**

1. Select **Users > Active Users**. The Active Users screen displays:
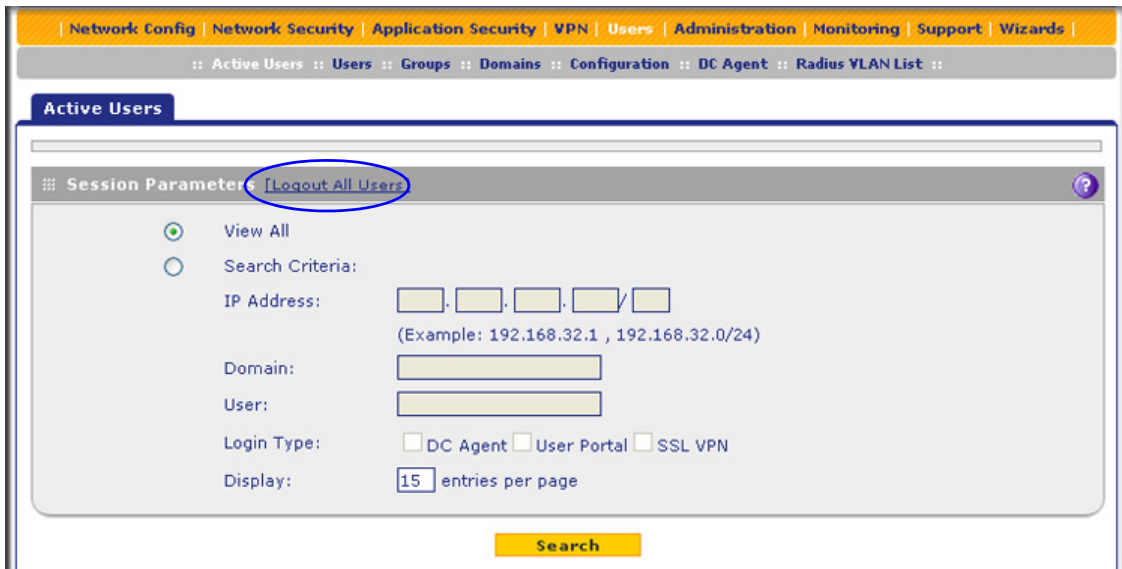
Figure 232.

2. Click the **Logout All Users** button in the gray settings bar at the top of the Active Users screen.

➢ **To view all or selected users:**

1. On the Active Users screen (see the previous figure), select one of the following radio buttons:

    • **View All**. This selection returns all active users after you click the Search button.

    • **Search Criteria**. Enter one or more search criteria as explained in the following table:

    Table 97. Active Users screen settings

Setting	Description
IP Address	Enter an IP address or an IP address and subnet mask in Classless Inter-Domain Routing (CIDR) notation (for example, /024).
Domain	Enter a domain (for example, geardomain).
User	Enter a user name (for example, JackP). If you do not enter a user name, all users of a specified domain are displayed in the search results.
Login Type	Select one or more of the following check boxes: • **DC Agent**. Display only users who logged in through the DC agent. • **User Portal**. Display only users who logged in through a user portal. • **SSL VPN**. Display only users who logged in through an SSL VPN connection.

2. In the Display field, enter a number to specify how many entries per page the search result screen returns.

3. Click **Search**. The search results screen displays. (The following figure contains many examples.)

Figure 233.

The List of Users table displays the following fields:

- **IP Address**. The IP address that is associated with the user.
- **Domain**. The domain to which the user belongs.
- **User**. The user name.
- **Groups**. The groups to which the user belongs, if any.
- **Last Seen**. The most recent time that scanned traffic associated with the user (that is, IP address) passed through the UTM.
- **Login Type**. The method through which the user logged in (DC agent, user portal, or SSL VPN).

➢ **To log out selected active users or all active users that your search yielded:**

1. On the search results screen select the check boxes to the left of the users that you want to log out, or select the check box at the upper left in the List of Users table.
2. Click **Logout**.
3. Click **Return**.

Manage Digital Certificates for VPN Connections

Note: For information about digital certificates for HTTPS scans, see *Manage Digital Certificates for HTTPS Scans* on page 213.

The UTM uses digital certificates (also known as X509 certificates) during the Internet Key Exchange (IKE) authentication phase to authenticate connecting IPSec VPN gateways or clients, or to be authenticated by remote entities. The same digital certificates are extended for secure web access connections over HTTPS (that is, SSL connections).

Digital certificates either can be self-signed or can be issued by certification authorities (CAs) such as an internal Windows server or an external organization such as Verisign or Thawte.

However, if the digital certificate contains the extKeyUsage extension, the certificate needs to be used for one of the purposes defined by the extension. For example, if the digital certificate contains the extKeyUsage extension that is defined for SNMPv2, the same certificate cannot be used for secure web management. The extKeyUsage would govern the certificate acceptance criteria on the UTM when the same digital certificate is being used for secure web management.

On the UTM, the uploaded digital certificate is checked for validity and purpose. The digital certificate is accepted when it passes the validity test and the purpose matches its use. The check for the purpose needs to correspond to its use for IPSec VPN, SSL VPN, or both. If the defined purpose is for IPSec VPN and SSL VPN, the digital certificate is uploaded to both the IPSec VPN certificate repository and the SSL VPN certificate repository. However, if the defined purpose is for IPSec VPN only, the certificate is uploaded only to the IPSec VPN certificate repository.

The UTM uses digital certificates to authenticate connecting VPN gateways or clients, and to be authenticated by remote entities. A digital certificate that authenticates a server, for example, is a file that contains the following elements:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

You can obtain a digital certificate from a well-known commercial certification authority (CA) such as Verisign or Thawte, or you can generate and sign your own digital certificate. Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity. A self-signed certificate triggers a warning from most browsers because it provides no protection against identity theft of the server.

The UTM contains a self-signed certificate from NETGEAR. This certificate can be downloaded from the UTM login screen for browser import. However, NETGEAR recommends that you replace this digital certificate with a digital certificate from a well-known commercial CA prior to deploying the UTM in your network.

VPN Certificates Screen

To display the Certificates screen, select **VPN > Certificates**. Because of the large size of this screen, and because of the way the information is presented, the Certificates screen is divided and presented in this manual in three figures (*Figure 234* on page 383, *Figure 236* on page 385, and *Figure 238* on page 388).

The Certificates screen lets you to view the currently loaded digital certificates, upload a new digital certificate, and generate a certificate signing request (CSR). The UTM typically holds two types of digital certificates:

- CA certificates. Each CA issues its own digital certificate to validate communication with the CA and to verify the validity of digital certificates that are signed by the CA.

- Self-signed certificates. The digital certificates that are issued to you by a CA to identify your device.

The Certificates screen contains four tables that are explained in detail in the following sections:

- **Trusted Certificates (CA Certificate) table**. Contains the trusted certificates that were issued by CAs and that you uploaded (see *Manage CA Certificates* on this page).

- **Active Self Certificates table**. Contains the self-signed certificates that were issued by CAs and that you uploaded (see *Manage Self-Signed Certificates* on page 384).

- **Self Certificate Requests table**. Contains the self-signed certificate requests that you generated. These requests might or might not have been submitted to CAs, and CAs might or might not have issued certificates for these requests. Only the self-signed certificates in the Active Self Certificates table are active on the UTM (see *Manage Self-Signed Certificates* on page 384).

- **Certificate Revocation Lists (CRL) table**. Contains the lists with certificates that have been revoked and are no longer valid, that were issued by CAs, and that you uploaded. Note, however, that the table displays only the active CAs and their critical release dates. (see *Manage the Certificate Revocation List* on page 388).

Manage CA Certificates

➢ **To view and upload trusted certificates:**

Select **VPN > Certificates**. The Certificates screen displays. (The following figure shows the top section of the screen with the trusted certificate information and some example certificates in the Trusted Certificates (CA Certificate) table.)
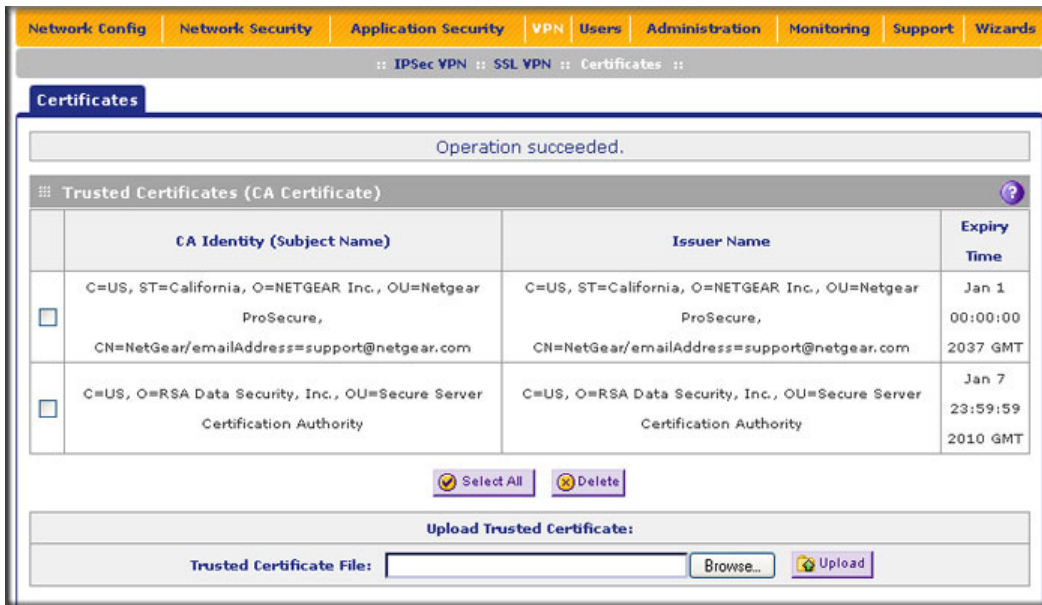
Figure 234. Certificates, screen 1 of 3

The Trusted Certificates (CA Certificate) table lists the digital certificates of CAs and contains the following fields:

- **CA Identity (Subject Name)**. The organization or person to whom the digital certificate is issued.

- **Issuer Name**. The name of the CA that issued the digital certificate.

- **Expiry Time**. The date after which the digital certificate becomes invalid.

➢ **To upload a digital certificate of a trusted CA on the UTM:**

1. Download a digital certificate file from a trusted CA and store it on your computer.

2. In the Upload Trusted Certificates section of the screen, click the **Browse** button and navigate to the trusted digital certificate file that you downloaded on your computer.

3. Click the **Upload** table button. If the verification process on the UTM approves the digital certificate for validity and purpose, the digital certificate is added to the Trusted Certificates (CA Certificates) table.

➢ **To delete one or more digital certificates:**

1. In the Trusted Certificates (CA Certificate) table, select the check box to the left of each digital certificate that you want to delete, or click the **Select All** table button to select all digital certificates.

2. Click the **Delete** table button.

Manage Self-Signed Certificates

Instead of obtaining a digital certificate from a CA, you can generate and sign your own digital certificate. However, a self-signed certificate triggers a warning from most browsers because it provides no protection against identity theft of the server. (The following figure shows an image of a browser security alert.)

There can be three reasons why a security alert is generated for a security certificate:

- The security certificate was issued by a company you have not chosen to trust.
- The date of the security certificate is invalid.
- The name on the security certificate is invalid or does not match the name of the site.

When a security alert is generated, the user can decide whether or not to trust the host.

Figure 235.

Generate a CSR and Obtain a Self-Signed Certificate from a CA

To use a self-signed certificate, you first need to request the certificate from a CA, and then download and activate the certificate on the UTM. To request a self-signed certificate from a CA, you need to generate a certificate signing request (CSR) for and on the UTM. The CSR is a file that contains information about your company and about the device that holds the certificate. Refer to the CA for guidelines about the information that you need to include in your CSR.

➢ **To generate a new CSR file, obtain a digital certificate from a CA, and upload it to the UTM:**

1. Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the middle section of the screen with the Active Self Certificates section, Generate Self Certificate Request section, and Self Certificate Requests section. (The Self Certificate Requests table contains some examples.)
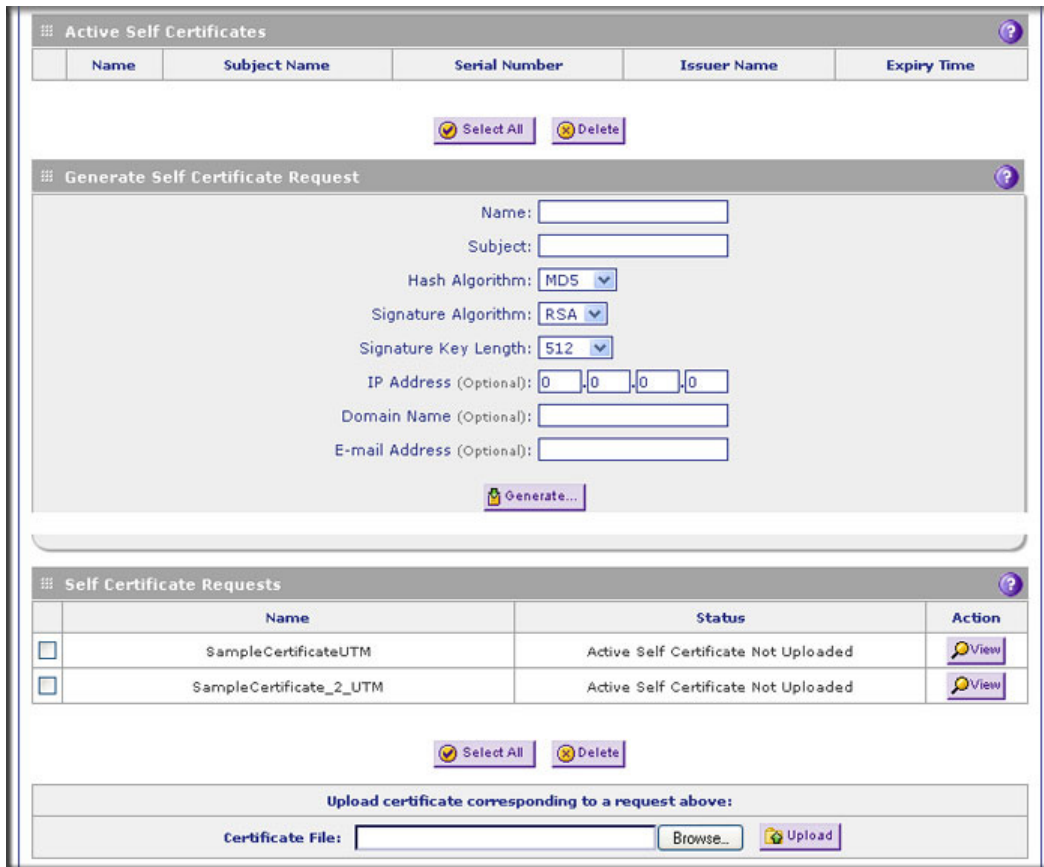
Figure 236. Certificates, screen 2 of 3

2. In the Generate Self Certificate Request section of the screen, enter the settings as explained in the following table:

Table 98. Generate self-signed certificate request settings

Setting	Description
Name	A descriptive name of the domain for identification and management purposes.
Subject	The name that other organizations see as the holder (owner) of the certificate. In general, use your registered business name or official company name for this purpose. **Note:** Generally, all of your certificates should have the same value in the Subject field.
Hash Algorithm	From the drop-down list, select one of the following hash algorithms: • **MD5**. A 128-bit (16-byte) message digest, slightly faster than SHA-1. • **SHA-1**. A 160-bit (20-byte) message digest, slightly stronger than MD5.
Signature Algorithm	Although this seems to be a drop-down list, the only possible selection is RSA. In other words, RSA is the default to generate a CSR.

Table 98. Generate self-signed certificate request settings (continued)

Setting	Description	
Signature Key Length	From the drop-down list, select one of the following signature key lengths in bits: • **512** • **1024** • **2048** **Note:** Larger key sizes might improve security, but might also decrease performance.	
Optional Fields	IP Address	Enter your fixed (static) IP address. If your IP address is dynamic, leave this field blank.
	Domain Name	Enter your Internet domain name, or leave this field blank.
	E-mail Address	Enter the email address of a technical contact in your company.

3. Click the **Generate** table button. A new SCR is created and added to the Self Certificate Requests table.

4. In the Self Certificate Requests table, click the **View** table button in the Action column to view the new SCR. The Certificate Request Data screen displays:
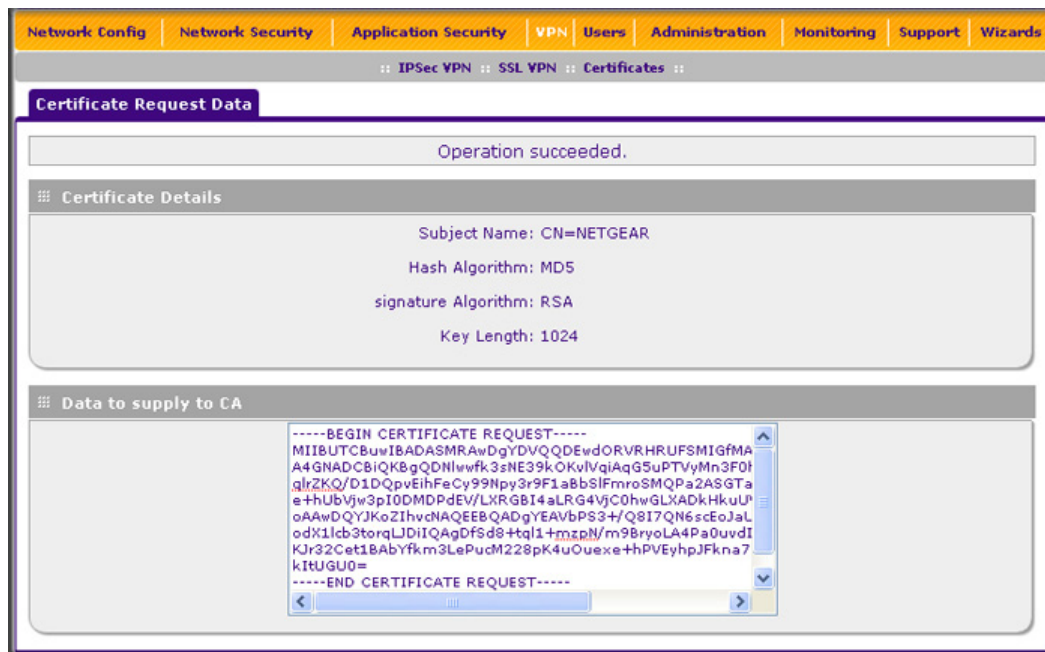
Figure 237.

5. Copy the contents of the Data to supply to CA text field into a text file, including all of the data contained from "-----BEGIN CERTIFICATE REQUEST-----" to "-----END CERTIFICATE REQUEST-----."

6. Submit your SCR to a CA:

    a. Connect to the website of the CA.

    b. Start the SCR procedure.

    c. When prompted for the requested data, copy the data from your saved text file (including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----").

    d. Submit the CA form. If no problems ensue, the digital certificate is issued by the CA.

7. Download the digital certificate file from the CA, and store it on your computer.

8. Return to the Certificates screen (see *Figure 236* on page 385) and locate the Self Certificate Requests section.

9. Select the check box next to the self-signed certificate request.

10. Click the **Browse** button and navigate to the digital certificate file from the CA that you just stored on your computer.

11. Click the **Upload** table button. If the verification process on the UTM approves the digital certificate for validity and purpose, the digital certificate is added to the Active Self Certificates table.

➢ **To delete one or more SCRs:**

1. In the Self Certificate Requests table, select the check box to the left of each SCR that you want to delete, or click the **Select All** table button to select all SCRs.

2. Click the **Delete** table button.

View and Manage Self-Signed Certificates

The Active Self Certificates table on the Certificates screen (see *Figure 236* on page 385) shows the digital certificates issued to you by a CA and available for use. For each self-signed certificate, the table lists the following information:

- **Name**. The name that you used to identify this certificate.

- **Subject Name**. The name that you used for your company and that other organizations see as the holder (owner) of the certificate.

- **Serial Number**. This is a serial number maintained by the CA. It is used to identify the certificate with the CA.

- **Issuer Name**. The name of the CA that issued the certificate.

- **Expiry Time**. The date on which the certificate expires. You should renew the certificate before it expires.

➢ **To delete one or more self-signed certificates:**

1. In the Active Self Certificates table, select the check box to the left of each self-signed certificate that you want to delete, or click the **Select All** table button to select all self-signed certificates.

2. Click the **Delete** table button.

Manage the Certificate Revocation List

A Certificate Revocation List (CRL) file shows digital certificates that have been revoked and are no longer valid. Each CA issues its own CRLs. It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

➢ **To view the currently loaded CRLs and upload a new CRL:**

1. Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the bottom section of the screen with the Certificate Revocation Lists (CRL) table. (There is one example in the table.)
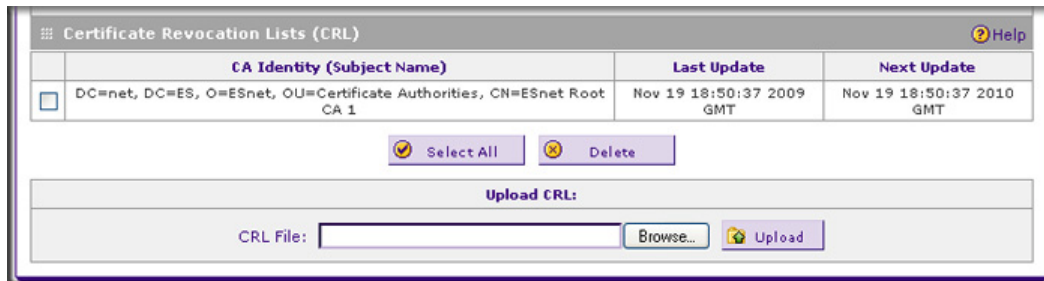
Figure 238. Certificates, screen 3 of 3

The Certificate Revocation Lists (CRL) table lists the active CAs and their critical release dates:

- **CA Identity**. The official name of the CA that issued the CRL.
- **Last Update**. The date when the CRL was released.
- **Next Update**. The date when the next CRL will be released.

2. In the Upload CRL section, click the **Browse** button and navigate to the CLR file that you previously downloaded from a CA.

3. Click the **Upload** table button. If the verification process on the UTM approves the CRL, the CRL is added to the Certificate Revocation Lists (CRL) table.

> **Note:** If the table already contains a CRL from the same CA, the old CRL is deleted when you upload the new CRL.

➢ **To delete one or more CRLs:**

1. In the Certificate Revocation Lists (CRL) table, select the check box to the left of each CRL that you want to delete, or click the **Select All** table button to select all CRLs.

2. Click the **Delete** table button.

Network and System Management

10

This chapter describes the tools for managing the network traffic to optimize its performance and the system management features of the UTM. This chapter contains the following sections:

- *Performance Management*
- *System Management*
- *Connect to a ReadyNAS and Configure Quarantine Settings (UTM9S Only)*

> **Note:** The ReadyNAS Integration configuration menu shows on the UTM9S only.

Performance Management

Performance management consists of controlling the traffic through the UTM so that the necessary traffic gets through when there is a bottleneck. You can either reduce unnecessary traffic or reschedule some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The UTM has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

The maximum bandwidth capacity of the UTM in each direction is as follows:

- LAN side (single WAN port models and multiple WAN port models). 4000 Mbps (four LAN ports at 1000 Mbps each), except for the UTM50, which has six LAN ports and therefore supports up to 6000 Mbps.
- WAN side
  - Load balancing mode (multiple WAN port models only). 2000 Mbps (two WAN ports at 1000 Mbps each), except for the UTM150, which has four WAN ports and therefore supports up to 4000 Mbps.
  - Auto-rollover mode (multiple WAN port models only). 1000 Mbps (one active WAN port at 1000 Mbps).
  - Primary WAN mode (single WAN port models and multiple WAN port models). 1000 Mbps (one active WAN port at 1000 Mbps).

In practice, the WAN-side bandwidth capacity is much lower when DSL or cable modems are used to connect to the Internet. At 1.5 Mbps, the WAN ports support the following traffic rates:

- Load balancing mode (multiple WAN port models only). 3 Mbps (two WAN ports at 1.5 Mbps each), except for the UTM150, which has four WAN ports and therefore supports up to 6 Mbps.
- Auto-rollover mode (multiple WAN port models only). 1.5 Mbps (one active WAN port at 1.5 Mbps).
- Primary WAN mode (single WAN port models and multiple WAN port models). 1.5 Mbps (one active WAN port at 1.5 Mbps).

As a result, and depending on the traffic that is being carried, the WAN side of the UTM is the limiting factor for the data rate for most installations.

Using the WAN ports in load balancing mode increases the bandwidth capacity of the WAN side of the UTM, but there is no backup in case one of the WAN ports fails. When such a failure occurs, the traffic that would have been sent on the failed WAN port is diverted to the WAN port that is still working, thus increasing its load. However, there is one exception: Traffic that is bound by protocol to the WAN port that failed is not diverted.

Features That Reduce Traffic

You can adjust the following features of the UTM in such a way that the traffic load on the WAN side decreases:

- LAN WAN outbound rules (also referred to as service blocking)
- DMZ WAN outbound rules (also referred to as service blocking)
- Content filtering
- Source MAC filtering

LAN WAN Outbound Rules and DMZ WAN Outbound Rules (Service Blocking)

You can control specific outbound traffic (from LAN to WAN and from the DMZ to WAN). The LAN WAN Rules screen and the DMZ WAN Rules screen list all existing rules for outbound traffic. If you have not defined any rules, only the default rule is listed. The default rule allows all outgoing traffic. Any outbound rule that you create restricts outgoing traffic and therefore decreases the traffic load on the WAN side.

> **WARNING!**
>
> **This feature is for advanced administrators. Incorrect configuration might cause serious problems.**

Each rule lets you specify the desired action for the connections that are covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise allow
- ALLOW always
- ALLOW by schedule, otherwise block

The following section summarizes the various criteria that you can apply to outbound rules in order to reduce traffic. For more information about outbound rules, see *Outbound Rules (Service Blocking)* on page 123. For detailed procedures on how to configure outbound rules, see *Set LAN WAN Rules* on page 130 and *Set DMZ WAN Rules* on page 133.

When you define outbound firewall rules, you can further refine their application according to the following criteria:

- **Services**. You can specify the services or applications, or groups of services or applications to be covered by an outbound rule. If the desired service or application does not display in the list, you need to define it using the Services screen (see *Service-Based Rules* on page 123 and *Add Customized Services* on page 152).

- **LAN users**. You can specify which computers on your network are affected by an outbound rule. There are several options:

  - **Any**. The rule applies to all PCs and devices on your LAN.
  - **Single address**. The rule applies to the address of a particular PC.
  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule applies to a group of PCs. (You can configure groups for LAN WAN outbound rules but not for DMZ WAN outbound rules.) The Known PCs and Devices table is an automatically maintained list of all known PCs and network devices and is generally referred to as the network database, which is described in *Manage the Network Database* on page 107. PCs and network devices are entered into the network database by various methods, which are described in *Manage Groups and Hosts (LAN Groups)* on page 106.
  - **IP Groups**. The rule applies to a group of individual LAN IP addresses. Use the IP Groups screen (under the Network Security main navigation menu) to assign IP addresses to groups. For more information, see *Create IP Groups* on page 156.

- **WAN users**. You can specify which Internet locations are covered by an outbound rule, based on their IP address:

  - **Any**. The rule applies to all Internet IP address.
  - **Single address**. The rule applies to a single Internet IP address.
  - **Address range**. The rule applies to a range of Internet IP addresses.
  - **IP Groups**. The rule applies to a group of individual WAN IP addresses. Use the IP Groups screen (under the Network Security main navigation menu) to assign IP addresses to groups. For more information, see *Create IP Groups* on page 156.

- **Schedule**. You can configure three different schedules to specify when a rule is applied. Once a schedule is configured, it affects all rules that use this schedule. You specify the

days of the week and time of day for each schedule. For more information, see *Set a Schedule to Block or Allow Specific Traffic* on page 163.

- **QoS profile**. You can define QoS profiles and then apply them to outbound rules to regulate the priority of traffic. For information about how to define QoS profiles, see *Create Quality of Service Profiles* on page 158.

- **Bandwidth profile**. You can define bandwidth profiles and then apply them to outbound rules to limit traffic. For information about how to define bandwidth profiles, see *Create Bandwidth Profiles* on page 160.

Content Filtering

If you want to reduce traffic by preventing undesired emails from reaching their destinations or by preventing access to certain sites on the Internet, you can use the UTM's content-filtering feature. By default, this feature is disabled; all requested traffic from any website is allowed with the exception of web content categories that are mentioned in *Default Email and Web Scan Settings* on page 176.

- **Email content filtering**. To reduce incoming email traffic, you can block emails with large attachments, reject emails based on keywords, file extensions, or file names, and set spam protection rules. There are several ways you can reduce undesired email traffic:
  - **Setting the size of email files to be scanned**. Scanning large email files requires network resources and might slow down traffic. You can specify the maximum size of the files or messages that are scanned, and if files that exceed the maximum size are skipped (which might compromise security) or blocked. For more information, see *Customize Email Antivirus and Notification Settings* on page 179.
  - **Keyword, file extension, and file name blocking**. You can reject emails based on keywords in the subject line, file type of the attachment, and file name of the attachment. For more information, see *Email Content Filtering* on page 183.
  - **Protecting against spam**. Set up spam protection to prevent spam from using up valuable bandwidth. For more information, see *Protect Against Email Spam* on page 186.

- **Web content filtering**. The UTM provides extensive methods to filter web content in order to reduce traffic:
  - **Web category blocking**. You can block entire web categories because their content is undesired, offensive, or not relevant, or simply to reduce traffic. For more information, see *Configure Web Content Filtering* on page 199.
  - **Keyword and file extension blocking**. You can specify words that, should they appear in the website name (URL), file extension, or newsgroup name, cause that site, file, or newsgroup to be blocked by the UTM. For more information, see *Configure Web Content Filtering* on page 199.
  - **URL blocking**. You can specify up to 200 URLs that are blocked by the UTM. For more information, see *Configure Web URL Filtering* on page 206.
  - **Web services blocking**. You can block web services such as instant messaging, peer-to-peer and media applications, and tools. For more information, see *Customize Web Protocol Scan Settings and Services (Web Applications)* on page 194.

- **Web object blocking**. You can block the following web component types: embedded objects (ActiveX, Java, Flash), proxies, and cookies; and you can disable JavaScripts. For more information, see *Configure Web Content Filtering* on page 199.

- **Setting the size of Web files to be scanned**. Scanning large web files requires network resources and might slow down traffic. You can specify the maximum size of the files that are scanned, and if files that exceed the maximum size are skipped (which might compromise security) or blocked. For more information, see *Configure Web Malware Scans* on page 197.

For these features (with the exception of web object blocking and setting the size of files to be scanned), you can set schedules to specify when web content is filtered (see *Configure Web Content Filtering* on page 199), and configure exceptions for groups (see *Set Web Access Exception Rules* on page 221).

Source MAC Filtering

If you want to reduce outgoing traffic by preventing Internet access by certain PCs on the LAN, you can use the source MAC filtering feature to drop the traffic received from the PCs with the specified MAC addresses. By default, this feature is disabled; all traffic received from PCs with any MAC address is allowed. See *Enable Source MAC Filtering* on page 164 for the procedure on how to use this feature.

Features That Increase Traffic

The following features of the UTM tend to increase the traffic load on the WAN side:

- LAN WAN inbound rules (also referred to as port forwarding)
- DMZ WAN inbound rules (also referred to as port forwarding)
- Port triggering
- Enabling the DMZ port
- Configuring exposed hosts
- Configuring VPN tunnels

LAN WAN Inbound Rules and DMZ WAN Inbound Rules (Port Forwarding)

The LAN WAN Rules screen and the DMZ WAN Rules screen list all existing rules for inbound traffic (from WAN to LAN and from WAN to the DMZ). If you have not defined any rules, only the default rule is listed. The default rule blocks all access from outside except responses to requests from the LAN side. Any inbound rule that you create allows additional incoming traffic and therefore increases the traffic load on the WAN side.

⚠ **WARNING!**

This feature is for advanced administrators. Incorrect configuration might cause serious problems.

Each rule lets you specify the desired action for the connections covered by the rule:

* BLOCK always
* BLOCK by schedule, otherwise allow
* ALLOW always
* ALLOW by schedule, otherwise block

The following section summarizes the various criteria that you can apply to inbound rules and that might increase traffic. For more information about inbound rules, see *Inbound Rules (Port Forwarding)* on page 126. For detailed procedures on how to configure inbound rules, see *Set LAN WAN Rules* on page 130 and *Set DMZ WAN Rules* on page 133.

When you define inbound firewall rules, you can further refine their application according to the following criteria:

* **Services**. You can specify the services or applications, or groups of services or applications to be covered by an inbound rule. If the desired service or application does not display in the list, you need to define it using the Services screen (see *Service-Based Rules* on page 123 and *Add Customized Services* on page 152).

* **WAN destination IP address**. For the multiple WAN port models only, you can specify the destination IP address for incoming traffic. Traffic is directed to the specified address only when the destination IP address of the incoming packet matches the IP address of the selected WAN interface. For the single WAN port models, the WAN Destination IP Address is a fixed field.

* **LAN users**. You can specify which computers on your network are affected by an inbound rule. There are several options:

  - **Any**. The rule applies to all PCs and devices on your LAN.

  - **Single address**. The rule applies to the address of a particular PC.

  - **Address range**. The rule applies to a range of addresses.

  - **Groups**. The rule is applied to a group of PCs. (You can configure groups for LAN WAN outbound rules but not for DMZ WAN outbound rules.) The Known PCs and Devices table is an automatically maintained list of all known PCs and network devices and is generally referred to as the network database, which is described in *Manage the Network Database* on page 107. PCs and network devices are entered into the network database by various methods, which are described in *Manage Groups and Hosts (LAN Groups)* on page 106.

  - **IP Groups**. The rule applies to a group of individual LAN IP addresses. Use the IP Groups screen (under the Network Security main navigation menu) to assign IP addresses to groups. For more information, see *Create IP Groups* on page 156.

* **WAN users**. You can specify which Internet locations are covered by an inbound rule, based on their IP address:

  - **Any**. The rule applies to all Internet IP address.

  - **Single address**. The rule applies to a single Internet IP address.

  - **Address range**. The rule applies to a range of Internet IP addresses.

- **IP Groups**. The rule applies to a group of individual WAN IP addresses. Use the IP Groups screen (under the Network Security main navigation menu) to assign IP addresses to groups. For more information, see *Create IP Groups* on page 156.

- **Schedule**. You can configure three different schedules to specify when a rule is applied. Once a schedule is configured, it affects all rules that use this schedule. You specify the days of the week and time of day for each schedule. For more information, see *Set a Schedule to Block or Allow Specific Traffic* on page 163.

- **QoS profile**. You can define QoS profiles and then apply them to inbound rules to regulate the priority of traffic. For information about how to define QoS profiles, see *Create Quality of Service Profiles* on page 158.

- **Bandwidth profile**. You can define bandwidth profiles and then apply them to inbound rules to limit traffic. For information about how to define bandwidth profiles, see *Create Bandwidth Profiles* on page 160.

Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port-triggering feature requires that you know the port numbers used by the application. Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a request from the LAN network. As such, it would be handled in accordance with the inbound port-forwarding rules, and most likely would be blocked.

For the procedure on how to configure port triggering, see *Configure Port Triggering* on page 168.

Configure the DMZ Port

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions when compared to the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. On the UTM5, UTM10, UTM25, and UTM150, LAN port 4 can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN. On the UTM50, LAN port 6 can be dedicated as a hardware DMZ port. By default, the DMZ port and both inbound and outbound DMZ traffic are disabled. Enabling the DMZ port and allowing traffic to and from the DMZ increases the traffic through the WAN ports.

For information about how to enable the DMZ port, see *Configure and Enable the DMZ Port* on page 112. For the procedures about how to configure DMZ traffic rules, see *Set DMZ WAN Rules* on page 133.

Configure Exposed Hosts

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined. For an example of how to set up an exposed host, see *LAN WAN or DMZ WAN Inbound Rule: Specify an Exposed Host* on page 142.

Configure VPN Tunnels

The UTM supports site-to-site IPSec VPN tunnels and dedicated SSL VPN tunnels. Each tunnel requires extensive processing for encryption and authentication, thereby increasing traffic through the WAN ports.

For information about IPSec VPN tunnels, see *Chapter 7, Virtual Private Networking Using IPSec Connections*. For information about SSL VPN tunnels, see *Chapter 8, Virtual Private Networking Using SSL Connections*.

Use QoS and Bandwidth Assignments to Shift the Traffic Mix

By specifying QoS and bandwidth profiles and assigning these profiles to outbound and inbound firewall rules, you can shift the traffic mix to aim for optimum performance of the UTM.

Assign QoS Profiles

The QoS profile settings determine the priority and, in turn, the quality of service for the traffic passing through the UTM. After you have created a QoS profile, you can assign the QoS profile to firewall rules. The QoS is set individually for each service. You can change the mix of traffic through the WAN ports by granting some services a higher priority than others:

- You can accept the default priority defined by the service itself by not changing its QoS setting.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

For more information about QoS profiles, see *Create Quality of Service Profiles* on page 158.

Assign Bandwidth Profiles

When you apply a QoS profile, the WAN bandwidth does not change. You change the WAN bandwidth that is assigned to a service or application by applying a bandwidth profile. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic, thus allocating LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN links.

For more information about bandwidth profiles, see *Create Bandwidth Profiles* on page 160.

Monitoring Tools for Traffic Management

The UTM includes several tools that can be used to monitor the traffic conditions of the firewall and content-filtering engine and to monitor the users' access to the Internet and the types of traffic that they are allowed to have. See *Chapter 11, Monitoring System Access and Performance*, for a description of these tools.

System Management

System management tasks are described in the following sections:

- *Change Passwords and Administrator and Guest Settings*
- *Configure Remote Management Access*
- *Use a Simple Network Management Protocol Manager*
- *Manage the Configuration File*
- *Update the Firmware*
- *Update the Scan Signatures and Scan Engine Firmware*
- *Configure Date and Time Service*

Change Passwords and Administrator and Guest Settings

The default administrator and default guest passwords for the web management interface are both password. NETGEAR recommends that you change the password for the administrator account to a more secure password, and that you configure a separate secure password for the guest account.

➢ **To modify the administrator and guest user account settings, including the password:**

1. Select **Users > Users**. The Users screen displays. (The following figure shows the UTM's default users—admin and guest—and, as an example, several other users in the List of Users table.)

Figure 239.

2. In the Action column of the List of Users table, click the **Edit** table button for the user with the name admin. The Edit User screen displays:

Figure 240.

3. Select the **Check to Edit Password** check box. The password fields become available.

4. Enter the old password, enter the new password, and then confirm the new password.

> **Note:** The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

5. As an option, you can change the idle time-out for an administrator login session. Enter a new number of minutes in the Idle Timeout field. (The default setting is 5 minutes.)

6. Click **Apply** to save your settings.

7. Repeat *step 1* through *step 6* for the user with the name guest.

> **Note:** After a factory defaults reset, the password and time-out value are changed back to password and 5 minutes, respectively.

You can also change the administrator login policies:

- Deny login access from a WAN interface. By default, the administrator can log in from a WAN interface.

- Deny or allow login access from specific IP addresses. By default, the administrator can log in from any IP address.

Note: For enhanced security, restrict access to as few external IP addresses as practical.

- Deny or allow login access from specific browsers. By default, the administrator can log in from any browser.

In general, these policy settings work well for an administrator. However, if you need to change any of these policy settings, see *Set User Login Policies* on page 365.

Configure Remote Management Access

An administrator can configure, upgrade, and check the status of the UTM over the Internet through a Secure Sockets Layer (SSL) VPN connection.

Note: When remote management is enabled and administrative access through a WAN interface is granted (see *Configure Login Policies* on page 365), the UTM's web management interface is accessible to anyone who knows its IP address and default password. Because a malicious WAN user can reconfigure the UTM and misuse it in many ways, NETGEAR highly recommends that you change the admin and guest default passwords before continuing (see *Change Passwords and Administrator and Guest Settings* on page 397).

➢ **To configure the UTM for remote management:**

1. Select **Administration > Remote Management**. The Remote Management screen displays:
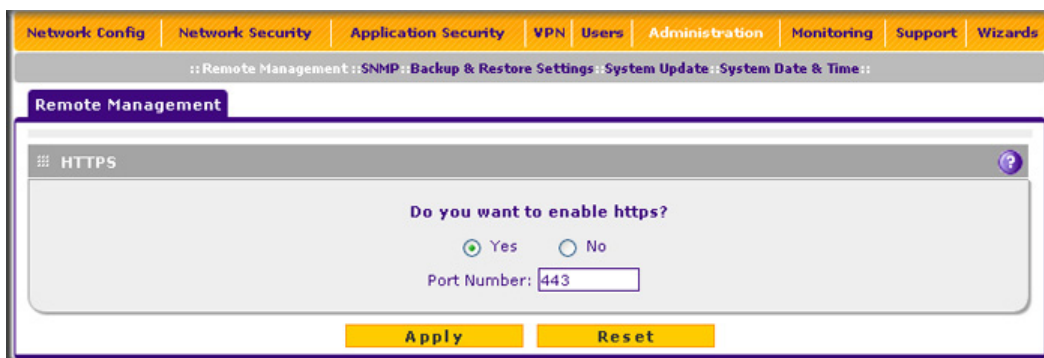
Figure 241.

2. Select one of the following radio buttons:
   - **Yes**. Enable HTTPS remote management. This is the default setting.
   - **No**. Disable HTTPS remote management.

Network and System Management

399

⚠️ **WARNING!**

If you are remotely connected to the UTM and you select the No radio button, you and all other SSL VPN users are disconnected when you click Apply.

3. As an option, you can change the default HTTPS port. The default port number is 443.

4. Click **Apply** to save your changes.

When remote management is enabled, you need to use an SSL connection to access the UTM from the Internet. You need to enter https:// (not http://) and type the UTM's WAN IP address in your browser. For example, if the UTM's WAN IP address is 10.16.0.123, type the following in your browser: **https://10.16.0.123**.

The UTM's remote login URL is:

https://<*IP_address*> or https://<*FullyQualifiedDomainName*>

Note: For enhanced security, restrict access to as few external IP addresses as practical. See *Set User Login Policies* on page 365 for instructions on restricting administrator access by IP address.

Note: To maintain security, the UTM rejects a login that uses http://*address* rather than the SSL https://*address*.

Note: The first time that you remotely connect to the UTM with a browser through an SSL connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or later, simply click **Yes** to accept the certificate.

Note: If you are unable to remotely connect to the UTM after enabling HTTPS remote management, check if other user policies, such as the default user policy, are preventing access. For access to the UTM's web management interface, check if administrative access through a WAN interface is granted (see *Configure Login Policies* on page 365).

> **Note:** If you disable HTTPS remote management, all SSL VPN user
>   connections are also disabled.

> **Tip:** If you are using a Dynamic DNS service such as TZO, you can identify
>   the WAN IP address of your UTM by running `tracert` from the
>   Windows Run menu option. Trace the route to your registered FQDN.
>   For example, enter `tracert UTM.mynetgear.net`, and the WAN IP
>   address that your ISP assigned to the UTM is displayed.

Use a Simple Network Management Protocol Manager

Simple Network Management Protocol (SNMP) forms part of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SNMP lets you monitor and manage your UTM from an SNMP manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

➢ **To configure the SNMP settings:**

1. Select **Administration > SNMP**. The SNMP screen displays:
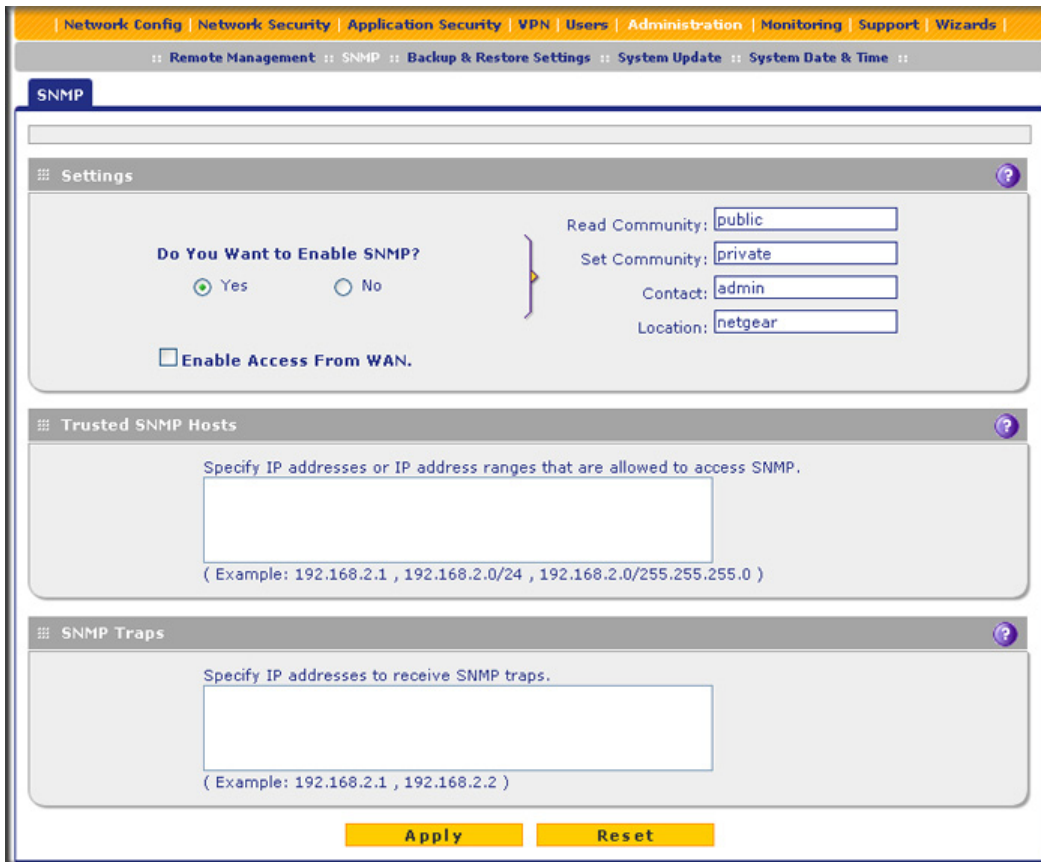
Figure 242.

2. Enter the settings as explained in the following table:

Table 99. SNMP screen settings

Setting	Description	
Settings		
Do You Want to Enable SNMP?	Select one of the following radio buttons: • **Yes**. Enable SNMP. • **No**. Disable SNMP. This is the default setting.	
	Read Community	The community string to allow an SNMP manager access to the MIB objects of the UTM for the purpose of reading only. The default setting is public.
	Set Community	The community string to allow an SNMP manager access to the MIB objects of the UTM for the purpose of reading and writing. The default setting is private.
	Contact	The SNMP system contact information that is available to the SNMP manager. This setting is optional.
	Location	The physical location of the UTM. This setting is optional.

Table 99. SNMP screen settings (continued)

Setting	Description
Enable Access From WAN	Select the **Enable Access From WAN** check box to allow SNMP management over a WAN connection. This check box is cleared by default, allowing SNMP management only over a LAN connection.
Trusted SNMP Hosts	
Enter the IP addresses of the computers and devices to which you want to grant read-only (GET) or write (SET) privileges on the UTM. Separate IP addresses by a comma. To allow any trusted SNMP host access, leave the field blank, which is the default setting.	
SNMP Traps	
Enter the IP addresses of the SNMP management stations that are allowed to receive the UTM's SNMP traps. Separate IP addresses by a comma. If you leave the field blank, which is the default setting, no SNMP management station can receive the UTM's SNMP traps.	

3. Click **Apply** to save your settings.

Manage the Configuration File

The configuration settings of the UTM are stored in a configuration file on the UTM. This file can be saved (backed up) to a PC, retrieved (restored) from the PC, or cleared to factory default settings.

Once the UTM is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the UTM settings from this file.

The Backup & Restore Settings screen lets you:

- Back up and save a copy of the current settings
- Restore saved settings from the backed-up file
- Revert to the factory default settings

To display the Backup & Restore Settings screen, select **Administration > Backup & Restore Settings**.
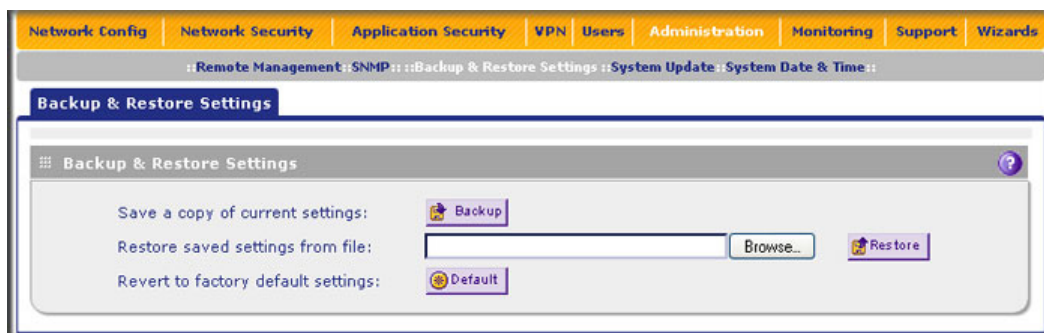
Figure 243.

Back Up Settings

The backup feature saves all UTM settings to a file. These settings include:

- **Network settings**. IP address, subnet mask, gateway, and so on.
- **Scan settings**. Services to scan, primary and secondary actions, and so on.
- **Update settings**. Update source, update frequency, and so on.
- **Antispam settings**. Whitelist, blacklist, content-filtering settings, and so on.

Back up your UTM settings periodically, and store the backup file in a safe place.

> **Tip:** You can use a backup file to export all settings to another UTM that has the same language and management software versions. Remember to change the IP address of the second UTM before deploying it to eliminate IP address conflicts on the network.

➢ **To back up settings:**

1. On the Backup & Restore Settings screen (see the previous figure), next to Save a copy of current settings, click the **Backup** button to save a copy of your current settings. A screen displays, showing the file name of the backup file (backup.pkg).
2. Select **Save file**, and then click **OK**.
3. Open the folder in which you have saved the backup file, and then verify that it has been saved successfully.

Note the following:

- If your browser is not configured to save downloaded files automatically, locate the folder in which you want to save the file, specify the file name, and save the file.
- If your browser is configured to save downloaded files automatically, the file is saved to your browser's download location on the hard disk.

Restore Settings

⚠️ **WARNING!**

Restore only settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the UTM system software.

➢ **To restore settings from a backup file:**

1. On the Backup & Restore Settings screen (see the previous figure), next to Restore saved settings from file, click **Browse**.
2. Locate and select the previously saved backup file (by default, backup.pkg).
3. After you have selected the file, click the **Restore** button. A warning message might display, and you might have to confirm that you want to restore the configuration.

The UTM reboots. During the reboot process, the Backup & Restore Settings screen remains visible. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

> ⚠️ **WARNING!**
>
> **Once you start restoring settings, do *not* interrupt the process. Do not try to go online, turn off the UTM, shut down the computer, or do anything else to the UTM until the settings have been fully restored.**

Revert to Factory Default Settings

To reset the UTM to the original factory defaults settings, you can use one of the following two methods:

- Using a sharp object, press and hold the factory default reset button on the rear panel of the UTM (see *Hardware Features* on page 22) for about 8 seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default settings when you do not know the administration password or IP address, you need to use the factory default reset button method.

- On the Backup & Restore Settings screen (see the previous figure), next to Revert to factory defaults settings, click the **Default** button.

The UTM reboots. If you use the software Default button, the Backup & Restore Settings screen remains visible during the reboot process. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

> ⚠️ **WARNING!**
>
> **When you press the hardware factory default reset button or click the software Default button, the UTM settings are erased. All firewall rules, VPN policies, LAN/WAN settings, and other settings are lost. Back up your settings if you intend on using them.**

> **Note:** After rebooting with factory default settings, the UTM's password is **password**, and the LAN IP address is **192.168.1.1**.

Update the Firmware

The UTM can automatically detect a new firmware version from a NETGEAR update server. The firmware upgrade process for the UTM consists of the following four stages:

1. Querying the available firmware versions from the NETGEAR update server.
2. Selecting a firmware version to download directly to the UTM (that is, not first to a computer in your network and then to the UTM).

3. Installing the downloaded firmware version.

4. Rebooting the UTM with the new firmware version.

These stages are explained in detail in the following sections.

View the Available Firmware Versions

➢ **To view the current version of the firmware that your UTM is running and the other available firmware versions:**

1. Select **Administration > System Update > Firmware**. The Firmware screen displays:
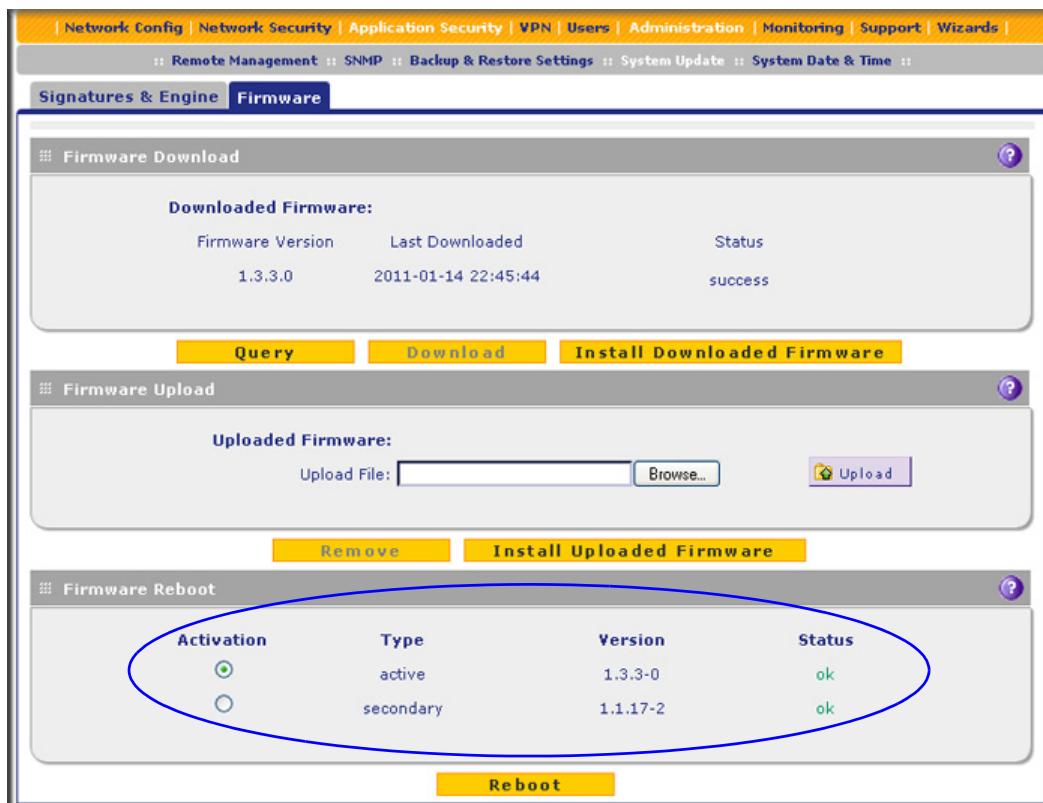
Figure 244. Firmware screen, available versions

The Firmware Reboot section shows the following information fields for both the active and secondary (that is, nonactive) firmware:

• **Type**. Active or secondary firmware.

• **Version**. The firmware version.

• **Status**. The status of the firmware (*ok* or *corrupted*).

2. To see which other firmware versions are available, click **Query** under the Firmware Download section to allow the UTM to connect to the NETGEAR update server. The Firmware Download section shows the available firmware versions, including any new versions, and the date when the current firmware version was downloaded to the UTM.

Upgrade the Firmware from an Update Server and Reboot the UTM

When the UTM is online, you can let the UTM connect to a remote update server to query new firmware versions. You can then decide whether or not you want to download new firmware, and whether or not you want to install new firmware.

Note: Upgrading the UTM firmware from an update server is also referred to as an online upgrade.

➢ **To upgrade the UTM's firmware directly from an update server and reboot the UTM:**

1. In the Firmware Download section of the Firmware screen, click **Query** to display the available firmware versions.

2. Select the radio button that corresponds to the firmware version that you want to download onto the UTM.

3. Click **Download**. The Download status bar shows the progress of the download. The following figure shows the Firmware screen after the firmware download is complete.

Figure 245. Firmware screen, after firmware download

4. Click **Install Downloaded Firmware**.

5. After the firmware installation process is complete, the newly installed firmware is the secondary firmware and not the active firmware. Ensure that the Activation radio button for the secondary firmware is selected (it should have been selected automatically).

---

6. Click the **Reboot** button at the bottom of the screen to start the reboot process. The UTM reboots automatically. During the reboot process, the Firmware screen remains visible. The reboot process is complete after several minutes when the Test LED on the front panel goes off and the Firmware screen disappears.

> **WARNING!**
>
> **After you have started the firmware installation process, do *not* interrupt the process. Do not try to go online, turn off the UTM, or do anything else to the UTM until the UTM has fully rebooted.**

7. Log back in to the UTM. The System Status screen displays.

8. In the System Information section of the System Status screen, verify that the newly installed firmware is the active firmware and that the old firmware is now the secondary firmware.

> **Note:** In some cases, such as a major upgrade, it might be necessary to erase the configuration and manually reconfigure your UTM after upgrading it. Refer to the firmware release notes that NETGEAR makes available.

Upgrade the Firmware from a Downloaded File and Reboot the UTM

Instead of downloading the UTM firmware directly from a NETGEAR update server, you can download the UTM firmware from a NETGEAR website to a computer in your network and then upgrade the firmware on the UTM.

This option prevents the UTM from taking bandwidth away from end users because the download does not occur on the UTM. This option is also convenient if you have multiple UTMs in your network, because you can download the firmware just once, make it available at a central location in your network, and then upload the firmware on each UTM.

> **Note:** Upgrading the UTM firmware from a downloaded file is also referred to as an offline upgrade.

➢ **To download the latest firmware for your UTM:**

1. Use one of the following two methods to go to the product support page:

- Visit the NETGEAR Support website at *http://support.netgear.com*. In the Find Your Product field, enter the model number of your UTM (for example, enter **UTM25**).

- Go directly to the product support page by entering **http://kbserver.netgear.com/products/<*productmodel*>.asp**, in which you need to replace <*productmodel*> with the model number of your UTM (for example, enter **http://kbserver.netgear.com/products/utm25.asp**).

2. When the product support page displays, click the **Download** tab to view the available firmware versions.

3. Follow the instructions onscreen to download the firmware to your computer.

➢ **To upgrade the UTM's firmware from a downloaded file and reboot the UTM:**

1. In the Firmware Upload section of the Firmware screen, click **Browse** to locate and select the previously saved firmware upgrade file (for example, UTM50-Firmware-1.3.4.0.pkg).

2. Click **Upload**.

⚠ **WARNING!**

Uploading firmware to the UTM stops any firmware downloading process that might be occurring and removes any downloaded and uploaded firmware files from the UTM. While the upload is occurring, do not leave or refresh the Firmware screen.

When the firmware upload process is complete, the new firmware version is displayed in the Firmware Upload section of the screen; a firmware version that previously might have been displayed in the Firmware Download section of the screen is no longer shown:
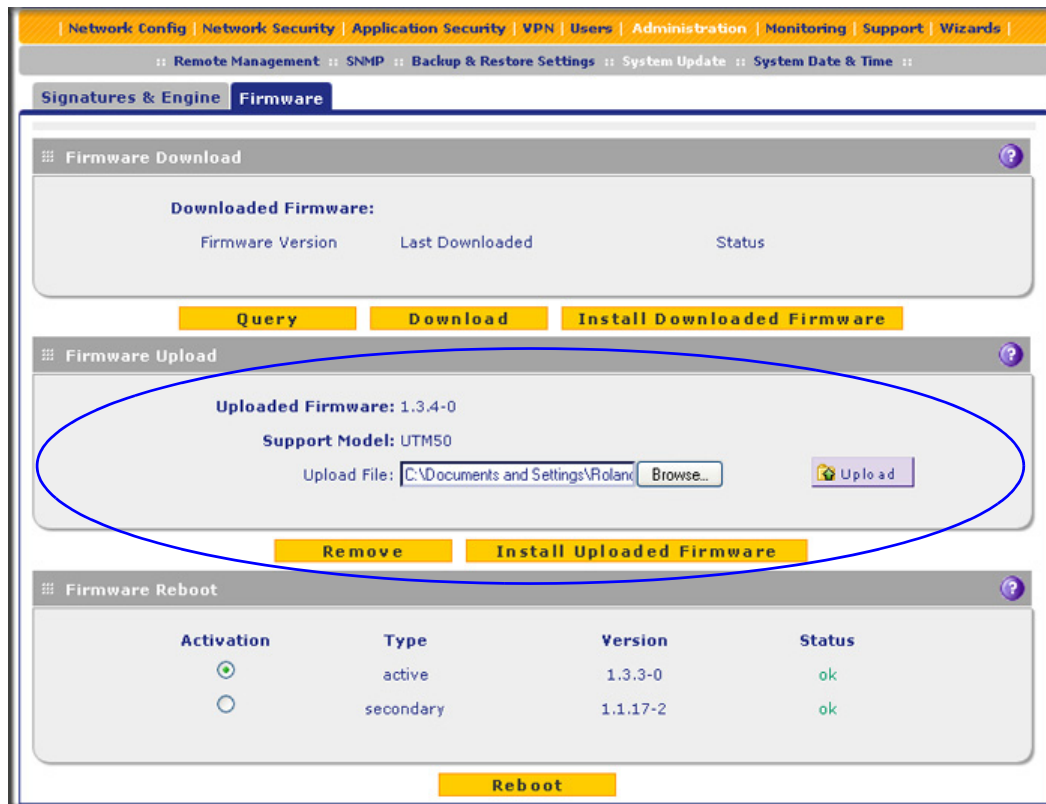
Figure 246.   Firmware screen, after firmware upload

3. Click **Install Uploaded Firmware**. (If you decide that you do not want to install the uploaded firmware, you can click **Remove** to remove the uploaded firmware.)

> **Note:** The license is verified during the firmware installation process, and the Install status bar shows the progress of the installation process.

4. After the firmware installation process is complete, the newly installed firmware is the secondary firmware and not the active firmware. Ensure that the Activation radio button for the secondary firmware is selected (it should have been selected automatically).

5. Click the **Reboot** button at the bottom of the screen to start the reboot process. A counter at the top of the screen displays the remaining time before the UTM actually reboots.

6. Log back in to the UTM. The System Status screen displays.

7. In the System Information section of the System Status screen, verify that the newly installed firmware is the active firmware and that the old firmware is now the secondary firmware.

> **Note:** In some cases, such as a major upgrade, it might be necessary to erase the configuration and manually reconfigure your UTM after upgrading it. Refer to the firmware release notes that NETGEAR makes available.

Reboot without Changing the Firmware

➢ **To reboot the UTM without changing the firmware:**

1. In the Firmware Reboot section of the Firmware screen (see the previous figure), select the active firmware version by selecting the **Activation** radio button for the firmware that is shown as active in the Type column.

2. Click **Reboot**. The UTM reboots. During the reboot process, the Firmware screen remains visible. The reboot process is complete after several minutes when the Test LED on the front panel goes off and the Firmware screen disappears.

3. Log back in to the UTM.

Update the Scan Signatures and Scan Engine Firmware

To scan and detect viruses, spyware, and other malware threats, the UTM's scan engine requires two components:

- A pattern file that contains the virus signature files and virus database
- Firmware that functions in conjunction with the pattern file

Because new virus threats can appear any hour of the day, it is very important to keep both the pattern file and scan engine firmware current. The UTM can automatically check for updates, as often as every 15 minutes, to ensure that your network protection is current.

To view the current versions and most recent updates of the pattern file and scan engine firmware that your UTM is running, select **Administration > System Update**. The System Update submenu tabs display, with the Signatures & Engine screen in view:
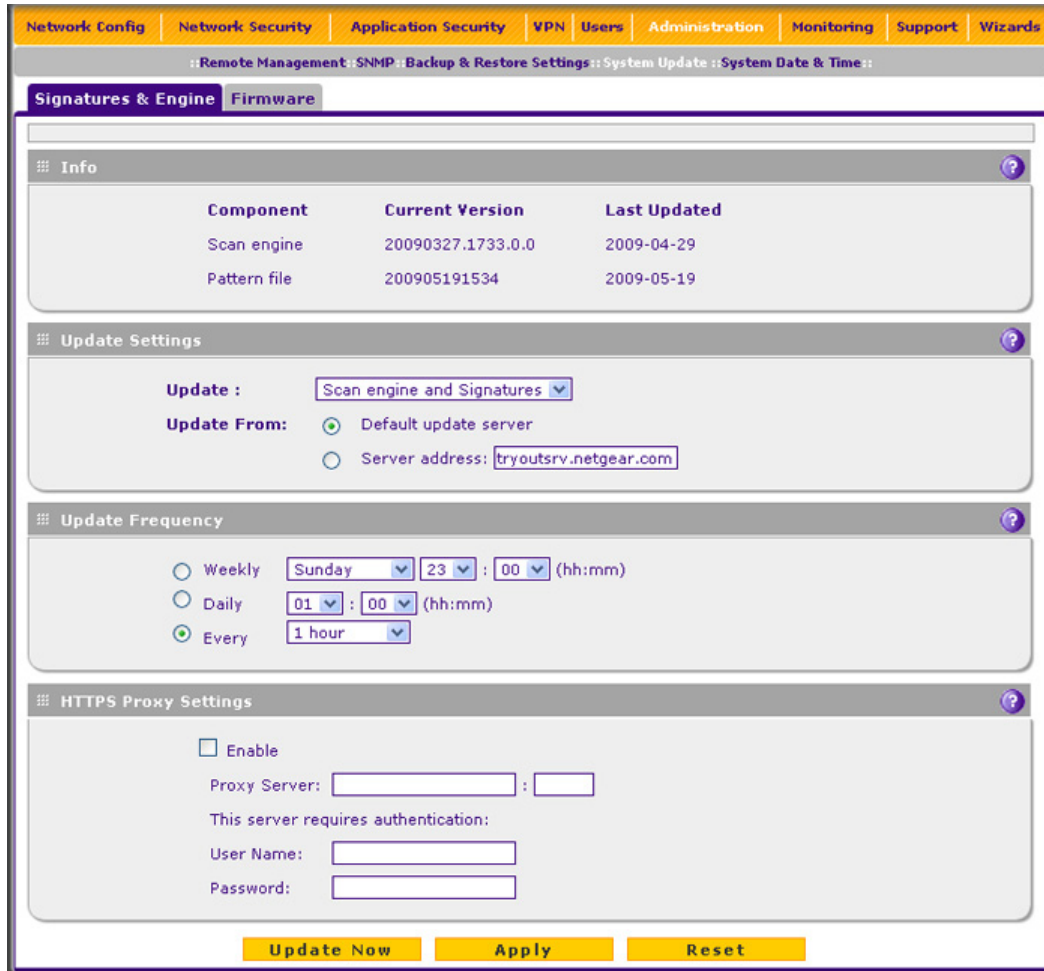
Figure 247.

The Info section on the screen shows the following information fields for the scan engine firmware and pattern file:

• **Current Version**. The version of the files.

• **Last Updated**. The date of the most recent update.

To immediately update the scan engine firmware and pattern file, click the **Update Now** button at the bottom of the screen.

Configure Automatic Update and Frequency Settings

➢ **To configure the update settings and frequency settings for automatic downloading of the scan engine firmware and pattern file:**

1. Locate the Update Settings, Frequency Settings, and HTTPS Proxy Settings sections on the Signatures & Engine screen (see the previous figure), and enter the settings as explained in the following table:

Table 100. Signatures & Engine screen settings

Setting	Description
Update Settings	
Update	From the drop-down list, select one of the following options: • **Never**. The pattern and firmware files are not automatically updated. • **Scan engine and Signatures**. The pattern and firmware files are automatically updated according to the settings in the Update Frequency section on the screen (see explanations later in this table).
Update From	Set the update source server by selecting one of the following radio buttons: • **Default update server**. Files are updated from the default NETGEAR update server. • **Server address**. Files are updated from the server that you specify. Enter the IP address or host name of the update server in the Server address field.
Update Frequency	
Specify the frequency with which the UTM checks for file updates by selecting one of the following radio buttons: • **Weekly**. From the drop-down lists, select the weekday, hour, and minutes that the updates occur. • **Daily**. From the drop-down lists, select the hour and minutes that the updates occur. • **Every**. From the drop-down list, select the frequency with which the updates occur. The range is from 15 minutes to 12 hours.	
HTTPS Proxy Settings	
Enable	If computers on the network connect to the Internet through a proxy server, select the **Enable** check box to specify and enable a proxy server. Enter the following settings.
	Proxy Server The IP address and port number of the proxy server.
	User Name The user name for proxy server authentication.
	Password The password for proxy server authentication.

2. Click **Apply** to save your settings.

Configure Date and Time Service

Configure date, time, and NTP server designations on the System Date & Time screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Setting the correct system time and time zone ensures that the date and time recorded in the UTM logs and reports are accurate.

➢ **To set time, date, and NTP servers:**

1. Select **Administration > System Date & Time**. The System Date & Time screen displays:
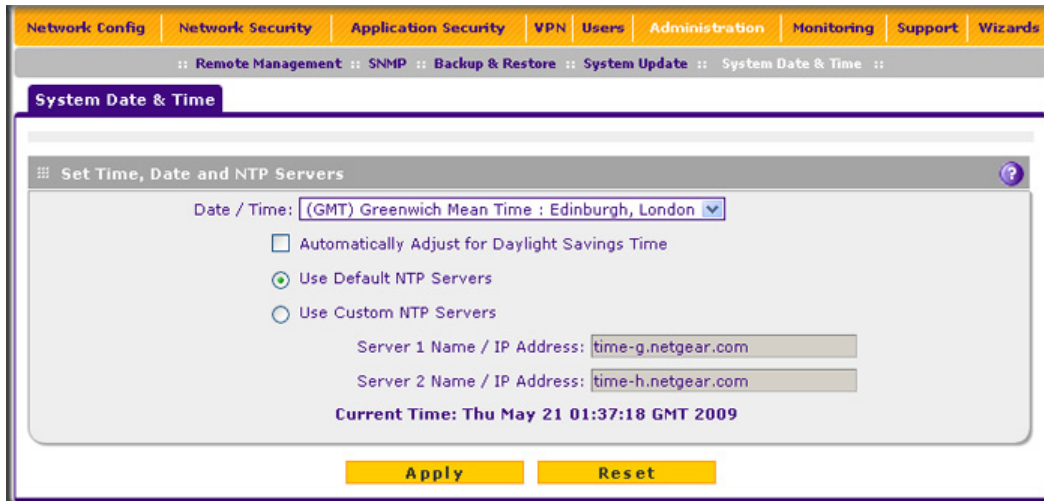
Figure 248.

The bottom of the screen displays the current weekday, date, time, time zone, and year (in the example in the previous figure: Current Time: Thu May 21 01:37:18 GMT 2009).

2. Enter the settings as explained in the following table:

Table 101. System Date & Time screen settings

Setting	Description
Date/Time	From the drop-down list, select the local time zone in which the UTM operates. The correct time zone is required in order for scheduling to work correctly. The UTM includes a real-time clock (RTC), which it uses for scheduling.
Automatically Adjust for Daylight Savings Time	If daylight savings time is supported in your region, select the **Automatically Adjust for Daylight Savings Time** check box.
NTP Server (default or custom)	From the drop-down list, select an NTP server: • **Use Default NTP Servers**. The UTM regularly updates its RTC by contacting a default NETGEAR NTP server on the Internet. • **Use Custom NTP Servers**. The UTM regularly updates its RTC by contacting one of two custom NTP servers (primary and backup), both of which you need to specify in the fields that become available with this selection. **Note:** If you select the Use Custom NTP Servers option but leave either the Server 1 or Server 2 field blank, both fields are set to the default NETGEAR NTP servers. **Note:** A list of public NTP servers is available at *http://support.ntp.org/bin/view/Servers/WebHome*.

Table 101. System Date & Time screen settings (continued)

Setting	Description	
NTP Server (default or custom) (continued)	Server 1 Name / IP Address	Enter the IP address or host name of the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name of the backup NTP server.

3. Click **Apply** to save your settings.

> **Note:** If you select the default NTP servers or if you enter a custom server FQDN, the UTM determines the IP address of the NTP server by performing a DNS lookup. Before the UTM can perform this lookup, you need to configure a DNS server address on the WAN ISP Settings screen of the single WAN port models or on one of the WAN ISP Settings screens of the multiple WAN port models (see *Manually Configure the Internet Connection* on page 71.)

Connect to a ReadyNAS and Configure Quarantine Settings (UTM9S Only)

The UTM9S can quarantine questionable emails (including spam), attachments, objects, and web files. This requires an increasing amount of storage space, which is not available on the UTM9S. To accommodate these storage requirements, you need to connect the UTM9S to a NETGEAR ReadyNAS and configure the quarantine settings. Without integration with a ReasyNAS, you cannot use the quarantine options of the UTM9S.

You can select to quarantine emails, attachments, objects, and web files on one or more of the following screens:

- Email Anti-Virus screen (see *Customize Email Antivirus and Notification Settings* on page 179)
- Distributed Spam Analysis screen (see *Configure Distributed Spam Analysis* on page 191)
- Malware Scan screen (see *Configure Web Malware Scans* on page 197)
- FTP screen (*Configure FTP Scans* on page 219)

Log Storage

After you have integrated a ReadyNAS with the UTM9S—whether or not you have configured the quarantine settings—all logs that are normally stored on the UTM9S are now stored on the ReadyNAS. That is, all logs that you can specify on the Email and Syslog screen (see *Configure and Activate System, Email, and Syslog Logs* on page 423) and that you can query

on the Log Query screen and view onscreen (see *Query the Quarantine Logs (UTM9S Only)* on page 467) are stored on the ReadyNAS. However, after you have integrated a ReadyNAS with the UTM9S, logs can no longer be sent to an email address (see the Email Logs to Administrator section on the Email and Syslog screen). If you have enabled a syslog server on the Email and Syslog screen, logs are still send to the syslog server.

> **WARNING!**
>
> **When you integrate a ReadyNAS with the UTM9S, the logs that were saved on the UTM9S are deleted.**

Note: If the network connection to the ReadyNAS goes down, the quarantine logs are no longer saved, and all other logs are saved on the UTM9S. In this situation, the ReadyNAS and quarantine status fields show OFF on the System Status screen (see *View the System Status Screen* on page 440). When the network connection comes back up, the quarantine logs and all other logs are saved on the ReadyNAS once again, but the logs that were saved on the UTM9S are deleted.

Connect to a ReadyNAS

➢ **To connect to the ReadyNAS on the UTM9S:**

1. Select **Administration > ReadyNAS Integration**. The ReadyNAS Integration screen displays:

Figure 249.

2. To connect to the ReadyNAS, select the **Yes** radio button.

3. Enter the settings as explained in the following table:

Table 102. ReadyNAS Integration screen settings

Setting	Description
ReadyNAS Server	The IP address of the ReadyNAS server.
ReadyNAS Username	The user name to access the ReadyNAS. By default, the user name is admin.
ReadyNAS Password	The password to access the ReadyNAS. By default, the password is netgear1.

1. Click **Apply** to save your settings.

> **Note:** For additional information about how to set up a UTM9S with a
>   ReadyNAS, see *Appendix D, ReadyNAS Integration*.

Configure the Quarantine Settings

You can apply the quarantine settings only after you have integrated a ReadyNAS with the UTM9S (see the previous section).

➢ **To configure the quarantine settings:**

1. Select **Administration > ReadyNAS Integration > Quarantine Settings**. The Quarantine Settings screen displays:

Figure 250.

2. To enable the UTM9S to quarantine files, select the **Yes** radio button.

---

3. Enter the settings as explained in the following table:

Table 103. Quarantine settings

Setting	Description
Allow anonymous users to check quarantined mails	Select this check box to allow anonymous users to view their quarantined emails. Anonymous users do not log in to the UTM: the UTM's default email and web access policies apply to them. For information about how anonymous users can log in to view their quarantined emails, see *Unauthenticated or Anonymous Users* on page 348. If this check box is cleared, only administrative users and users with guest privileges can view quarantined emails and spam messages.
Malware Quarantine Area Size	The amount of storage space that is reserved for quarantined malware. The default is 100 MB; the maximum is 512 MB.
Spam Quarantine Area Size	The amount of storage space that is reserved for quarantined spam. The default is 100 MB; the maximum is 1024 MB.
Quarantine Lifetime	The period that the quarantined files remain saved. The default period is 10 days; the maximum period is 30 days.
Quarantine Directory	The directory on the ReadyNAS where the quarantined files are saved.

4. Click **Apply** to save your settings.

Monitoring System Access and Performance

This chapter describes the system-monitoring features of the UTM. You can be alerted to important events such as a WAN port rollover, WAN traffic limits reached, login failures, and attacks. You can also view status information about the firewall, WAN ports, LAN ports, active VPN users and tunnels, and more. In addition, the diagnostics utilities are described. This chapter contains the following sections:

- *Enable the WAN Traffic Meter*
- *Configure Logging, Alerts, and Event Notifications*
- *Monitor Real-Time Traffic, Security, and Statistics*
- *View Status Screens*
- *Query the Logs*
- *Query the Quarantine Logs (UTM9S Only)*
- *View, Schedule, and Generate Reports*
- *Use Diagnostics Utilities*

Note: The Quarantine configuration menu shows on the UTM9S only, accessible under the Monitoring main navigation menu.

Note: All log and report functions that are part of the Logs & Reports screen and some of the functions that are part of the Diagnostics screen require that you configure the email notification server—see *Configure the Email Notification Server* on page 422.

Note: For all UTM models except for the UTM9S, the Email Notification configuration menu is accessible under the Network Config main navigation menu. On the UTM9S, the Email Notification configuration menu is accessible under the Monitoring main navigation menu.

Enable the WAN Traffic Meter

If your ISP charges by traffic volume over a given period of time, or if you want to study traffic types over a period of time, you can activate the traffic meter for one or more WAN ports.

➢ **To monitor traffic limits on each of the WAN ports:**

1. Select **Network Config > WAN Metering**. On the multiple WAN port models, the WAN Metering tabs display, with the WAN1 Traffic Meter screen in view (the following figure shows the WAN1 Traffic Meter screen of the UTM50). On the single WAN port models, the WAN Traffic Meter screen displays.

   The Internet Traffic Statistics section in the lower part of the screen displays statistics on Internet traffic through the WAN port. If you have not enabled the traffic meter, these statistics are not available.

Figure 251.

2. Enter the settings as explained in the following table:

Table 104. WAN traffic meter settings

Setting	Description
Enable Traffic Meter	
Do you want to enable Traffic Metering on WAN1? (multiple WAN port models) or Do you want to enable Traffic Metering on WAN? (single WAN port models)	Select one of the following radio buttons to configure traffic metering: • **Yes**. Traffic metering is enabled, and the traffic meter records the volume of Internet traffic passing through the WAN1 interface (multiple WAN port models) or WAN interface (single WAN port models). Complete the fields that are shown on the right side of the screen (see explanations later in this table). • **No**. Traffic metering is disabled. This is the default setting.

Setting	Description	
	Select one of the following radio buttons to specify if or how the UTM applies restrictions when the traffic limit is reached: • **No Limit**. No restrictions are applied when the traffic limit is reached. • **Download only**. Restrictions are applied to incoming traffic when the traffic limit is reached. Fill in the Monthly Limit field. • **Both Directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached. Fill in the Monthly Limit field.	
	Monthly Limit	Enter the monthly traffic volume limit in MB. The default setting is 0 MB.
	Increase this month limit by	Select this check box to temporarily increase a previously specified monthly traffic volume limit, and enter the additional allowed volume in MB. The default setting is 0 MB. **Note:** When you click Apply to save these settings, this field is reset to 0 MB so that the increase is applied only once.
	This month limit	This is a nonconfigurable field that displays the total monthly traffic volume limit that is applicable to this month. This total is the sum of the monthly traffic volume and the increased traffic volume.

Setting	Description
Traffic Counter	
Restart Traffic Counter	Select one of the following radio buttons to specify when the traffic counter restarts: • **Restart Traffic Counter Now**. Select this option, and click **Apply** at the bottom of the screen to restart the traffic counter immediately. • **Restart Traffic Counter at a Specific Time**. Restart the traffic counter at a specific time and day of the month. Fill in the time fields, and select **AM** or **PM** and the day of the month from the drop-down lists.
Send e-mail report before restarting counter	An email report is sent immediately before the counter restarts. Ensure that emailing of logs is enabled on the Email and Syslog screen (see *Configure Logging, Alerts, and Event Notifications* on page 422).

Table 104. WAN traffic meter settings (continued)

Setting	Description
When Limit is reached	
Block Traffic	Select one of the following radio buttons to specify which action the UTM performs when the traffic limit has been reached: • **Block All Traffic**. All incoming and outgoing Internet and email traffic is blocked. • **Block All Traffic Except E-Mail**. All incoming and outgoing Internet traffic is blocked, but incoming and outgoing email traffic is still allowed.
Send e-mail alert	An email alert is sent when traffic is blocked. Ensure that emailing of logs is enabled on the Email and Syslog screen (see *Configure and Activate System, Email, and Syslog Logs* on page 423).

3. Click **Apply** to save your settings.

4. For the multiple WAN port models only, click the **WAN2 Traffic Meter**, **WAN3 Traffic Meter** (UTM150 only), or **WAN4 Traffic Meter** (UTM150 only) submenu tab to display the corresponding WAN Traffic Meter screen. These screens are identical to the WAN1 Traffic Meter screen (see *Figure 251* on page 419).

5. For the multiple WAN port models only, repeat *step 2* and *step 3* for the additional WAN interface or interfaces.

To display a report of the Internet traffic by type, click the **Traffic by Protocol** option arrow in the upper right of the WAN Traffic Meter screen (single WAN port models) or in the upper right of one of the WAN Traffic Meter screens (multiple WAN port models). The Traffic by Protocol screen displays in a pop-up screen. The incoming and outgoing volume of traffic for each protocol and the total volume of traffic are displayed. Traffic counters are updated in MBs; the counter starts only when traffic passed is at least 1 MB. In addition, the pop-up screen displays the traffic meter's start and end dates.
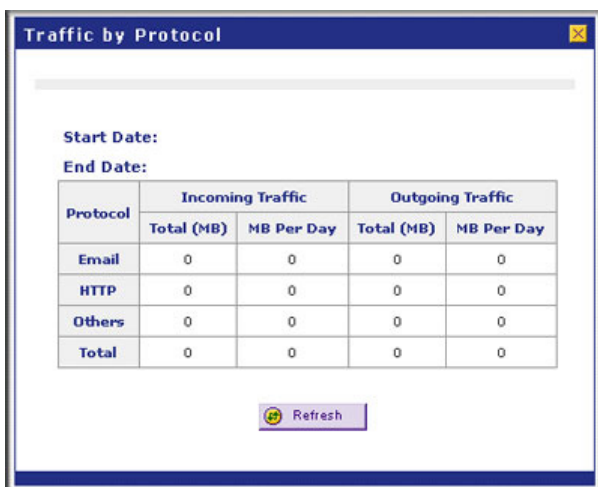
Figure 252.

Configure Logging, Alerts, and Event Notifications

By default, the UTM logs security-related events such as accepted and dropped packets on different segments of your LAN, denied incoming and outgoing service requests, hacker probes and login attempts, content-filtering events such as attempts to access blocked sites and URLs, unwanted email content, spam attempts, and many other types of events. You can configure the UTM to email logs and alerts to a specified email address.

> ⚠️ **WARNING!**
>
> **When you reboot the UTM, the logs are lost. If you want to save the logs, make sure that you configure the UTM to send the logs to a syslog server. For information about how to do this, see *Configure and Activate System, Email, and Syslog Logs* on page 423.**

For you to receive the logs in an email message, the UTM's email notification server needs to be configured, and email notification needs to be enabled. If the email notification server is not configured or email notification is disabled, you can still query the logs and generate log reports that you then can view on the web management interface screen or save in CSV format.

The logging, alerts, and event notifications are described in the following sections:

• *Configure the Email Notification Server*

• *Configure and Activate System, Email, and Syslog Logs*

• *How to Send Syslogs over a VPN Tunnel between Sites*

• *Configure and Activate Update Failure and Attack Alerts*

• *Configure and Activate Firewall Logs*

For more information about logs, see *Query the Logs* on page 460.

Configure the Email Notification Server

The UTM can automatically send information such as notifications and reports to the administrator. You need to configure the necessary information for sending email, such as the administrator's email address, email server, user name, and password.

➢ **To configure the email notification server:**

1. The menu selection to access the Email Notification screen depends on the UTM model:
   • On the UTM5, UTM10, UTM25, UTM50, and UTM150, select **Network Config > Email Notification**.
   • On the UTM9S, select **Monitoring > Email Notification**.

   The Email Notification screen displays. (The following figure shows an example.)
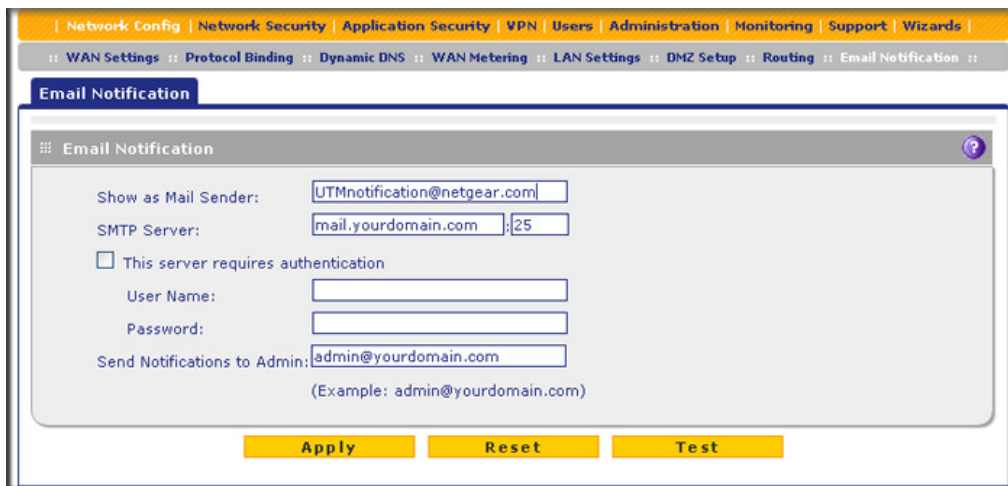
Figure 253.

2. Enter the settings as explained in the following table:

Table 105. Email Notification screen settings

Setting	Description
Show as Mail Sender	A descriptive name of the sender for email identification purposes. For example, enter UTMnotification@netgear.com.
SMTP Server	The IP address and port number or Internet name and port number of your ISP's outgoing email SMTP server. The default port number is 25. **Note:** If you leave this field blank, the UTM cannot send email notifications.
This server requires authentication	If the SMTP server requires authentication, select the **This server requires authentication** check box, and enter the user name and password.
	User Name	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.
Send Notifications to Admin	The email address to which the notifications should be sent. Typically, this is the email address of the administrator.

3. Click **Test** to ensure that the connection to the server and email address succeeds.

4. Click **Apply** to save your settings.

Configure and Activate System, Email, and Syslog Logs

You can configure the UTM to log system events such as a change of time by an NTP server, secure login attempts, reboots, and other events. You can also send logs to the administrator or schedule logs to be sent to the administrator or to a syslog server on the network. In addition, the Email and Syslog screen provides the option to selectively clear logs.

➢ **To configure and activate logs:**

1. Select **Monitoring > Logs & Reports**. The Logs & Reports submenu tabs display, with the Email and Syslog screen in view:
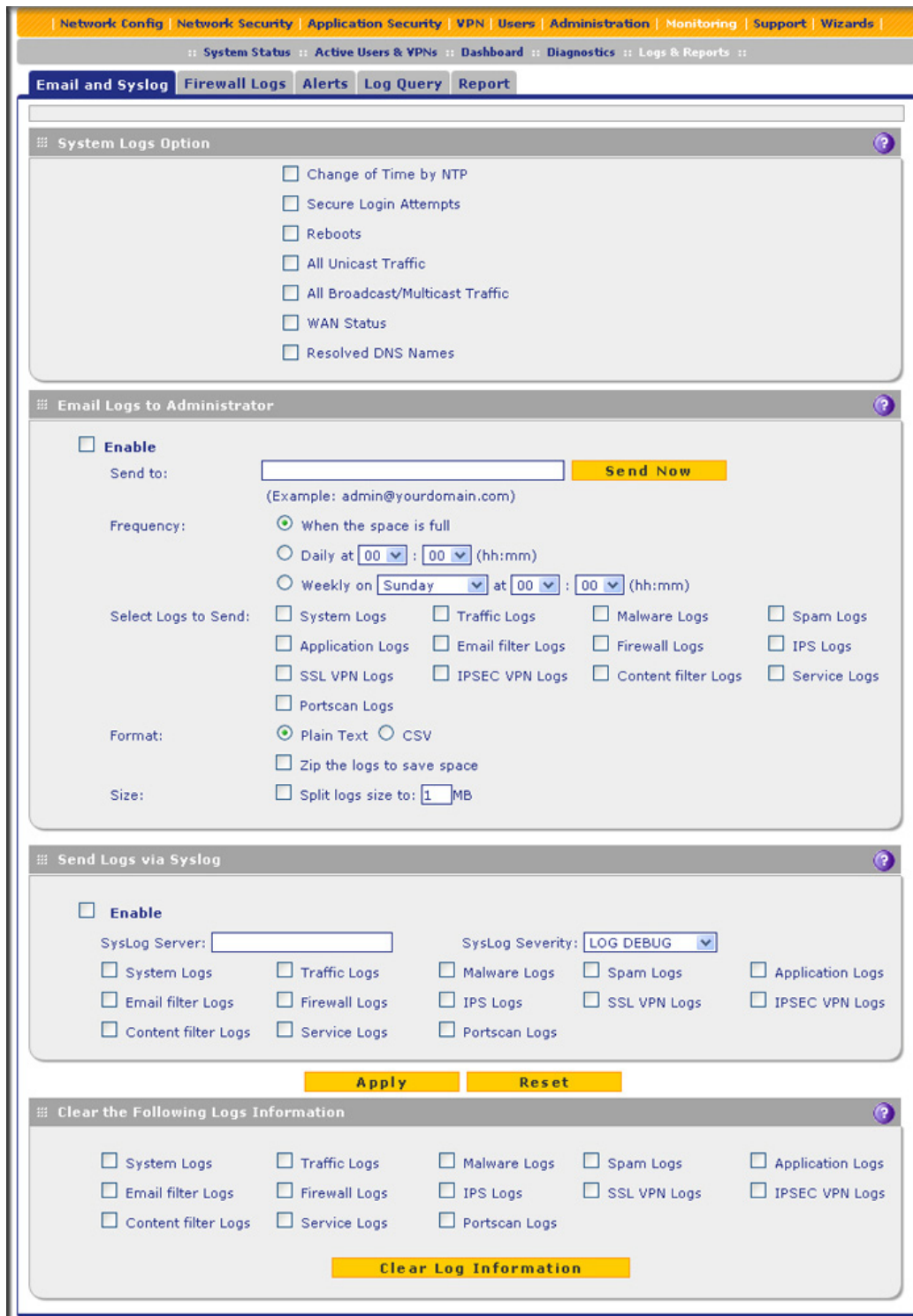
Figure 254.

2. Enter the settings as explained in the following table:

Table 106. Email and Syslog screen settings

Setting	Description
System Logs Option	
Select the check boxes to specify which system events are logged: • **Change of Time by NTP**. Logs a message when the system time changes after a request from an NTP server. • **Secure Login Attempts**. Logs a message when a secure login is attempted. Both successful and failed login attempts are logged. • **Reboots**. Logs a message when the UTM has been rebooted through the web management interface. (No message is logged when the factory default reset button has been pressed.) • **All Unicast Traffic**. All incoming unicast packets are logged. • **All Broadcast/Multicast Traffic**. All incoming broadcast and multicast packets are logged. • **WAN Status**. WAN link status–related events are logged. • **Resolved DNS Names**. All resolved DNS names are logged.	
Email Logs to Administrator	
Note: For the UTM9S only, when you have integrated a ReadyNAS with the UTM9S, the UTM9S cannot send the logs to an email address.	

Enable		Select this check box to enable the UTM to send a log file to an email address.
	Send to	The email address of the recipient of the log file. Click **Send Now** to immediately send the logs, which you first need to specify in the *Select Logs to Send* subsection (see later in this table).
	Frequency	Select a radio button to specify how often the log file is sent: • **When the space is full**. Logs are sent when the storage space that is assigned to the logs is full. (This option is not available for the UTM9S.) • **Daily**. Logs are sent daily at the time that you specify from the drop-down lists (hours and minutes). • **Weekly**. Logs are sent weekly at the day and time that you specify from the drop-down lists (weekday, hours, and minutes).
	Select Logs to Send	Select the check boxes to specify which logs are sent by email: • **System Logs**. The system event logs that you have specified in the System Logs Options section at the top of the screen. However, by default, many more types of events are logged in the system logs. • **Traffic Logs**. All scanned incoming and outgoing traffic. • **Malware Logs**. All intercepted viruses and malware threats. • **Spam Logs**. All intercepted spam. • **Application Logs**. All instant messaging, peer-to-peer and media applications, and tools access violations. • **Email filter Logs**. All emails that are blocked because of file extension and keyword violations. • **Firewall Logs**. The firewall logs that you have specified on the Firewall Logs screen (see *Configure and Activate Firewall Logs* on page 432).

Table 106. Email and Syslog screen settings (continued)

Setting	Description	
Enable (continued)	Select Logs to Send (continued)	• **IPS Logs**. All IPS events. • **SSL VPN Logs**. All SSL VPN events. • **IPSEC VPN Logs**. All IPSec VPN events. • **Content Filter Logs**. All attempts to access blocked websites and URLs. • **Service Logs**. All events that are related to the status of scanning and filtering services that you access from the Application Security main navigation menu. These events include update success messages, update failed messages, network connection errors, and so on. • **Portscan Logs**. All port scan events.
	Format	Select a radio button to specify the format in which the log file is sent: • **Plain text**. The log file is sent as a plain text file. • **CSV**. The log file is sent as a comma-separated values (CSV) file.
		Select the **Zip the logs to save space** check box to enable the UTM to compress the log file.
	Size	Select the **Split logs size to** check box to break up the log file into smaller files, and specify the maximum size of each file in MB.
Send Logs via Syslog		
Enable	Select this check box to enable the UTM to send a log file to a syslog server.	
	SysLog Server	The IP address or name of the syslog server.
	SysLog Severity	All the logs with a severity that is equal to and above the severity that you specify are logged on the specified syslog server. For example, if you select LOG_CRITICAL as the severity, then the logs with the severities LOG_CRITICAL, LOG_ALERT, and LOG_EMERG are logged. Select one of the following syslog severities from the drop-down list: • **LOG EMERG**. The UTM is unusable. • **LOG ALERT**. An action has to be taken immediately. • **LOG CRITICAL**. There are critical conditions. • **LOG ERROR**. There are error conditions. • **LOG WARNING**. There are warning conditions. • **LOG NOTICE**. There are normal but significant conditions. • **LOG INFO**. Informational messages. • **LOG DEBUG**. Debug-level messages.
	Logs	Select the check boxes to specify which logs are sent through the syslog server. The Send Logs via Syslog section of the screen lists the same check boxes as the Select Logs to Send subsection in the Email Logs to Administrator section of the screen (see earlier in this table).
Clear the Following Logs Information		
Select the check boxes to specify which logs are cleared. The Clear the Following Logs Information section of the screen lists the same check boxes as the *Select Logs to Send* subsection in the *Email Logs to Administrator* section of the screen (see earlier in this table).		

3. Click **Apply** to save your settings, or click **Clear Log Information** to clear the selected logs.

How to Send Syslogs over a VPN Tunnel between Sites

➢ **To send syslogs from one site to another over a gateway-to-gateway VPN tunnel:**

1. At Site 1, set up a syslog server that is connected to Gateway 1.

2. Set up a VPN tunnel between Gateway 1 at Site 1 and Gateway 2 at Site 2.

3. Change the remote IP address in the VPN policy on Gateway 1 to the WAN IP address of Gateway 2.

4. Change the local IP address in the VPN policy on Gateway 2 to the WAN IP address of Gateway 2.

5. At Site 2, specify that Gateway 2 should send the syslogs to the syslog server at Site 1.

This section describes steps 2 through 4, using the topology that is described in the following table:

Type of address	Gateway 1 at Site 1	Gateway 2 at Site 2
WAN IP address	10.0.0.1	10.0.0.2
LAN IP address	192.168.10.0	192.168.20.0
LAN subnet mask	255.255.255.0	255.255.255.0
LAN IP address syslog server	192.168.10.2	not applicable

Configure Gateway 1 at Site 1

➢ **To create a gateway-to-gateway VPN tunnel to Gateway 2, using the IPSec VPN wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays.

2. Configure a gateway-to-gateway VPN tunnel using the following information:
   - Connection name. Any name of your choice
   - Pre-shared key. Any key of your choice
   - Remote WAN IP address. 10.0.0.2
   - Local WAN IP address. 10.0.0.1
   - Remote LAN IP Address. 192.168.20.0
   - Remote LAN subnet mask. 255.255.255.0

3. Click **Apply** to save the settings.

➢ **To change the remote IP address in the VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policy screen displays.

2. Next to the policy name for the Gateway 1–to–Gateway 2 autopolicy, click **Edit**. The Edit VPN Policy screen displays.

3. In the General section of the screen, clear the **Enable NetBIOS** check box.
4. In the Traffic Selector section of the screen, make the following changes:
   - From the Remote IP drop-down list, select **Single**.
   - In the Start IP fields, type **10.0.0.2**, which is the WAN IP address of Gateway 2.
5. Click **Apply** to save the settings.

Configure Gateway 2 at Site 2

➢ **To create a gateway-to-gateway VPN tunnel to Gateway 1, using the IPSec VPN wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays.
2. Configure a gateway-to-gateway VPN tunnel using the following information:
   - Connection name. Any name of your choice
   - Pre-shared key. The same key as you configured on Gateway 1
   - Remote WAN IP address. 10.0.0.1
   - Local WAN IP address. 10.0.0.2
   - Remote LAN IP Address. 192.168.10.0
   - Remote LAN subnet mask. 255.255.255.0
3. Click **Apply** to save the settings.

➢ **To change the local IP address in the VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policy screen displays.
2. Next to the policy name for the Gateway 2–to–Gateway 1 autopolicy, click **Edit**. The Edit VPN Policy screen displays.
3. In the General section of the screen, clear the **Enable NetBIOS** check box.
4. In the Traffic Selector section of the screen, make the following changes:
   - From the Local IP drop-down list, select **Single**.
   - In the Start IP fields, type **10.0.0.2**, which is the WAN IP address of Gateway 2.
5. Click **Apply** to save the settings.

➢ **To specify the syslog server that is connected to Gateway 1:**

1. Select **Monitoring > Logs & Reports > Email and Syslog** to display the Email and Syslog screen)
2. Enable the syslog server and specify its IP address at Site 1. Enter **192.168.10.2** as the IP address.
3. Click **Apply** to save the settings.

> **Note:** The VPN tunnel should be established automatically, and the syslogs should be sent to the syslog server at Site 1. You can use the IPSec VPN Connection Status screen to verify the connection.

Configure and Activate Update Failure and Attack Alerts

You can configure the UTM to send an email alert when a failure, malware attack, malware outbreak attack, Intrusion Prevention System (IPS) attack, or IPS outbreak attack occurs. Six types of alerts (seven types for the UTM9S) are supported:

- **Update failure alert**. Sent when an attempt to update any component such as a pattern file or scan engine firmware fails.
- **Malware alert**. Sent when the UTM detects a malware threat.
- **ReadyNAS failure alert** (UTM9S only). Sent when an integrated ReadyNAS is down or disconnected.
- **License expiration alert**. Sent when one or more licenses (web protection, email protection, support and maintenance) are near their expiration dates and when they expire.
- **Malware outbreak alert**. Sent when the malware outbreak criteria that you have configured are reached or exceeded. Outbreak criteria are based on the number of malware threats detected within a specified period of time.
- **IPS alert**. Sent when the UTM detects an attack.
- **IPS outbreak alert**. Sent when the IPS outbreak criteria that you have configured are reached or exceeded. Outbreak criteria are based on the number of IPS attacks detected within a specified period of time.

> **To configure and activate the email alerts:**

1. Select **Monitoring > Logs & Reports > Alerts**. The Alerts screen displays:
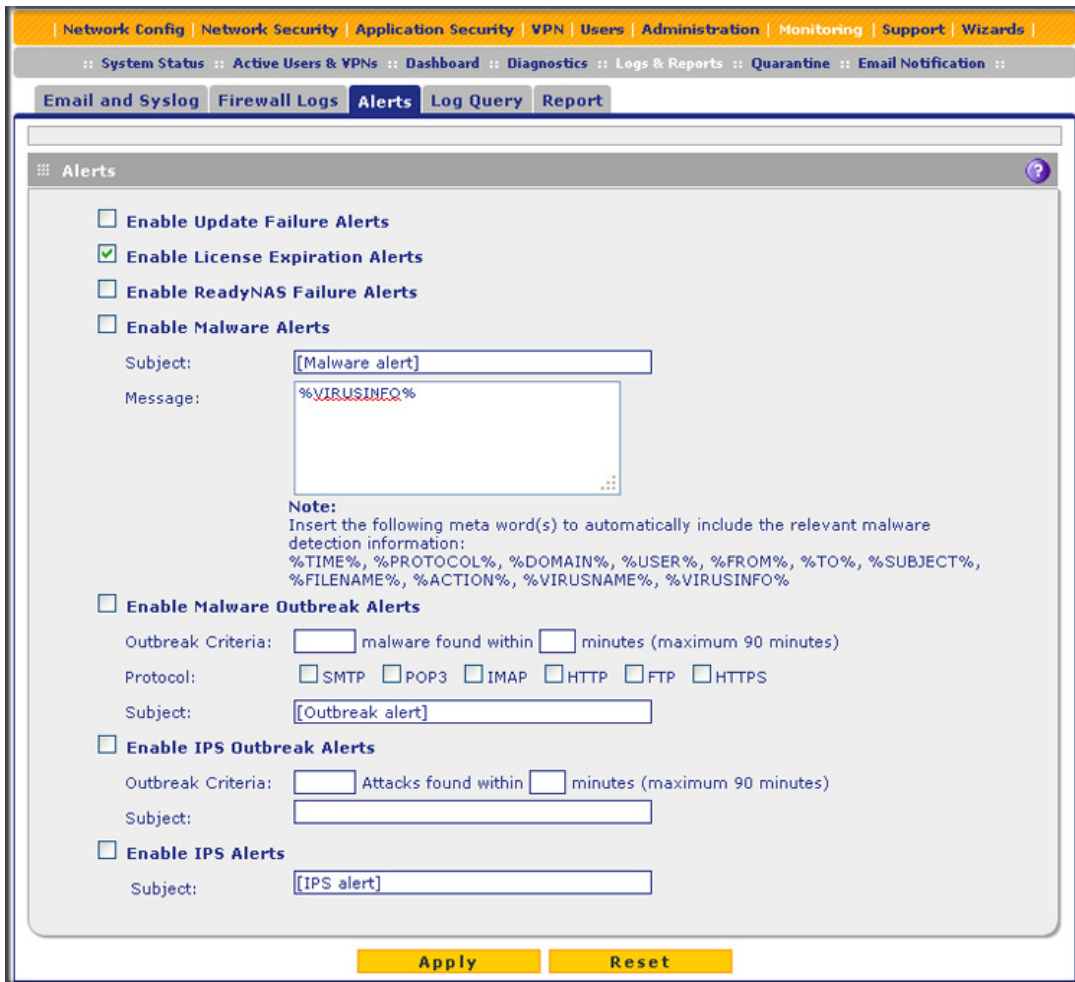
Figure 255.

2. Enter the settings as explained in the following table:

Table 107. Alerts screen settings

Setting	Description
Enable Update Failure Alerts	Select this check box to enable update failure alerts.
Enable License Expiration Alerts	Select this check box to enable license expiration alerts. This check box is selected by default.
Enable ReadyNAS Failure Alerts	Select this check box to enable ReadyNAS failure alerts. This check box is selected by default. **Note:** This option is shown on the Alerts screen of the UTM9S only.

Table 107. Alerts screen settings (continued)

Setting	Description	
Enable Malware Alerts	Select this check box to enable malware alerts, and fill in the Subject and Message fields.	
	Subject	Enter the subject line for the email alert. The default text is [Malware alert].
	Message	Enter the content for the email alert. **Note:** Make sure that you keep the %VIRUSINFO% and %TIME% metawords in a message to enable the UTM to insert the correct malware name and time information. In addition to these metaword, you can insert the following metawords in your customized message: %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.
Enable Malware Outbreak Alerts	Select this check box to enable malware outbreak alerts, and fill in the Outbreak Criteria, Protocol, and Subject fields.	
	Outbreak Criteria	To define a malware outbreak, fill in the following fields: • **malware found within**. The number of malware threats that are detected. • **minutes (maximum 90 minutes)**. The period in which the specified number of malware threats are detected. **Note:** When the specified number of detected malware threats is reached within the time threshold, the UTM sends a malware outbreak alert.
	Protocol	Select the check box or check boxes to specify the protocols (SMTP, POP3, IMAP, HTTP, FTP, and HTTPS) for which malware threats are detected.
	Subject	Enter the subject line for the email alert. The default text is [Outbreak alert].
Enable IPS Outbreak Alerts	Select this check box to enable malware outbreak alerts, and fill in the Outbreak Criteria and Subject fields.	
	Outbreak Criteria	To define an IPS outbreak, fill in the following fields: • **Attacks found within**. The number of IPS attacks that are detected. • **minutes (maximum 90 minutes)**. The period in which the specified number of IPS attacks are detected. **Note:** When the specified number of IPS attacks is reached within the time threshold, the UTM sends a malware outbreak alert.
	Subject	Enter the subject line for the email alert. The default text is [Outbreak alert].
Enable IPS Alerts	Select this check box to enable IPS alerts, and fill in the Subject field.	
	Subject	Enter the subject line for the email alert. The default text is [IPS alert].

3. Click **Apply** to save your settings.

Configure and Activate Firewall Logs

You can configure the logging options for each network segment. For example, the UTM can log accepted packets for LAN-to-WAN traffic, dropped packets for WAN-to-DMZ traffic, and so on. You can also configure logging of packets from MAC addresses that match the source MAC address filter settings (see *Enable Source MAC Filtering* on page 164), and packets that are dropped because the session limit (see *Set Session Limits* on page 150), bandwidth limit (see *Create Bandwidth Profiles* on page 160), or both, have been exceeded.

Note: Enabling firewall logs might generate a significant volume of log messages. NETGEAR recommends that you enable firewall logs for debugging purposes only.

➢ **To configure and activate firewall logs:**

1. Select **Monitoring > Logs & Reports > Firewall Logs**. The Firewall Logs screen displays:

Figure 256.

2. Enter the settings as explained in the following table:

Table 108. Firewall Logs screen settings

Setting	Description
Routing Logs	
In the Accepted Packets and Dropped Packets columns, select check boxes to specify which traffic is logged: • **LAN to WAN** • **LAN to DMZ** • **DMZ to WAN** • **WAN to LAN** • **DMZ to LAN** • **WAN to DMZ** • **VLAN to VLA**N	
Other Event Logs	
Source MAC Filter	Select this check box to log packets from MAC addresses that match the source MAC address filter settings.
Session Limit	Select this check box to log packets that are dropped because the session limit has been exceeded.
Bandwidth Limit	Select this check box to log packets that are dropped because the bandwidth limit has been exceeded.

3. Click **Apply** to save your settings.

Monitor Real-Time Traffic, Security, and Statistics

The Dashboard screen lets you monitor the real-time security scanning status with detected network threats, detected network traffic, and service statistics for the six supported protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP). In addition, the screen displays statistics for the most recent five and top five malware threats detected, IPS signatures matched, applications blocked, web categories blocked, and spam emails blocked.

To display the Dashboard screen, select **Monitoring > Dashboard**. Because of the size of the Dashboard screen, it is divided and presented in this manual in three figures (the following figure, *Figure 258* on page 436, and *Figure 259* on page 438), each with its own table that explains the fields.

Except for setting the poll interval and clearing the statistics, you cannot configure the fields on the Dashboard screen. Any changes need to be made on other screens.

> **Note:** Adobe Flash Player 10 or later is required to display the graphics.
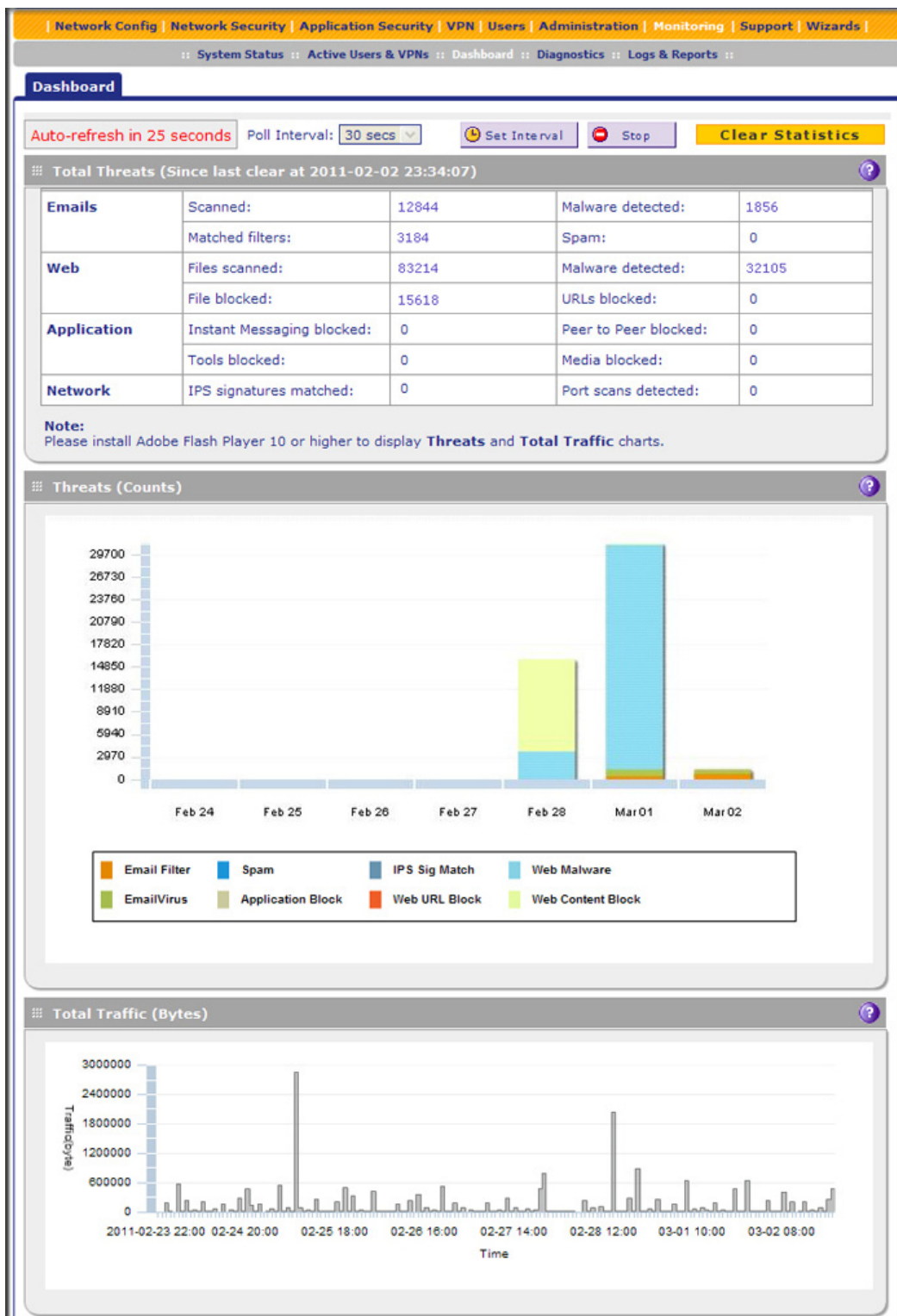
Figure 257. Dashboard, screen 1 of 3

To clear the statistics, click **Clear Statistics**.

➢ **To set the poll interval:**

1. Click the **Stop** button.

2. From the Poll Interval drop-down list, select a new interval. The minimum is 5 seconds; the maximum is 5 minutes.

3. Click the **Set Interval** button.

The following table explains the fields of the Total Threats, Threats (Counts), and Total Traffic (Bytes) sections of the Dashboard screen:

Table 109. Dashboard screen: threats and traffic information

Item	Description
Total Threats	
Emails	Displays the total number of: • Scanned emails. • Viruses (malware) detected. For information about how to configure these settings, see *Customize Email Antivirus and Notification Settings* on page 179. • Emails that matched filters. For information about how to configure these settings, see *Email Content Filtering* on page 183. • Spam. For information about how to configure these settings, see *Protect Against Email Spam* on page 186. • Quarantined emails, attachments, and objects (UTM9S only, information is not shown in the previous figure). For information about how to configure these settings, see *Customize Email Antivirus and Notification Settings* on page 179 and *Configure Distributed Spam Analysis* on page 191.
Web	Displays the total number of: • Files scanned. • Malware detected. For information about how to configure these settings, see *Configure Web Malware Scans* on page 197. • Files blocked. For information about how to configure these settings, see *Configure Web Content Filtering* on page 199. • URLs blocked. For information about how to configure these settings, see *Configure Web URL Filtering* on page 206. • Quarantined web files and objects (UTM9S only, information is not shown in the previous figure). For information about how to configure these settings, see *Configure Web Malware Scans* on page 197 and *Configure FTP Scans* on page 219.
Applications	Displays the total number of: • Instant messages blocked. • Peer-to-peer file-sharing applications blocked. • Web tools blocked. • Media applications blocked. For information about how to configure these settings, see *Customize Web Protocol Scan Settings and Services (Web Applications)* on page 194.

Table 109. Dashboard screen: threats and traffic information (continued)

Item	Description
Network	Displays the total number of: • IPS attack signatures matched. • Port scans detected. For information about how to configure these settings, see *Use the Intrusion Prevention System* on page 172.
Threats (Counts)	
This is a graphic that shows the relative number of threats and access violations over the last week, using different colors for the various components, most of which are self-explanatory: Email Filter, Spam, IPS Sig Match (which stands for IPS signatures matched), Web Malware, Email Virus, Application Block, Web URL Block, and Web Content Block.	
Total Traffic (Bytes)	
This is a graphic that shows the relative number of traffic in bytes over the last week.	
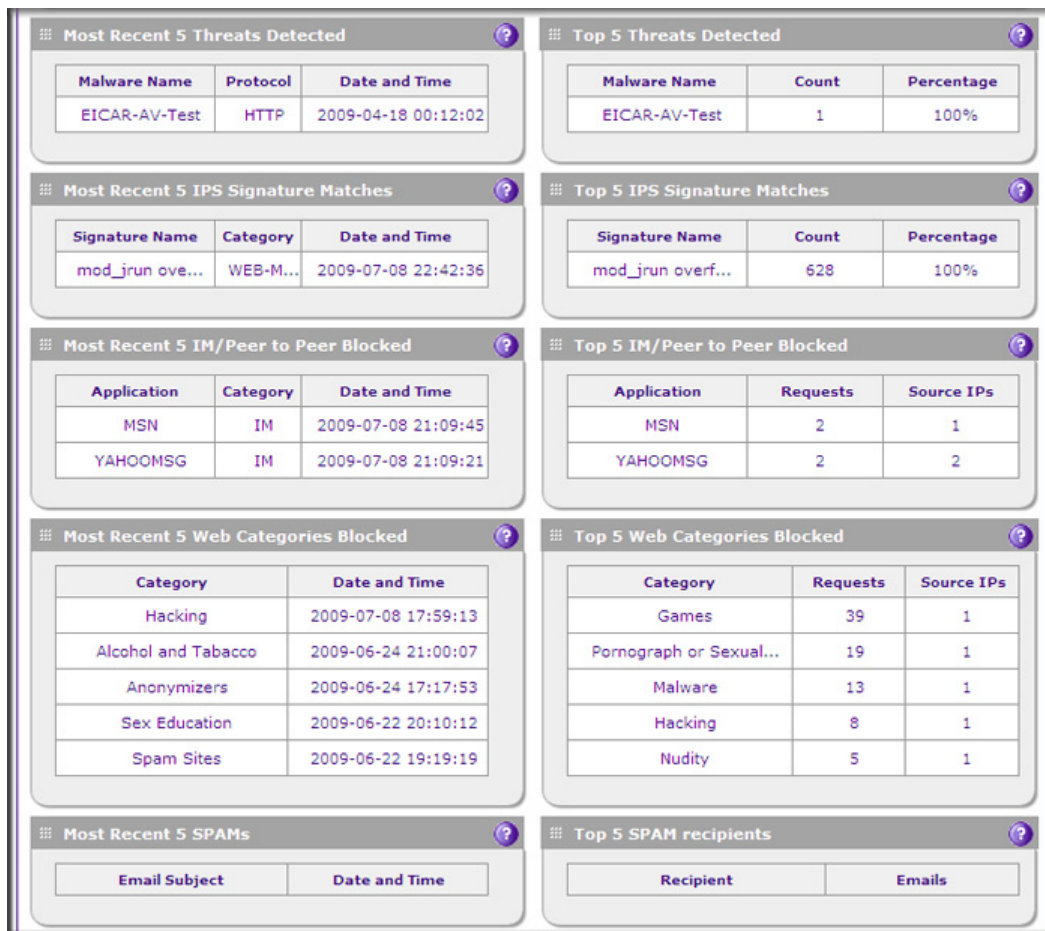
Figure 258. Dashboard, screen 2 of 3

The following table explains the fields of the Most Recent 5 and Top 5 sections of the Dashboard screen:

Table 110. Dashboard screen: most recent 5 threats and top 5 threats information

Category	Most recent 5 threats description	Top 5 threats description
Threats	• **Malware Name**. The name of the malware threat. • **Protocol**. The protocol in which the malware threat was detected. • **Date and Time**. The date and time that the malware threat was detected.	• **Malware Name**. The name of the malware threat. • **Count**. The number of times that the malware threat was detected. • **Percentage**. The percentage that the malware threat represents in relation to the total number of detected malware threats.
IPS Signatures	• **Signature Name**. The name of the attack. • **Category**. The category in which the attack was detected, such as Web, Mail, Databases, and so on. (For more information about categories, see *Use the Intrusion Prevention System* on page 172.) • **Date and Time**. The date and time that the attack was detected.	• **Signature Name**. The name of the attack. • **Count**. The number of times that the attack was detected. • **Percentage**. The percentage that the attack represents in relation to the total number of detected attacks.
Applications	• **Application**. The name of the application that was blocked. • **Category**. Instant messaging or peer-to-peer. • **Date and Time**. The date and time that the application request was blocked.	• **Application**. The name of the application that was blocked. • **Requests**. The total number of user requests for the blocked application. • **Source IPs**. The source IP address from which the request came.
Web Categories	• **Category**. The web category that was blocked. (For more information about web categories, see *Configure Web Content Filtering* on page 199.) • **Date and Time**. The date and time that the web request was blocked.	• **Category**. The web category that was blocked. (For more information about web categories, see *Configure Web Content Filtering* on page 199.) • **Requests**. The total number of user requests for the blocked web category. • **Source IPs**. The source IP address from which the request came.
Spam	• **Email Subject**. The email subject line in the spam message. • **Date and Time**. The date and time that the spam message was detected.	• **Recipient**. The intended recipient of the spam message. • **Emails**. The number of spam messages for the intended recipient.

Figure 259. Dashboard, screen 3 of 3

The following table explains the fields of the Service Statistics section of the Dashboard screen:

Table 111. Dashboard screen: service statistics information

Item	Description
For each of the six supported protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP), this section provides the following statistics:	
Total Scanned Traffic (MB)	The total quantity of scanned traffic in MB.
Total Emails/Files Scanned	The total number of scanned emails.
Total Malwares Found	The total number of detected viruses and attacks.
Total Files Blocked	The total number of files that were blocked from being downloaded.
Total URLs Blocked	The total number of URL requests that were blocked. These statistics are applicable only to HTTP and HTTPS.
Total Malware Quarantined	UTM9S only (information is not shown in the previous figure). The total number of viruses (attachments, objects and web files) that were quarantined.
Total Spam Quarantined	UTM9S only (information is not shown in the previous figure). The total number of spam messages that were quarantined.

Table 111. Dashboard screen: service statistics information (continued)

Item	Description	
Total Spam Emails	The total number of spam messages that were blocked. These statistics are applicable only to SMTP and POP3.	
	Blacklist	The total number of emails that were detected from sources on the spam blacklist (see *Set Up the Whitelist and Blacklist* on page 187). These statistics are applicable only to SMTP and POP3.
	RBL	The total number of emails that were detected from sources on the real-time blacklist (see *Configure the Real-Time Blacklist* on page 189). These statistics are applicable only to SMTP.
	Distributed Spam Analysis	The total number of spam messages that were detected through distributed spam analysis (see *Configure Distributed Spam Analysis* on page 191). These statistics are applicable only to SMTP and POP3.

View Status Screens

The UTM provides real-time information in a variety of status screens that are described in the following sections:

- *View the System Status*
- *View the Active VPN Users*
- *View the VPN Tunnel Connection Status*
- *View the Port Triggering Status*
- *View the WAN Ports Status*
- *View Attached Devices and the DHCP Log*

View the System Status

When you start up the UTM, the default screen that displays is the System Status screen.

The System Status screen, Network Status screen, Router Statistics screen, Detailed Status screen, VLAN Status screen, and xDSL statistics screen (UTM9S only) provide real-time information about the following important components of the UTM:

- CPU, memory, and hard disk status
- ReadyNAS and quarantine status (UTM9S only, information is not shown on the following screen)
- Services status (indicating whether or not the protocols are scanned for malware) and the number of active connections per service
- Firmware versions and update information of the UTM, software versions and update information of the components, license expiration dates for each type of license, and hardware serial number

- WAN and LAN port information
- Interface statistics
- VLAN status, including port memberships
- xDSL statistics

These status screens are described in the following sections:

- *View the System Status Screen*
- *View the Network Status Screen*
- *View the Router Statistics Screen*
- *View the Wireless Statistics Screen (UTM9S Only)*
- *View the Detailed Status Screen*
- *View the VLAN Status Screen*
- *View the xDSL Statistics Screen (UTM9S Only)*

View the System Status Screen

To view the System Status screen, select **Monitoring > System Status**. The System Status tabs display, with the System Status screen in view:
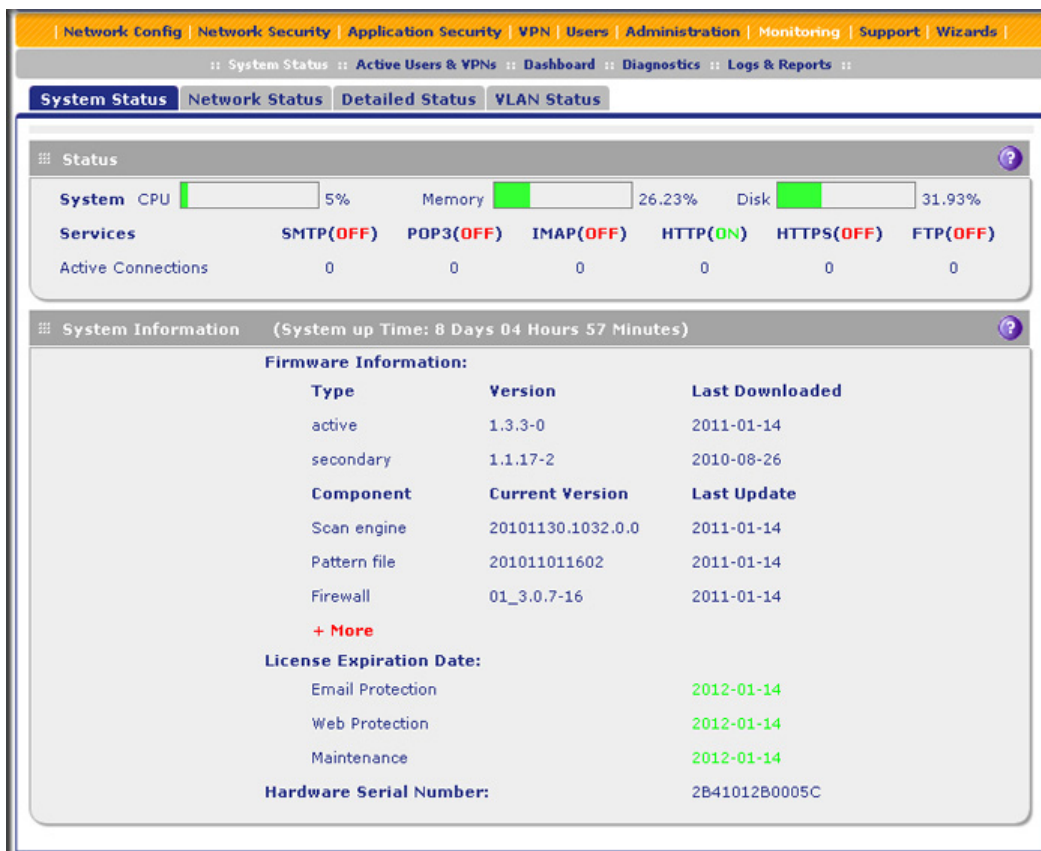
Figure 260.
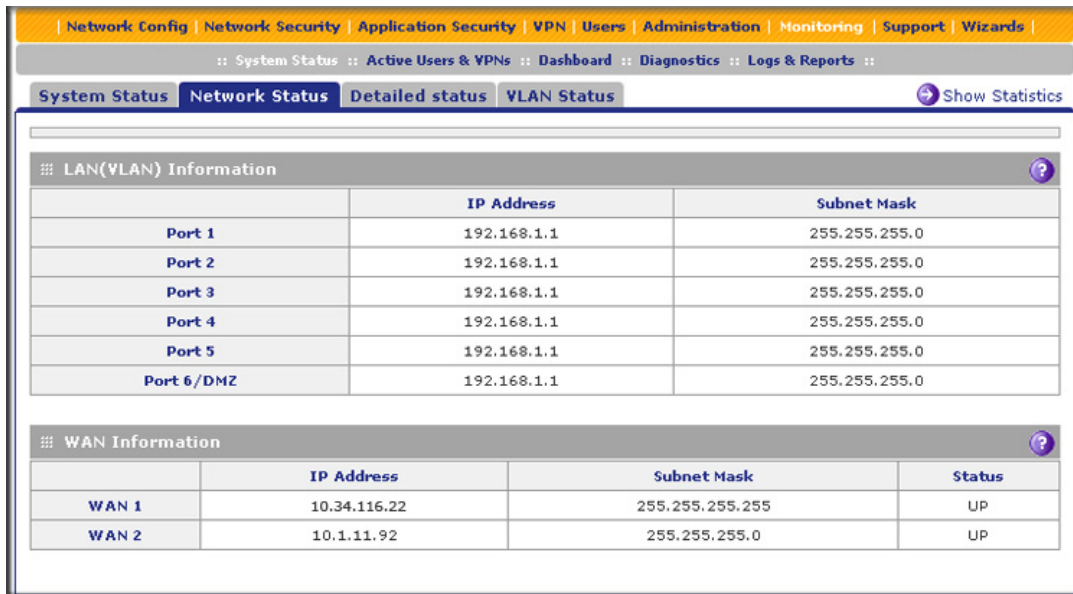
The following table explains the fields of the System Status screen:

Table 112. System Status screen fields

Item	Description
Status	
System	The current CPU, memory, and hard disk usage. When usage is within safe limits, the status bars show green.
ReadyNAS Status	UTM9S only (information is not shown on the previous screen). The status of the ReadyNAS connection (ON or OFF).
Quarantine Status	UTM9S only (information is not shown on the previous screen). The status of the quarantine area (ON or OFF).
Services	The protocols that are being scanned for malware threats (ON or OFF is stated next to the protocol) and the number of active connections for each protocol.
System Information States the system up time since last reboot.	
Firmware Information	The versions and most recent downloads for the active and secondary firmware of the UTM, the scan engine, pattern file, and firewall. Click **+ More** to display the versions and most recent downloads for the DC agent, SSE engine, SSE pattern, Mini engine, Mini pattern, Update client, IPS engine, IPS rules, Scand, and Urld.
License Expiration Date	The license expiration dates for the email protection, web protection, and maintenance licenses. **Note:** When a license has expired, the license expiration date is displayed in red font.
Hardware Serial Number	The hardware serial number of the UTM.

View the Network Status Screen

To view the Network Status screen, select **Monitoring > System Status > Network Status**. The Network Status screen displays. (The following figure shows the Network Status screen of the UTM50. The Network Status screen of the UTM9S also shows the available wireless access point, and has a Wireless Statistics option arrow in the upper right of the screen.)

Figure 261.

The following table explains the fields of the Network Status screen:

Table 113. Network Status screen fields

Item	Description
LAN (VLAN) Information	
For each of the LAN ports, the screen shows the IP address and subnet mask. For more detailed information, see *Table 116* on page 447.	
WAN Information	
For each of the WAN ports, the screen shows the IP address, subnet mask, and status of the port (UP or DOWN). For more detailed information, see *Table 116* on page 447.	

View the Router Statistics Screen

➢ **To view the Router Statistics screen:**

1. Select **Monitoring > System Status > Network Status**. The Network Status screen displays.

2. Click the **Show Statistics** option arrow in the upper right of the Network Status screen. The Router Statistics screen displays. (The following figure shows the Router Statistics screen of the UTM50.)
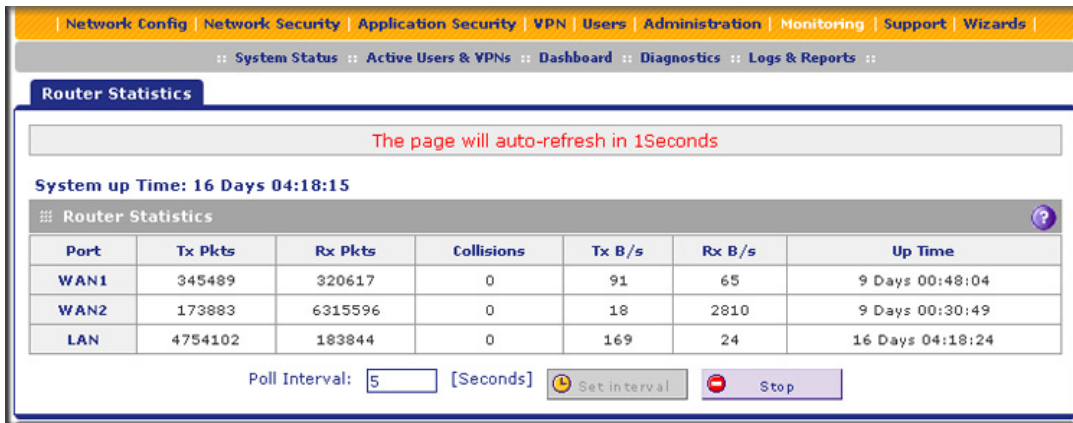
Figure 262.

The following table explains the fields of the Router Statistics screen.

To change the poll interval period, enter a new value in the Poll Interval field, and then click **Set interval**. To stop polling, click **Stop**.

Table 114. Router Statistics screen fields

Item	Description
System up Time. The period since the last time that the UTM was started up.	
Router Statistics	
For each of the WAN interfaces, for the DSL interface (UTM9S only, not shown on the previous figure), and for all LAN interfaces combined, the following statistics are displayed:	
Tx Pkts	The number of packets transmitted on the port in bytes.
Rx Pxts	The number of packets received on the port in bytes.
Collisions	The number of signal collisions that have occurred on the port. A collision occurs when the port attempts to send data at the same time as a port on the other router or computer that is connected to this port.
Tx B/s	The number of bytes transmitted per second on the port.
Rx B/s	The number of bytes received per second on the port.
Up Time	The period that the port has been active since it was restarted.

View the Wireless Statistics Screen (UTM9S Only)

> **To view the Wireless Statistics screen:**

1. Select **Monitoring > System Status > Network Status**. The Network Status screen displays.

2. Click the **Wireless Statistics** option arrow in the upper right of the Network Status screen. The Wireless Statistics screen displays:
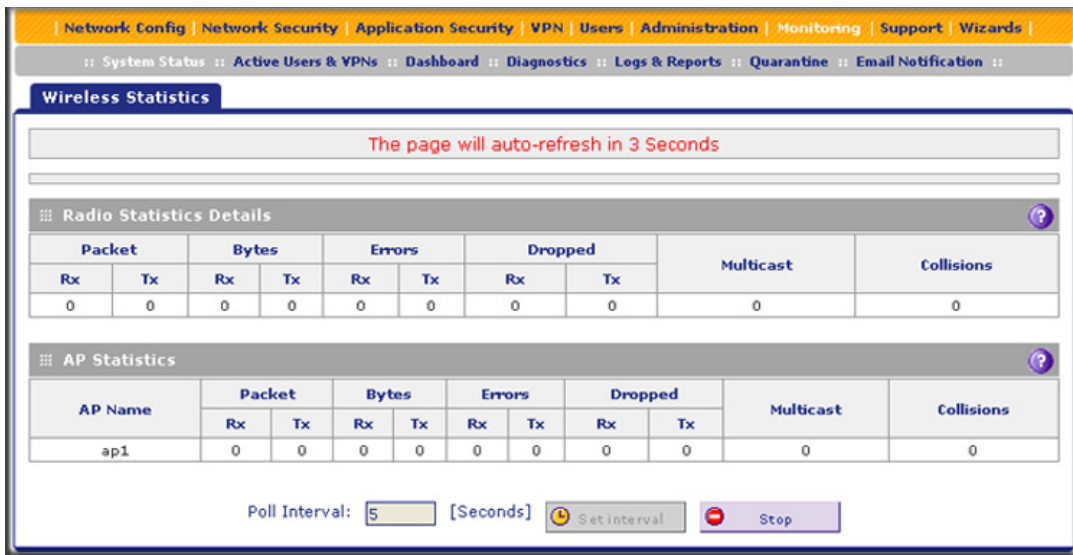
Figure 263.

The following table explains the fields of the Wireless Statistics screen.

To change the poll interval period, enter a new value in the Poll Interval field, and then click **Set interval**. To stop polling, click **Stop**.

Table 115. Wireless Statistics screen fields

Item	Description
Radio Statistics Details	
Packets	The number of received (Rx) and transmitted (Tx) packets on the radio in bytes.
Bytes	The number of received (Rx) and transmitted (Tx) bytes on the radio.
Errors	The number of received (Rx) and transmitted (Tx) errors on the radio.
Dropped	The number of received (Rx) and transmitted (Tx) dropped packets on the radio.
Multicast	The number of received (Rx) and transmitted (Tx) multicast packets on the radio.
Collisions	The number of signal collisions that have occurred on the radio. A collision occurs when the radio attempts to send data at the same time as a wireless station that is connected to the radio.

Table 115. Wireless Statistics screen fields (continued)

Item	Description
AP Statistics	
AP Name	The name for the virtual access point (VAP) is ap1.
Packets	The number of received (Rx) and transmitted (Tx) packets on the access point in bytes.
Bytes	The number of received (Rx) and transmitted (Tx) bytes on the access point.
Errors	The number of received (Rx) and transmitted (Tx) errors on the access point.
Dropped	The number of received (Rx) and transmitted (Tx) dropped packets on the access point.
Multicast	The number of received (Rx) and transmitted (Tx) multicast packets on the access point.
Collisions	The number of signal collisions that have occurred on the access point. A collision occurs when the access point attempts to send data at the same time as a wireless station that is connected to the access point.

Note: For information about clients that are connected to the access point, see *View the Access Point Status and Connected Clients* on page 546.

View the Detailed Status Screen

To view the Detailed Status screen, select **Monitoring > System Status > Detailed Status**. The Detailed Status screen displays. (The following figure shows the Detailed Status screen of the UTM50.)

Figure 264.

The UTM9S also shows SLOT-1 Info and SLOT-2 Info sections at the bottom of the Detailed Status screen:
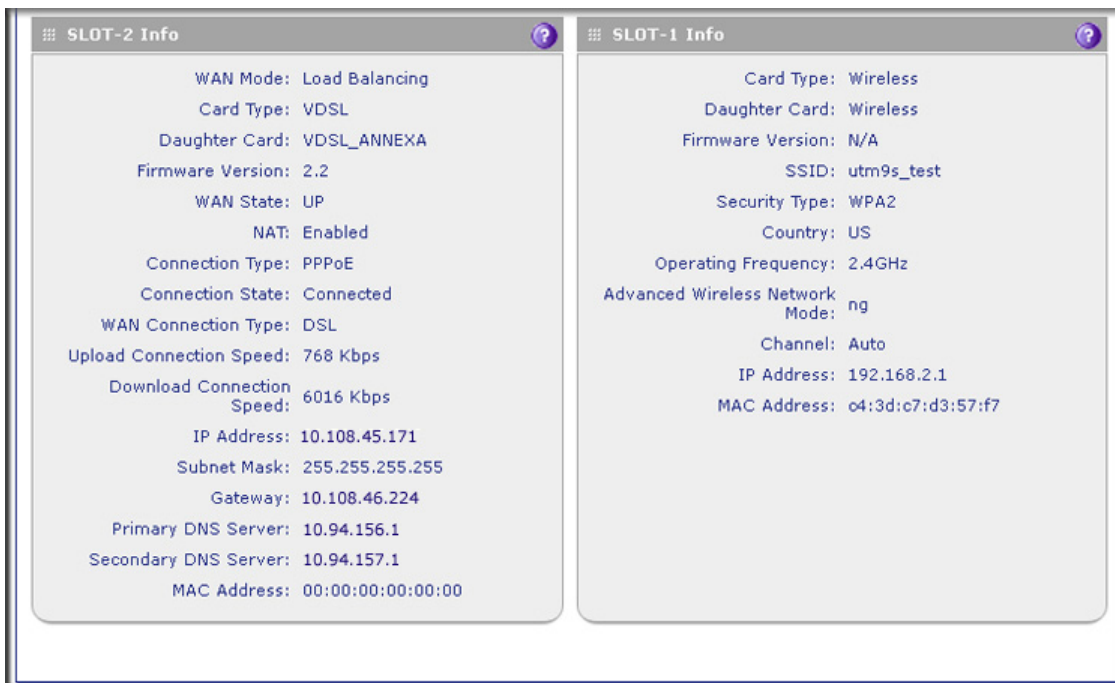
Figure 265. SLOT-1 Info and SLOT-2 Info sections (UTM9S only)

The following table explains the fields of the Detailed Status screen:

Table 116. Detailed Status screen fields

Item	Description
LAN Port Configuration The following fields are shown for each of the LAN ports.	
VLAN Profile	The name of the VLAN profile that you assigned to this port on the LAN Setup screen (see *Assign and Manage VLAN Profiles* on page 95). If the VLAN is not enabled on this port, the default profile (with VLAN ID 1) is assigned automatically.
VLAN ID	The VLAN ID that you assigned to this port on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 98). If the default VLAN profile is used, the VLAN ID is 1, which means that all tagged and untagged traffic can pass on this port.
MAC Address	The MAC address of this port. All LAN ports share the same MAC address if they are part of the default VLAN. However, if LAN port 4 (UTM5, UTM10, UTM25, and UTM150) or LAN port 6 (UTM50) is enabled as the DMZ port, its MAC address is changed to the MAC address of the WAN2 interface plus 1. (For example, if the MAC address of the WAN2 interface is 00:26:f2:b5:db:80, the MAC address of the DM port is 00:26:f2:b5:db:81.) For information about configuring the DMZ port, see *Configure and Enable the DMZ Port* on page 112.
IP Address	The IP address for this port. If the VLAN is not enabled on this port, the IP address is the default LAN IP address (192.168.1.1). For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 98.

Table 116. Detailed Status screen fields (continued)

Item	Description
Subnet Mask	The subnet mask for this port. If the VLAN is not enabled on this port, the subnet mask is the default LAN IP subnet mask (255.255.255.0). For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 98.
DHCP Status	The status can be either DHCP Enabled or DHCP Disabled. For information about enabling DHCP for this port, see *Configure a VLAN Profile* on page 98.
WAN Info and xDSL information in SLOT-1 Info or SLOT-2 Info **Note:** For the UTM9S only: DSL information is shown in SLOT-1 Info or SLOT-2 Info section, depending on the slot in which the xDLS module is installed. All other fields that are shown in the SLOT-1 Info or SLOT-2 Info section are also shown in the WAN Info sections. The following fields are shown for each of the WAN ports and for the slot in which the xDSL module is installed:	
WAN Mode	The WAN mode can be Single Port, Load Balancing, or Auto Rollover. For information about configuring the WAN mode, see *Configure the WAN Mode* on page 75.
UTM9S only: Card Type	The configuration of the xDSL module: VDSL or ADSL.
UTM9S only: Daughter Card	The type of supported annex on the xDLS module: Annex A or Annex B (VDSL_ANNEXA, VDSL_ANNEXB, ADSL_ANNEXA, or ADSL_ANNEXB).
UTM9S only: Firmware Version	The firmware on the xDSL module.
WAN State	The WAN state can be either UP or DOWN, depending on whether the port is connected to the Internet and whether the port is enabled. For information about connecting WAN ports, see *Chapter 3, Manually Configuring Internet and WAN Settings*.
NAT	The NAT state can be either Enabled or Disabled, depending on whether NAT is enabled (see *Configure Network Address Translation (All Models)* on page 77) or classical routing is enabled (see *Configure Classical Routing (All Models)* on page 77).
Connection Type	The connection type can be Static IP, DHCP, PPPoE, or PPTP, depending on whether the WAN address is obtained dynamically through a DHCP server or assigned statically by you. For information about connection types, see *Manually Configure the Internet Connection* on page 71.
Connection State	The connection state can be either Connected or Not Connected, depending on whether the WAN port is physically connected to a modem or router. For information about connecting a WAN port, see the *ProSecure Unified Threat Management UTM Installation Guide*.
WAN Connection Type	The detected type of Internet connection that is used on this port. The WAN connection type can be DSL, ADSL, CableModem, T1, or T3.
Upload Connection Speed	The maximum upload speed that is provided by your ISP.
Download Connection Speed	The maximum download speed that is provided by your ISP.

Table 116. Detailed Status screen fields (continued)

Item	Description	
IP Address	The IP address of the WAN port.	These settings are either obtained dynamically from your ISP or specified by you on the WAN ISP Settings screen for this port (see *Manually Configure the Internet Connection* on page 71).
Subnet Mask	The subnet mask of the WAN port.	
Gateway	The IP address of the gateway.	
Primary DNS Server	The IP address of the primary DNS server.	
Secondary DNS Server	The IP address of the secondary DNS server.	
MAC Address	The default MAC address for the port or the MAC address that you have specified on the WAN Advanced Options screen for the port. For information about configuring the MAC address, see *Configure Advanced WAN Options* on page 90.	

Wireless information in SLOT-1 Info or SLOT-2 Info

Note: For the UTM9S only: Wireless information is shown in the SLOT-1 Info or SLOT-2 Info section, depending on the slot in which the wireless module is installed.

The following fields are shown for the wireless module:

Card Type	This is a fixed field that states Wireless.	
Daughter Card	This is a fixed field that states Wireless.	
Firmware Version	This is a fixed field that states N/A. This field might show a software version in a future release.	
SSID	The SSID of the wireless access point that you have specified on the Edit Profile screen. For information about configuring the SSID, see *Configure and Enable Wireless Security Profiles* on page 538.	
Security Type	The type of wireless security and encryption that you have specified on the Edit Profile screen. For information about configuring wireless security, see *Wireless Data Security Options* on page 534 and *Wireless Security Profile* on page 536.	
Country	The region and country that you have specified on the Radio Settings screen.	For information about configuring the basic wireless radio settings, see *Configure the Basic Radio Settings* on page 531.
Operating Frequency	The operating frequency that you have specified on the Radio Settings screen: 2.4 GHz or 5 GHz.	
Advanced Wireless Network Mode	The wireless mode that you have specified on the Radio Settings screen.	
Channel	The channel or automatic channel selection that you have specified on the Radio Settings screen.	
IP Address	The IP address of the default WLAN that is specified on the LAN Setup screen. For information about how to change the default WLAN IP address, see *Configure a VLAN Profile* on page 98.	
MAC Address	The MAC address for the wireless access point is a fixed address that is assigned to the wireless module.	

View the VLAN Status Screen

The VLAN Status screen displays information about the VLANs (both enabled and disabled) that are configured on the UTM. For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 98. For information about enabling and disabling VLAN profiles, see *Assign and Manage VLAN Profiles* on page 95.

To view the VLAN Status screen, select **Monitoring > System Status > VLAN Status**. The VLAN Status screen displays. (The following figure shows the VLAN Status screen of the UTM50.)

Figure 266.

The following table explains the fields of the VLAN Status screen:

Table 117. VLAN Status screen fields

Item	Description
Profile Name	The unique name for the VLAN that you have assigned on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 98).
VLAN ID	The identifier for the VLAN that you have assigned on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 98).
MAC Address	VLANs can have the same MAC address as the associated LAN port or can be assigned a unique MAC address, depending on the selection that you have made on the LAN Advanced screen (see *Configure VLAN MAC Addresses and Advanced LAN Settings* on page 103). If a VLAN is configured but disabled, the MAC address displays as 00:00:00:00:00:00.
Subnet IP	The IP address and subnet mask that you have assigned on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 98).
DHCP Status	The DHCP status for the VLAN, which can be either DHCP Enabled or DHCP Disabled, depending on the DHCP configuration that you have specified on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 98).
Port Membership	The ports that you have associated with the VLAN on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 98).

View the xDSL Statistics Screen (UTM9S Only)

To view the xDSL Statistics screen, select **Monitoring > System Status > xDSL Statistics**.
The xDSL Statistics screen displays:
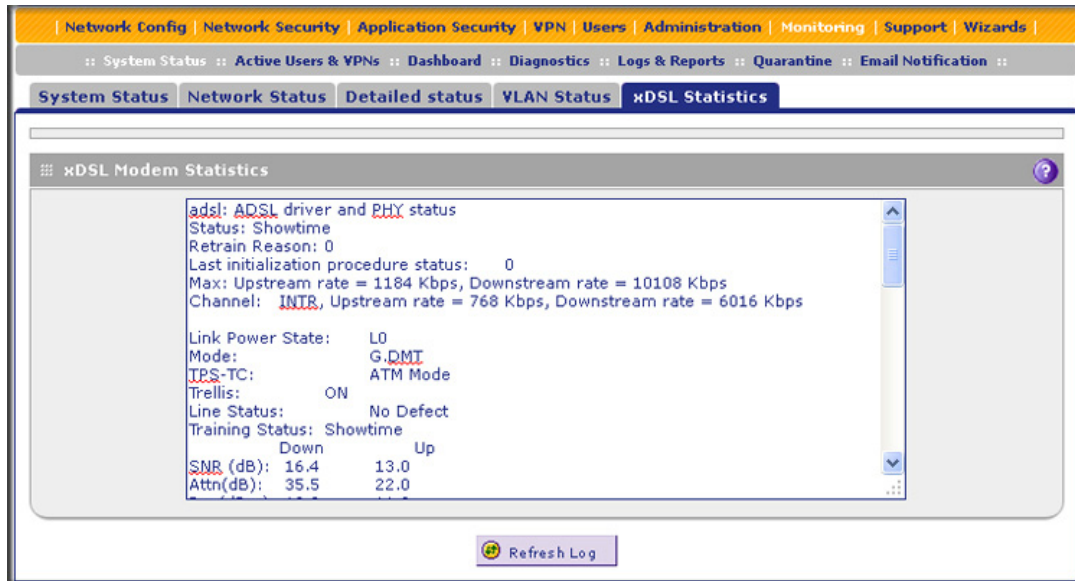
Figure 267.

View the Active VPN Users

The Active Users screen displays a list of administrators, IPSec VPN users, and SSL VPN
users that are currently logged in to the UTM.

To display the list of active VPN users, select **Monitoring > Active Users & VPNs**. The
Active Users & VPN submenu tabs display, with the Active Users screen in view:

Figure 268.

The active user's user name, group, and IP address are listed in the table with a time stamp
indicating the time and date that the user logged in.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table
entry.

View the VPN Tunnel Connection Status

To review the status of current IPSec VPN tunnels, select **Monitoring > Active Users & VPNs > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays:
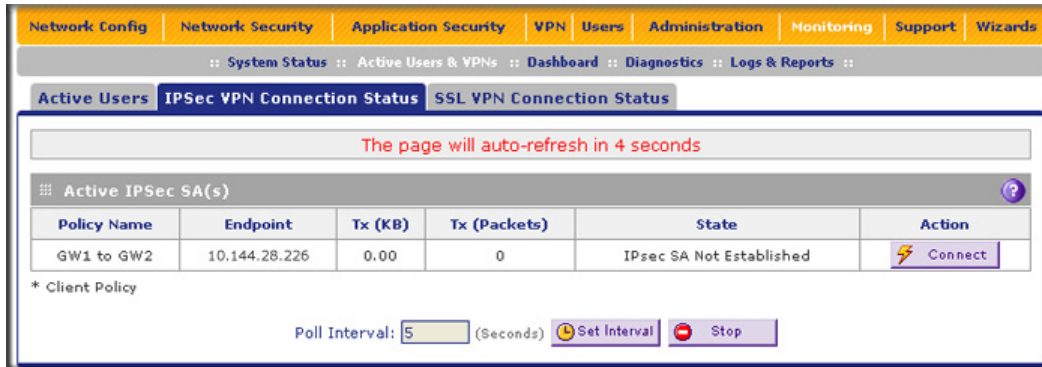
Figure 269.

The Active IPSec SA(s) table lists each active connection with the information that is described in the following table. The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and then click **Set Interval**. To stop polling, click **Stop**.

Table 118. IPSec VPN Connection Status screen information

Item	Description
Policy Name	The name of the VPN policy that is associated with this SA.
Endpoint	The IP address on the remote VPN endpoint.
Tx (KB)	The amount of data that is transmitted over this SA.
Tx (Packets)	The number of IP packets that are transmitted over this SA.
State	The current status of the SA. Phase 1 is the authentication phase, and Phase 2 is key exchange phase. If there is no connection, the status is IPSec SA Not Established.
Action	Click the **Connect** table button to build the connection, or click the **Disconnect** table button to terminate the connection.

To review the status of current SSL VPN tunnels, select **Monitoring > Active Users & VPNs > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:

Figure 270.

The active user's user name, group, and IP address are listed in the table with a time stamp indicating the time and date that the user connected.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

View the PPTP and L2TP Server Status (UTM9S Only)

To view the active PPTP tunnel users, select **Monitoring > Active Users & VPNs > PPTP Active Users**. The PPTP Active Users screen displays:
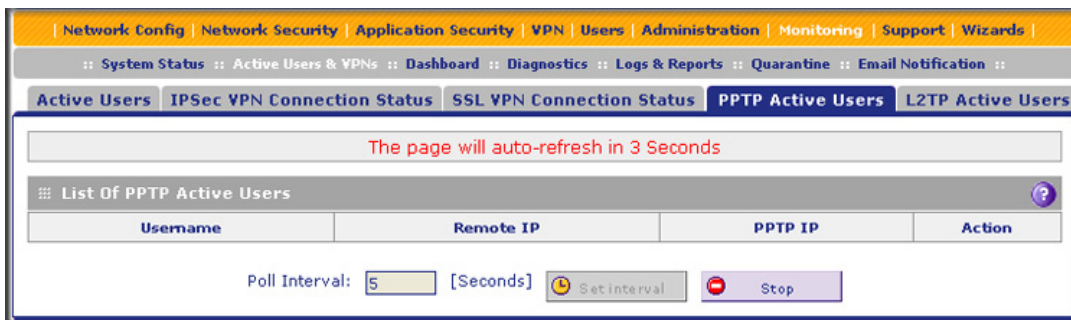
The List of PPTP Active Users table lists each active connection with the information that is described in the following table.

Table 119. PPTP Active Users screen information

Item	Description
Username	The name of the PPTP user that you have defined (see *Configure User Accounts* on page 362).
Remote IP	The remote client's IP address.
L2TP IP	The IP address that is assigned by the PPTP server on the UTM9S.
Action	This column is not applicable to PPTP.

The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and then click the **Set Interval** button. To stop polling, click the **Stop** button.

To view the active L2TP tunnel users, select **Monitoring > Active Users & VPNs > L2TP Active Users**. The L2TP Active Users screen displays:
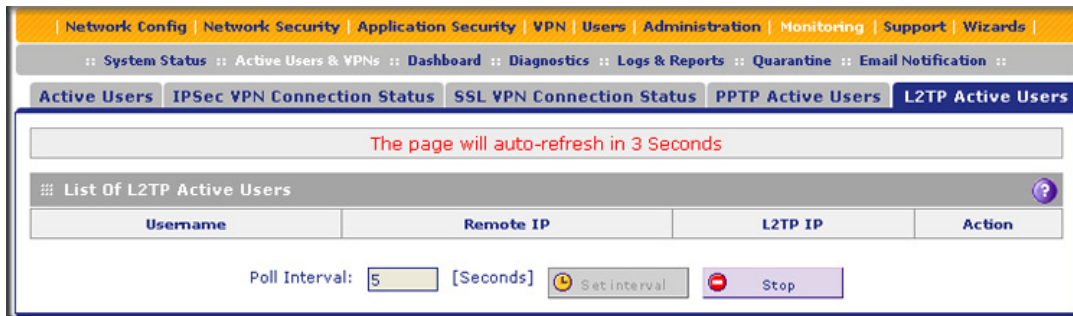
Figure 271.

The List of L2TP Active Users table lists each active connection with the information that is described in the following table.

Table 120. L2TP Active Users screen information

Item	Description
Username	The name of the L2TP user that you have defined (see *Configure User Accounts* on page 362).
Remote IP	The client's IP address on the remote LAC.
L2TP IP	The IP address that is assigned by the L2TP server on the UTM9S.
Action	This column is not applicable to L2TP.

The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and then click the **Set Interval** button. To stop polling, click the **Stop** button.

View the Port Triggering Status

➢ **To view the status of the port-triggering feature:**

1. Select **Network Security > Port Triggering**. The Port Triggering screen displays. (The following figure shows one rule in the Port Triggering Rules table as an example.)
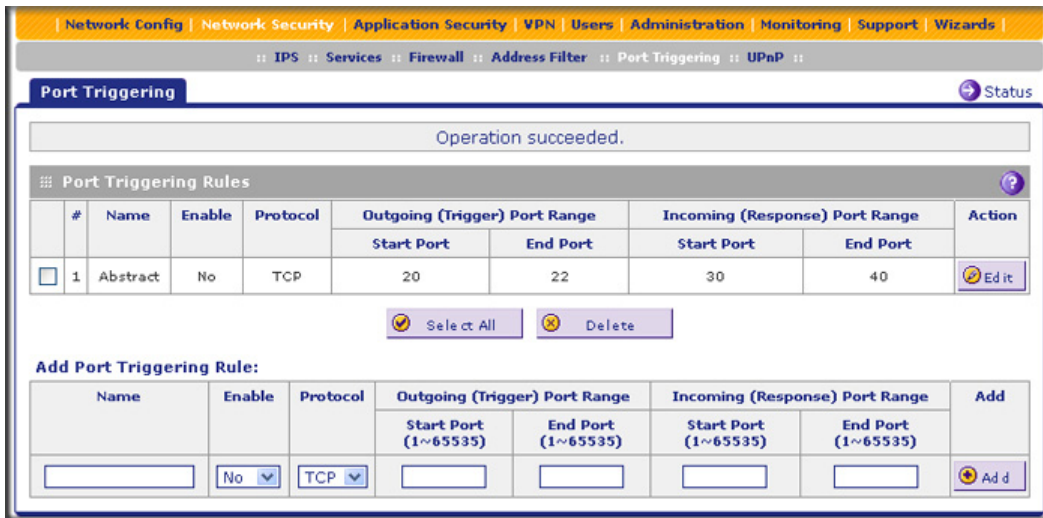
Figure 272.

2. Select the **Status** option arrow in the upper right of the Port Triggering screen. The Port Triggering Status screen displays in a pop-up screen.
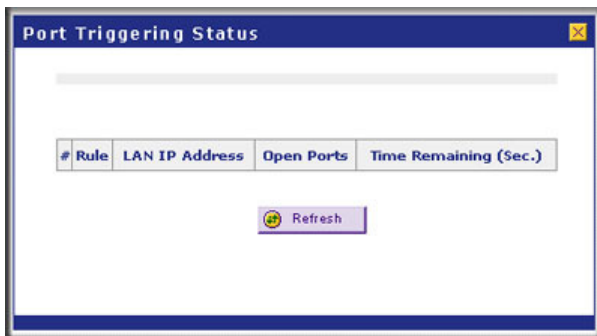
Figure 273.

The Port Triggering Status screen displays the information that is described in the following table:

Table 121. Port Triggering Status pop-up screen information

Item	Description
#	The sequence number of the rule on screen.
Rule	The name of the port-triggering rule that is associated with this entry.
LAN IP Address	The IP address of the computer or device that is currently using this rule.
Open Ports	The incoming ports that are associated with this rule. Incoming traffic using one of these ports is sent to the IP address that is listed in the LAN IP Address field.
Time Remaining	The time remaining before this rule is released and made available for other computers or devices. This timer is restarted when incoming or outgoing traffic is received.

View the WAN Ports Status

You can view the status of both of the WAN connections, the DNS servers, and the DHCP servers.

> **To view the status of the WAN1 port (multiple WAN port models) or WAN port (single WAN port models):**

1. Select **Network Config > WAN Settings**. The WAN screen displays (see *Figure 36* on page 68).
2. Click the **Status** button in the Action column for the WAN interface for which you want to view the status. The Connection Status screen displays in a pop-up screen.
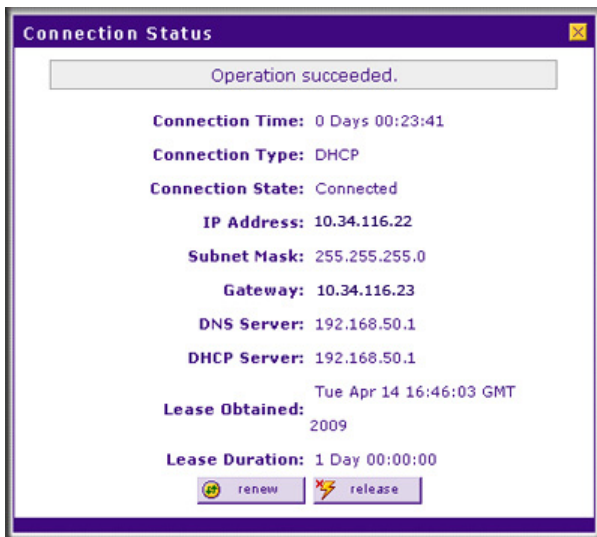
Figure 274.

The Connection Status screen displays the information that is described in the following table:

Table 122. Connection Status pop-up screen information

Item	Description
Connection Time	The period that the UTM has been connected through the WAN port.
Connection Type	The connection type can be either DHCP or Static IP.
Connection Status	The connection status can be either Connected or Disconnected.
IP Address	The addresses that were automatically detected or that you configured on the WAN ISP Setting screen (single WAN port models) or on one of the WAN ISP Settings screens (multiple WAN port models).
Subnet Mask	
Gateway	**Note:** For more information, see *Automatically Detecting and Connecting the Internet Connections* on page 67 and *Manually Configure the Internet Connection* on page 71.
DNS Server	

Table 122. Connection Status pop-up screen information (continued)

Item	Description
DHCP Server	The DHCP server that was automatically detected. This field displays only if your ISP does not require a login and the IP address is acquired dynamically from your ISP. You have configured these ISP settings on the WAN ISP Settings screen (single WAN port models) or on one of the WAN ISP Settings screens (multiple WAN port models). **Note:** For more information, see *Automatically Detecting and Connecting the Internet Connections* on page 67 and *Manually Configure the Internet Connection* on page 71.
Lease Obtained	The time when the DHCP lease was obtained.
Lease Duration	The period that the DHCP lease remains in effect.

Depending on the type of connections, any of the following buttons might display on the Connection Status screen:

- **Renew**. Click to renew the DHCP lease.
- **Release**. Click to disconnect the DHCP connection.
- **Disconnect**. Click to disconnect the static IP connection.

For the multiple WAN port models only, the procedure to view the status of other WAN ports is similar to the one for the WAN1 port. After you have selected **Network Config > WAN Settings**, click the **Status** button in the Action column for the selected WAN interface to display the Connection Status screen for that WAN interface.

View Attached Devices and the DHCP Log

The LAN Groups screen shows the network database, which is the Known PCs and Devices table, which contains all IP devices that UTM has discovered on the local network. The LAN Setup screen lets you access the DHCP log.

View Attached Devices

➢ **To view the attached devices in the LAN Groups screen:**

1. Select **Network Config > LAN Settings**. The LAN Settings submenu tabs display, with the LAN Setup screen in view. (The following figure shows some profiles in the VLAN Profiles table as an example.)
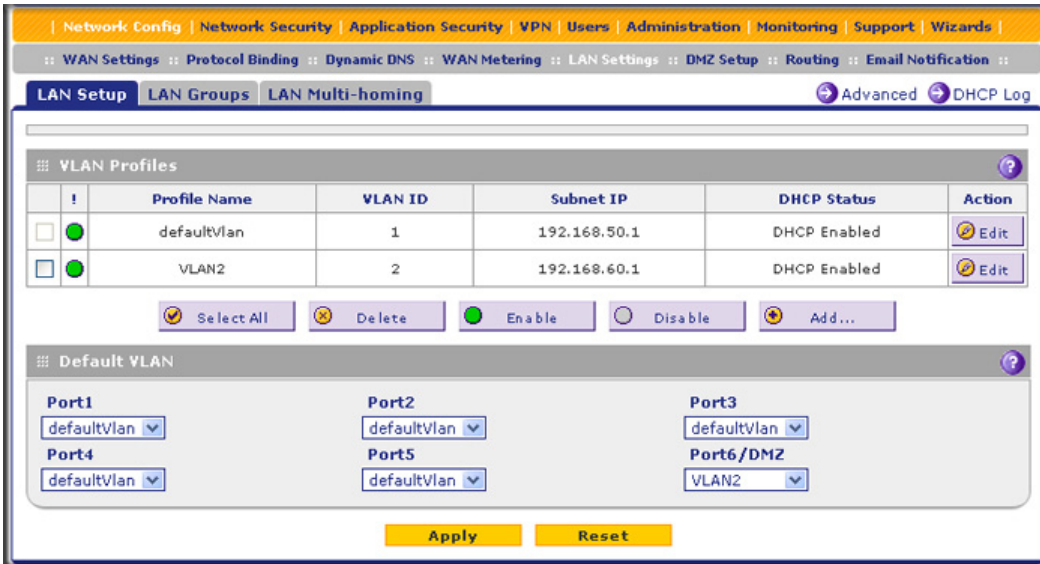
Figure 275.

2. Select the **LAN Groups** submenu tab. The LAN Groups screen displays. (The following figure shows some examples in the Known PCs and Devices table.)
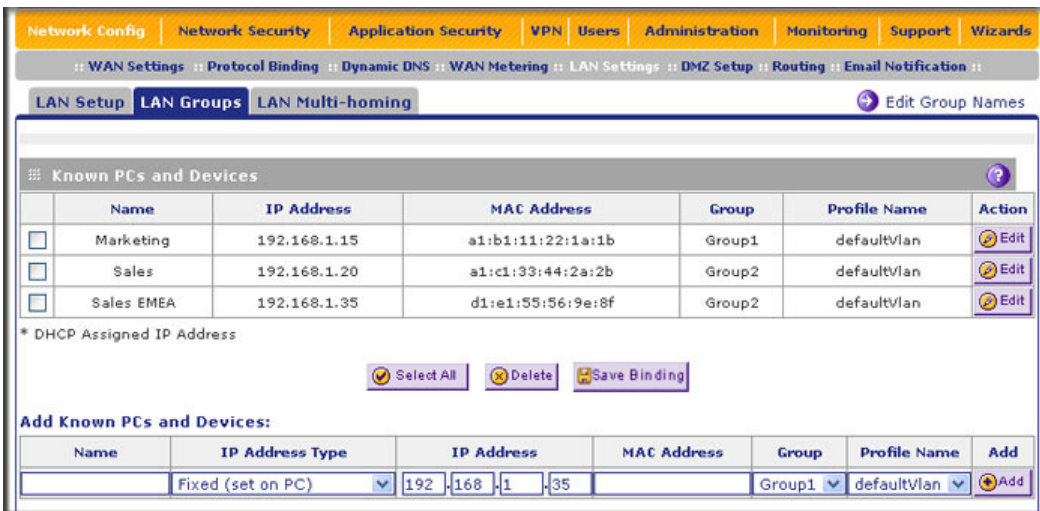
Figure 276.

The Known PCs and Devices table contains a list of all known PCs and network devices that are assigned dynamic IP addresses by the UTM, or have been discovered by other means. Collectively, these entries make up the network database.

For each attached PC or device, the Known PCs and Devices table displays the following fields:

- **Check box**. Allows you to select the PC or device in the table.
- **Name**. The name of the PC or device. For computers that do not support the NetBIOS protocol, the name is displayed as *Unknown* (you can edit the entry manually to add a

meaningful name). If the PC or device was assigned an IP address by the DHCP server, then the name is appended by an asterisk.

- **IP Address**. The current IP address of the PC or device. For DHCP clients of the UTM, this IP address does not change. If a PC or device is assigned a static IP address, you need to update this entry manually after the IP address on the PC or device has changed.

- **MAC Address**. The MAC address of the PC or device's network interface.

- **Group**. Each PC or device can be assigned to a single LAN group. By default, a PC or device is assigned to Group 1. You can select a different LAN group from the Group drop-down list in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen.

- **Action**. The **Edit** table button, which provides access to the Edit Groups and Hosts screen.

Note: If the UTM is rebooted, the data in the Known PCs and Devices table is lost until the UTM rediscovers the devices.

View the DHCP Log

Note: There is no separate DHCP log on the UTM9S. To view the DHCP entries on the UTM9S, query the system logs (see *Query the Logs* on page 460).

➢ **To review the most recent entries in the DHCP log:**

1. Select **Network Config > LAN Settings**. The LAN Settings submenu tabs display, with the LAN Setup screen in view (see *Figure 275* on page 458).

2. Click the **DHCP Log** option arrow in the upper right of the LAN Setup screen. The DHCP Log displays in a pop-up screen:
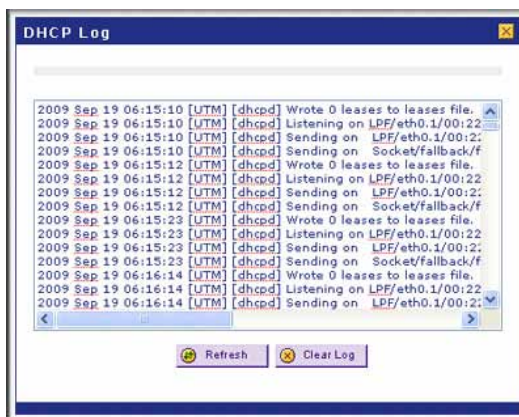
Figure 277.

To view the most recent entries, click **Refresh**. To delete all the existing log entries, click **Clear Log**.

Query the Logs

The UTM generates logs that provide detailed information about malware threats and traffic activities on the network. You can view these logs through the web management interface or save the log records in CSV or HTML format and download them to a computer (the downloading option is not available for all logs).

Note: For information about the quarantine logs, which are stored externally, see *Query the Quarantine Logs (UTM9S Only)* on page 467.

⚠️ **WARNING!**

When you reboot the UTM, the logs are lost. If you want to save the logs, make sure that you configure the UTM to send the logs to a syslog server. For information about how to do this, and also about how to email logs, see *Configure and Activate System, Email, and Syslog Logs* on page 423.

The UTM provides 13 types of logs:

- **Traffic**. All scanned incoming and outgoing traffic.
- **Spam**. All intercepted spam.
- **System**. The system event logs that you have specified on the Email and Syslog screen (see *Configure and Activate System, Email, and Syslog Logs* on page 423). However, by default, many more types of events are logged in the system logs.
- **Service**. All events that are related to the status of scanning and filtering services that you access from the Application Security main navigation menu. These events include update success messages, update failed messages, network connection errors, and so on.
- **Malware**. All intercepted viruses, spyware, and other malware threats.
- **Email filters**. All emails that are blocked because of file extension and keyword violations.
- **Content filters**. All attempts to access blocked websites and URLs.
- **IPS**. All IPS events.
- **Port scan**. All port scan events.
- **Application**. All instant messaging, peer-to-peer and media application, and tool access violations.

- **Firewall**. The firewall logs that you have specified on the Firewall Logs screen (see *Configure and Activate Firewall Logs* on page 432).

- **IPSec VPN**. All IPSec VPN events.

- **SSL VPN**. All SSL VPN events.

You can query and generate each type of log separately and filter the information based on a number of criteria. For example, you can filter the malware logs using the following criteria (other log types have similar filtering criteria):

- Start date/time and end date/time

- Protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP)

- Malware name

- Action

- Domain

- User

- Client and server IP addresses

- Recipient email address

Querying logs is described in the following sections:

- *Query and Download Logs*

- *Example: Use the Logs to Identify Infected Clients*

- *Log Management*

Query and Download Logs

➢ **To query and download logs:**

1. Select **Monitoring > Logs & Reports > Logs Query**. The Logs Query screen displays. (The following figure shows the Malware log information settings as an example.)

   Depending on the selection that you make from the Log Type drop-down list, the screen adjusts to display the settings for the selected type of log.
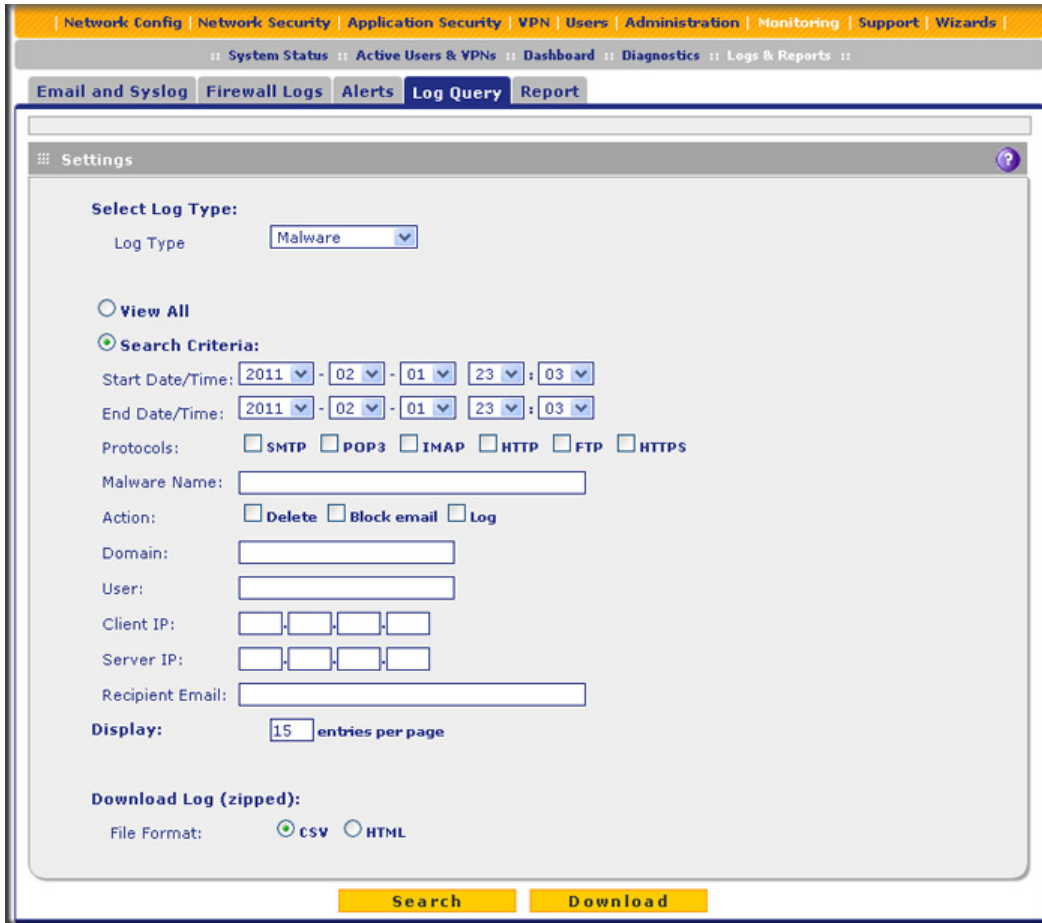
Figure 278.

2. Enter the settings as explained in the following table:

Table 123. Logs Query screen settings

Setting	Description
Log Type	Select one of the following log types from the drop-down list: • **Traffic**. All scanned incoming and outgoing traffic. • **Spam**. All intercepted spam. • **System**. The system event logs that you have specified on the Email and Syslog screen (see *Configure and Activate System, Email, and Syslog Logs* on page 423). However, by default, many more types of events are logged in the system logs. Note that you cannot specify further search criteria on the Log Query screen, that is, when you select **System** from the drop-down list, the System Logs screen displays. • **Service Logs**. All events that are related to the status of scanning and filtering services that you access from the Application Security main navigation menu. These events include update success messages, update failed messages, network connection errors, and so on. • **Malware**. All intercepted viruses, spyware, and other malware threats.

Table 123. Logs Query screen settings (continued)

Setting	Description		
Log Type (continued)	• **Port Scan**. All port scan events. • **Application**. All instant messaging, peer-to-peer and media application, and tools access violations. • **Firewall**. The firewall logs that you have specified on the Firewall Logs screen (see *Configure and Activate Firewall Logs* on page 432). Note that you cannot specify further search criteria on the Log Query screen, that is, when you select **Firewall** from the drop-down list, the Firewall Logs screen displays. • **IPSEC VPN**. All IPSec VPN events. Note that you cannot specify further search criteria on the Log Query screen, that is, when you select **IPSEC VPN** from the drop-down list, the IPSec VPN Logs screen displays. • **SSL VPN**. All SSL VPN events. Note that you cannot specify further search criteria on the Log Query screen, that is, when you select **SSL VPN** from the drop-down list, the SSL VPN Logs screen displays. • **Content filters**. All attempts to access blocked websites and URLs. • **IPS**. All IPS events. • **Email filters**. All emails that are blocked because of file extension and keyword violations.		
View All	Select one of the following radio buttons: • **View All**. Display or download the entire selected log.		
Search Criteria	• **Search Criteria**. Query the selected log by configuring the search criteria that are available for the selected log.		
	Start Date/Time	From the drop-down lists, select the year, month, day, hours, and minutes for the start date and time. This field is available for the following logs: Traffic, Spam, Service, Malware, Email filters, Content filters, Port Scan, IPS, and Application.	
	End Date/Time	From the drop-down lists, select the year, month, day, hours, and minutes for the end date and time. This field is available for the following logs: Traffic, Spam, Service, Malware, Email filters, Content filters, Port Scan, IPS, and Application.	
	Protocols	Select one or more check boxes to specify the protocols that are queried. The following protocols can be selected: • For Traffic and Malware logs: SMTP, POP3, IMAP, HTTP, FTP, and HTTPS. • For the Spam log: SMTP and POP3. • For the Email filters log: SMTP, POP3, and IMAP. • For the Content filters log: HTTP, FTP, and HTTPS.	
	Domain	The domain name that is queried. This field is available for the following logs: Traffic, Spam, Malware, Email filters, Content filters, and Application.	

Table 123. Logs Query screen settings (continued)

Setting	Description	
Search Criteria (continued)	User	The user name that is queried. This field is available for the following logs: Traffic, Spam, Malware, Email filters, Content filters, and Application.
	Client IP	The client IP address that is queried. This field is available for the following logs: Traffic, Spam, Malware, Content filters, Port Scan, IPS, Application.
	Server IP	The server IP address that is queried. This field is available for the following logs: Traffic, Malware, Content filters, Port Scan, IPS, Application.
	Category or Categories	From the drop-down list, select a category that is queried. You can select the following from the drop-down list: • For the IPS log: an attack. • For the Application log: an instant messaging, peer-to-peer, media, or tool application.
	Reason	Select one or more check boxes to specify the reasons that are queried: You can select one or more of the following check boxes: • For the Email filters log: Keyword, FileType, Filename, Password, and SizeLimit. • For the Content filters log: URL, FileType, SizeLimit, Proxy, and Keyword.
	Spam Found By	This field is available only for the Spam log. Select one of the following check boxes to specify the method by which spam is detected: Blacklist or Distributed Spam Analysis.
	Malware Name	The name of the malware threat that is queried. This field is available only for the Malware log.
	Action	The spam or malware detection action that is queried. The following actions can be selected: • For the Spam log: Select the **Block** or **Tag** check box. • For the Malware log: Select the **Delete**, **Block email**, or **Log** check box.
	Email Subject	The email subject that is queried: This field is available for the following logs: Spam and Email filters.
	Sender Email	The sender's email address that is queried. This field is available only for the Traffic log.

Table 123. Logs Query screen settings (continued)

Setting	Description	
Search Criteria (continued)	Recipient Email	The recipient's email address that is queried. This field is available for the following logs: Traffic, Spam, Malware, and Email filters.
	Message	The email message text that is queried. This field is available for the following logs: Port Scan, IPS, and Application.
	Subject	The email subject line that is queried. This field is available only for the Traffic log.
	Size	The minimum and maximum size (in bytes) of the file that is queried. This field is available only for the Traffic log.
	Event	The type of event that is queried. These events are the same events that are used to indicate the syslog server severity: EMERG, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFO, and DEBUG. This field is available only for the Service log.
	URL	The URL that is queried. This field is available only for the Content filters log.
Display	The maximum number of pages that is displayed.	
Download Log (zipped) File Format	Select a radio button to specify the format to download the zipped log file: • **CSV**. Download the log file as a comma-separated values (CSV) file. • **HTML**. Download the log file as an HTML file.	

3. Click one of the following action buttons:

- **Search**. Query the log according to the search criteria that you specified, and view the log through the web management interface, that is, onscreen.

- **Download**. Query the log according to the search criteria that you specified, and download the log to a computer.

> **Note:** You cannot query or download the system, firewall, IPSec VPN, and SSL VPN logs. When you select any of these logs, you can view them through the web management interface, that is, the logs display onscreen.

Example: Use the Logs to Identify Infected Clients

You can use the UTM logs to help identify potentially infected clients on the network. For example, clients that are generating abnormally high volumes of HTTP traffic might be infected with spyware or other malware threats.

To identify infected clients that are sending spyware in outbound traffic, query the UTM malware logs and see if any of your internal IP addresses are the source of spyware.

➢ **To identify infected clients:**

1. On the Log Query screen (see *Figure 278* on page 462), select **Traffic** as the log type.
2. Select the start date and time from the drop-down lists.
3. Select the end date and time from the drop-down lists.
4. Next to Protocols, select the **HTTP** check box.
5. Click **Search**. After a few minutes, the log displays onscreen.
6. Check if there are clients that are sending out suspicious volumes of data, especially to the same destination IP address, on a regular basis.

If you find a client exhibiting this behavior, you can run a query on that client's HTTP traffic activities to get more information. Do this by running the same HTTP traffic query and entering the client IP address in the Client IP field.

Log Management

Generated logs take up space and resources on the UTM internal disk. To ensure that there is always sufficient space to save newer logs, the UTM automatically deletes older logs whenever the total log size reaches 50 percent of the allocated file size for each log type.

Automated log purging means that you do not need to constantly manage the size of the UTM logs and ensures that the latest malware threats and traffic activities are always recorded.

Note: After the UTM reboots, traffic logs are lost. Therefore, NETGEAR recommends that you connect the UTM to a syslog server to save the traffic logs externally. Other logs (that is, nontraffic logs) are automatically backed up on the UTM every 15 minutes. However, if a power failure affects the UTM, logs that were created within this 15-minute period are lost.

For information about how to manually purge selected logs, see *Configure and Activate System, Email, and Syslog Logs* on page 423.

Query the Quarantine Logs (UTM9S Only)

The UTM9S can quarantine spam and malware files. Before you can query the Spam and Malware logs, you need to have done the following:

1. You have integrated a ReadyNAS (see *Connect to a ReadyNAS* on page 415).

2. You have configured the quarantine settings (see *Configure the Quarantine Settings* on page 416).

3. You have selected to quarantine emails, attachments, objects, and web files on one or more of the following screens:

   - Email Anti-Virus screen (see *Customize Email Antivirus and Notification Settings* on page 179)

   - Distributed Spam Analysis screen (see *Configure Distributed Spam Analysis* on page 191)

   - Malware Scan screen (see *Configure Web Malware Scans* on page 197)

   - FTP screen (*Configure FTP Scans* on page 219)

Querying and viewing quarantined logs is described in the following sections:

- *Query the Quarantined Logs*
- *View and Manage the Quarantined Spam Table*
- *View and Manage the Quarantined Infected Files Table*
- *Spam Reports for End Users*

Query the Quarantined Logs

➢ **To query the quarantine logs:**

1. Select **Monitoring > Quarantine**. The Quarantine screen displays. (The following figure shows the Spam log information settings as an example.)

   Depending on the selection that you make from the File Type drop-down list, the screen adjusts to display either the settings for the Spam log or the Malware log.
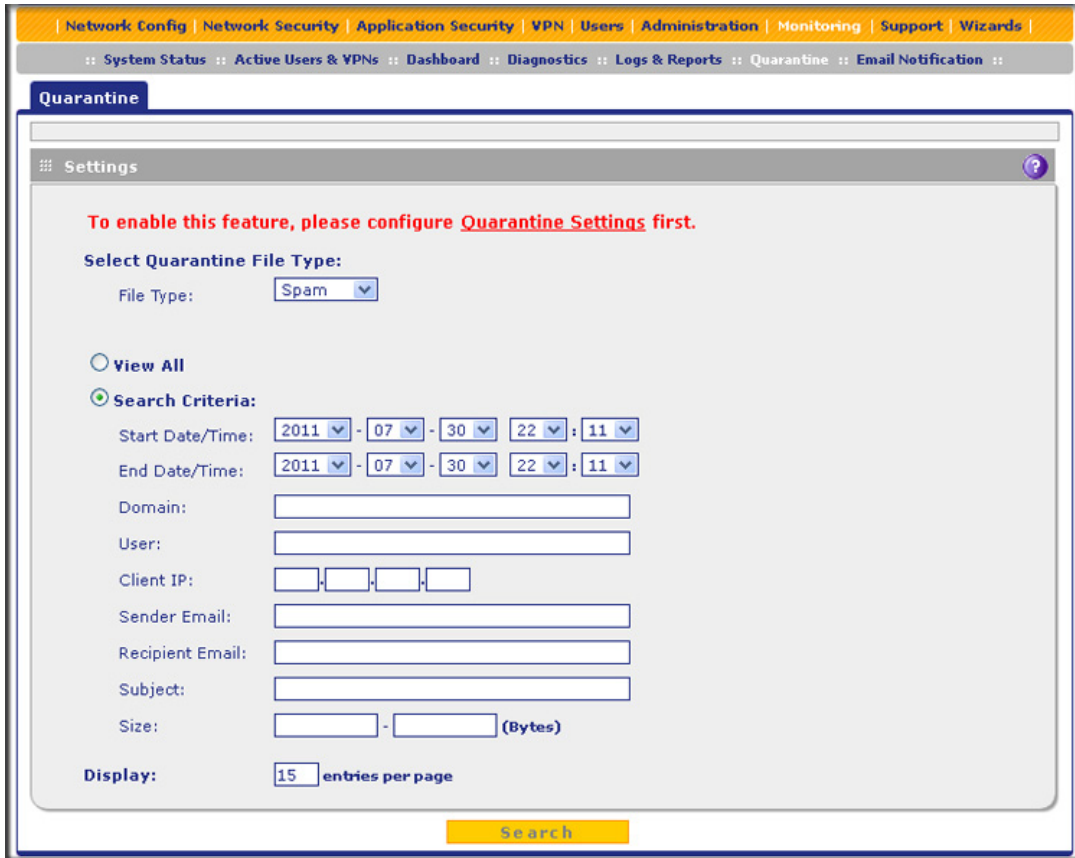
Figure 279.

2. Enter the settings as explained in the following table:

Table 124. Quarantine screen settings

Setting	Description	
File Type	Select one of the following file types from the drop-down list: • **Spam**. All intercepted spam. • **Malware**. All intercepted viruses, spyware, and other malware threats.	
View All	Select one of the following radio buttons: • **View All**. Display or download the entire selected log.	
Search Criteria	• **Search Criteria**. Query the selected log by configuring the search criteria that are available for the selected log.	
	Start Date/Time	From the drop-down lists, select the year, month, day, hours, and minutes for the start date and time. This field is available for both the Spam and Malware logs.
	End Date/Time	From the drop-down lists, select the year, month, day, hours, and minutes for the end date and time. This field is available for both the Spam and Malware logs.

Table 124. Quarantine screen settings (continued)

Setting		Description
Search Criteria (continued)	Protocols	For the Malware log only, select one or more check boxes to specify the protocols that are queried: SMTP, POP3, IMAP, HTTP, FTP, and HTTPS.
	Domain	The domain name that is queried. This field is available for both the Spam and Malware logs.
	User	The user name that is queried. This field is available for both the Spam and Malware logs.
	Malware Name	The name of the malware threat that is queried. This field is available only for the Malware log.
	Client IP	The client IP address that is queried. This field is available for both the Spam and Malware logs.
	Sender Email	The sender's email address that is queried. This field is available only for the Spam log.
	Recipient Email	The recipient's email address that is queried. This field is available for both the Spam and Malware logs.
	Subject	The email subject line that is queried. This field is available for both the Spam and Malware logs.
	Size	The minimum and maximum size (in bytes) of the file that is queried. This field is available for both the Spam and Malware logs.
Display		The maximum number of pages that is displayed.

3. Click **Search**. The log is queried according to the search criteria that you specified, and the search results are displayed onscreen.

View and Manage the Quarantined Spam Table

When you query the spam quarantine file, the Quarantine screen with the Quarantined Spam table displays:

Figure 280.

The Quarantined Spam table has the following columns (not all columns are shown in the previous figure):

- **Check box**. Lets you select the table entry.
- **Date**. The date that the email was received.
- **Protocol**. The protocol (SMTP) in which the spam was found.
- **Domain**. The domain in which the spam was found.
- **User**. The user name that was used to log in to the UTM.
- **Client IP**. The client IP address from which the spam originated.
- **From**. The email address of the sender.
- **To**. The email address of the recipient.
- **Subject**. The email subject line.
- **Size (Bytes)**. The size of the email in bytes.

After you have selected one or more table entries, take one of the following actions (or click the **return** link to return to the previous screen):

- **Send as Spam**. The selected spam email files are tagged as spam for distributed spam analysis, and are sent to the intended recipients.

- **Send as Ham**. The selected spam email files are not tagged as spam for distributed spam analysis, are removed from quarantine, and are sent to the intended recipients.

- **Delete**. The selected spam email files are removed from quarantine and deleted.

View and Manage the Quarantined Infected Files Table

When you query the malware quarantine file, the Quarantine screen with the Quarantined Infected Files table displays:

Figure 281.

The Quarantined Infected Files table has the following columns (not all columns are shown in the previous figure):

- **Check box**. Lets you select the table entry.
- **Date**. The date that the file was received.
- **Protocol**. The protocol (SMTP, POP3, IMAP, HTTP, FTP, HTTPS) in which the spyware or virus was found.
- **Domain**. The domain name that was used to log in to the UTM.
- **User**. The user name that was used to log in to the UTM.
- **Malware Name**. The name of the spyware or virus.
- **Filename**. The name of the file in which the spyware or virus was found.

- **Client IP**. The client IP address from which the spyware or virus originated.
- **Server IP**. The server IP address from which the spyware or virus originated.
- **From**. The email address of the sender.
- **To**. The email address of the recipient.
- **URL/Subject**. The URL or subject that is associated with the spyware or virus.
- **Size (Bytes)**. The size of the virus or spyware file in bytes.

After you have selected one or more table entries, take one of the following actions (or click the **return** link to return to the previous screen):

- **Resend to Admin**. The selected malware files are removed from quarantine, zipped together as an email attachment, and then sent to the recipient that you have specified on the Email Notification Server screen (see *Configure the Email Notification Server* on page 422).
- **Delete**. The selected malware files are removed from quarantine and deleted.

Spam Reports for End Users

Any user, including unauthenticated users who have the link to the User Portal Login screen, can email a spam report to an email address.

➢ **For an end user to send a spam report:**

   1. Open the User Portal Login screen (for information about how to access this screen, see *Users with Special Access Privileges* on page 346):
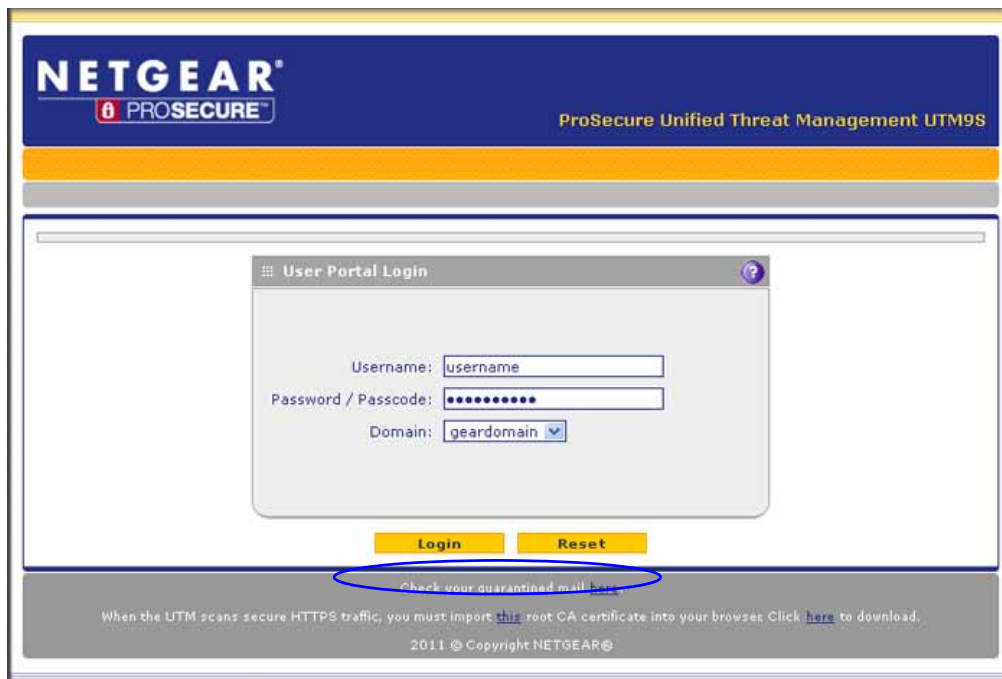
Figure 282.

2. Click the **here** link in the Check your quarantined mail here section. The following screen displays:

Figure 283.

3. From the drop-down lists, specify the start date, start time, end date, and end time for the spam report.

4. In the Send to field, enter an email address.

5. Click **Send Report**.

> **Note:** The spam report contains only spam messages that were sent to the email address that is specified in the Send to field.

View, Schedule, and Generate Reports

The reporting functions of the UTM let you perform the following tasks that help you to monitor the protection of the network and the performance of the UTM:

- Generating, viewing, and downloading web activity, IPS and application, email activity, and system reports

- Scheduling automatic web activity, IPS and application, email activity, and system reports, and emailing these reports to specified recipients

You can view the reports onscreen, download them to your computer, and configure the UTM to send them to one or more email addresses.

The UTM provides preconfigured report templates. As an option, you can apply filtering options to narrow down and specify the following options:

- The period that is covered in the report
- The categories and domains to be included in the report
- The number of entries per report (for example, how many entries—from 1 to 10—are included in reports that show the "top number.")
- The chart type of the report (horizontal bar, pie, or vertical bar)

Because of the nature of the Report screen, it is divided and presented in this manual in three figures that are explained in the following sections:

- *Report Filtering Options*
- *Use Report Templates and View Reports Onscreen*
- *Schedule, Email, and Manage Reports*

Report Filtering Options

Before you generate reports to view onscreen or schedule reports to be emailed, you might want to configure filtering options. If you do not configure filtering options, the default settings apply. The report default settings are:

- Time range. The last 24 hours.
- Destination. None.
- Count. 10.
- Chart Type. Vertical bar.

➢ **To configure filtering options:**

1. Select **Monitoring > Logs & Reports > Report**. The Report screen displays. (The following figure shows only the sections with the preconfigured report templates.)
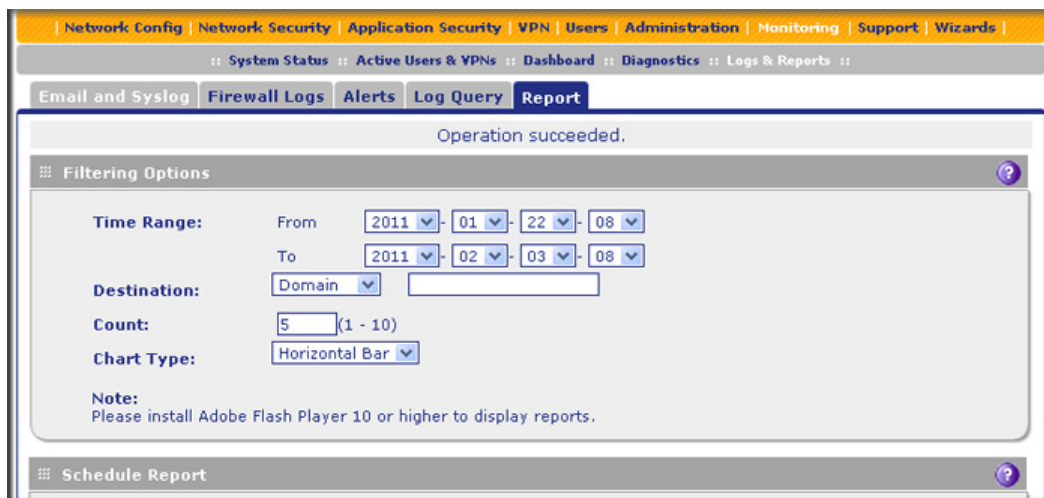
Figure 284. Report, screen 1 of 4

2. Enter the settings as explained in the following table:

Table 125. Report screen: filtering options settings

Setting	Description		
Time Range **Note:** Even if you click Apply to save the filtering options, when you leave the Report screen and then return to it, the From and To drop-down lists are reset to their defaults. You cannot save these settings.	From	From the drop-down lists, specify the start year, month, day, and hour for the report. **Note:** By default, the beginning time is 24 hours earlier than the ending time. The maximum time range is 31 days.	
	To	From the drop-down lists, specify the end year, month, day, and hour for the report. **Note:** By default, the ending time is the current hour. The maximum time range is 31 days.	
Destination	You can narrow down the reports to a single domain (wildcards are not applicable), a single IP address, a single category, or a selection of categories. Specifying a destination affects the following reports in the Web Activity section: • Top n Domain by Bandwidth • Top n Category by Bandwidth • Top n Blocked Domains • Top n Blocked Categories • Top n Domains By Request • Top n Categories By Request • Top n Domains by Session Time • Top n Categories by Session Time		
	Domain	Enter a URL or an IP address in the field next to Domain. The report is restricted to the specified URL.	
	Category	Select one or more web categories from the drop-down list next to Category. The report is restricted to the selected category or categories. When you select Category from the drop-down list, you also have the option to select the **Exclude selected Categories** check box, which allows you to run a report from which the selected category or categories are excluded.	
Count	Enter a number between 1 and 10 to specify how many entries are included in reports that provide a top count, such as the Top n(umber of) Blocked Domain report or the Top n(umber of) Infected Clients report. The default number is 10, which means that a maximum of 10 domains are included in the Top n Blocked Domain report and a maximum of 10 clients are included in the Top n Infected Clients report, for example.		
Chart Type	Specify the type of chart that is generated in the report by making one of the following selections from the drop-down list: • **Horizontal Bar**. • **Pie**. • **Vertical Bar**. This is the default selection.		

3. The next steps depends on whether you want to view the report on screen or schedule it to
    be emailed:

    • **Viewing onscreen**. To view a filtered report onscreen, select a report by clicking **View**
      next to the report. (For more information, see the following section.) To save the
      configured filtering options for future use, click **Apply** at the bottom of the Report
      screen.

    • **Scheduling to be emailed**. To save the configured filtering options to use them to
      schedule a filtered report that can be emailed, click **Apply** at the bottom of the Report
      screen, and then follow the procedure in *Schedule, Email, and Manage Reports* on
      page 480.

> **Note:** Even if you click Apply to save the filtering options, when you leave
> the Report screen and then return to it, the From and To drop-down
> lists are reset to their defaults. You cannot save these settings. The
> other filtering options are saved when you click Apply.

Use Report Templates and View Reports Onscreen

The UTM provides preconfigured report templates in four categories:

• Web Activity
• IPS & Applications
• Email Activity
• System

> **Note:** Adobe Flash Player 10 or later is required to display the reports.

> **Note:** To generate web reports, make sure that the Log HTTP Traffic check
> box on the Content Filtering screen is selected (see *Configure Web
> Content Filtering* on page 199).

➢ **To display the report templates and view reports onscreen:**

1. Select **Monitoring > Logs & Reports > Report**. The Report screen displays. (The
    following figure shows only the sections with the preconfigured report templates.)

Figure 285. Report, screen 2 of 4

Note: For information about setting a time range and other filtering options for a report, see the previous section.

---

2. Select a report by clicking **View** next to the report to display the selected report onscreen. The following table explains the contents of the reports.

Table 126. Report screen: report template information

Report template	Information reported for the specified time range
Web Activity	
Note: To generate web reports, make sure that the Log HTTP Traffic check box on the Content Filtering screen is selected (see *Configure Web Content Filtering* on page 199).	
Requests by Time	For each of the three web server protocols separately, a chart and a table with the number of web requests.
Traffic Volume by Time	For each of the three web server protocols separately, a chart and a table with the processed traffic, expressed in bytes.

Table 126. Report screen: report template information (continued)

Report template	Information reported for the specified time range
URL Filtering by Time	For the HTTPS and HTTP protocols separately, a chart and a table with the number of blocked attempts to access URLs that are on the blacklist.
File Blocked by Time	For each of the three web server protocols separately, a chart and a table with the number of blocked files (FTP files, HTTPS attachments, or HTTP attachments).
Malware by Time	For each of the three web server protocols separately, a chart and a table with the number of detected malware incidents.
Top n Domain by Bandwidth	For all web server protocols combined, a chart and a table with the domains for which most bandwidth was consumed and the size of the bandwidth consumed (expressed in bytes), and drill-down links to the users who accessed the domains. When you click the drill-down link for a domain, the User by Bandwidth chart and table display, showing the users who accessed the domain. For each user, the user login name (including the domain to which the user belongs) and the size of the bandwidth consumed (expressed in bytes) are shown.
Top n Category by Bandwidth	For all web server protocols combined, a chart and a table with the web categories for which most bandwidth was consumed and the size of the bandwidth consumed (expressed in bytes), and drill-down links to the users who accessed the web categories. When you click the drill-down link for a web category, the Users by Bandwidth chart and table display, showing the users who accessed the web category. For each user, the user login name (including the domain to which the user belongs) and the size of the bandwidth consumed (expressed in bytes) are shown.
Top n Blocked Domains	For all web server protocols combined, a chart and a table with the domains that were blocked most often, including the number of blocked requests, and drill-down links to the users who requested them. When you click the drill-down link for a domain, the Blocked Users by Requests chart and table display, showing the users who requested the domain. For each user, the user login name (including the domain to which the user belongs) and the number of blocked requests are shown.
Top n Blocked Categories	For all web server protocols combined, a chart and a table with the web categories that were blocked most often, including the number of blocked requests, and drill-down links to the users who requested them. When you click the drill-down link for a domain, the Blocked Users by Requests chart and table display, showing the users who requested the domain. For each user, the user login name (including the domain to which the user belongs) and the number of blocked requests are shown.
Top n Domains By Request	For all web server protocols combined, a chart and a table with the domains that were requested most often, including the number of times that they were requested, and drill-down links to the users who requested them. When you click the drill-down link for a domain, the Users by Requests chart and table display, showing the users who requested the domain. For each user, the user login name (including the domain to which the user belongs) and the number of blocked requests are shown.

Table 126. Report screen: report template information (continued)

Report template	Information reported for the specified time range
Top n Categories By Request	For all web server protocols combined, a chart and a table with the web categories that were requested most often, including the number of times that they were requested, and drill-down links to the users who requested them.
	When you click the drill-down link for a web category, the Users by Requests chart and table display, showing the users who requested the web category. For each user, the user login name (including the domain to which the user belongs) and the number of blocked requests are shown.
Top n Domains By Session Time	For all web server protocols combined, a chart and a table with the domains at which users spent most time, including the session time, and drill-down links to the users who spent time at the domains.
	When you click the drill-down link for a domain, the Users by Session Time chart and table display, showing the users who spent time at the domain. For each user, the user login name (including the domain to which the user belongs) and the session time are shown.
Top n Categories By Session Time	For all web server protocols combined, a chart and a table with the web categories at which users spent most time, including the session time, and drill-down links to the users who spent time at the web categories.
	When you click the drill-down link for a web category, the Users by Session Time chart and table display, showing the users who spent time at the web category. For each user, the user login name (including the domain to which the user belongs) and the session time are shown.
IPS & Application	
IPS Incidents by Time	For each of the seven IPS attack types separately and for port scans separately, a chart and a table with the number of detected attacks or scans.
Application Incidents by Time	For each of the four types of applications separately, a chart and a table with the number of blocked applications.
Top n Scanned Destination IP	A chart and a table with the destination IP addresses that were scanned most often, including the number of times that they were scanned.
Top n Attacking Source IP	A chart and a table with the source IP addresses from which attacks were launched most often, including the number of times that the attacks were launched.
Top n Attacked Destination IP	A chart and a table with the destination IP addresses that were attacked most often, including the number of times that they were attacked.
Top n Attacking IPS Rule Name	A chart and a table with the names of the IPS attacks that occurred most often, including the number of times that they occurred.
Top n Blocked Applications	A chart and a table with the names of the applications that were blocked most often, including the number of times that they were blocked.
Top n Blocked Clients of Application	A chart and a table with the client IP address for which applications were blocked most often, including the number of times that they were blocked.
Email Activity	
Malware Incidents By Time	For each of the three email server protocols separately, a chart and a table with the number of detected malware incidents.

Table 126. Report screen: report template information (continued)

Report template	Information reported for the specified time range
File Blocked By Time	For each of the three email server protocols separately, a chart and a table with the number of blocked files (attachments).
Spams By Time	For the POP3 and SMTP protocols separately, a chart and a table with the number of spam emails that are detected by distributed spam analysis.
Requests By Time	For each of the three email server protocols separately, a chart and a table with the number of processed emails.
Traffic By Time	For each of the three email server protocols separately, a chart and a table with the processed traffic, expressed in bytes.
Blacklist By Time	For the POP3 and SMTP protocols separately, a chart and a table with the number of blocked emails from email addresses that are on the blacklist, and for the SMTP protocol only, a chart and a table with the number of blocked emails from email addresses that are on the real-time blacklist (RBL).
System	
Total Bandwidth Usage By Time	A chart and a table with the consumed bandwidth, expressed in bytes.
Top n User By Bandwidth	A chart and a table with the IP addresses that consume most bandwidth, expressed in bytes.
Total Malware Incidents By Time	For email and web traffic separately, a chart and a table with the number of detected malware incidents.
Top n Malwares	For email and web traffic separately, a chart and a table with the names of the malware that were detected most often, including the number of times that they were detected.
Top n Infected Clients	For email and web clients separately, a chart and a table with the IP addresses of the clients that were infected by malware most often, including the number of times that they were infected.
CPU & Mem Usage	For the UTM's CPU and memory separately, a chart and a table with the usage, expressed in percentage.

Schedule, Email, and Manage Reports

➢ **To schedule automatic generation and emailing of reports:**

1. Select **Monitoring > Logs & Reports > Report**. The Report screen displays. (The following two figures show only the Schedule Reports and Report History sections of the Report screen.)
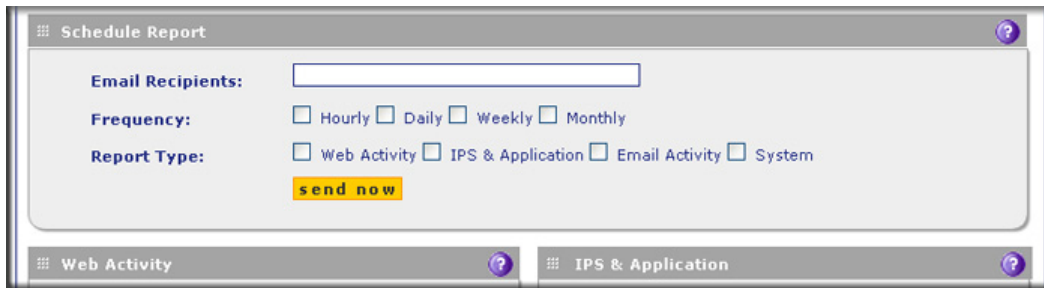
Figure 286. Report, screen 3 of 4

2. Enter the settings in the Schedule Reports section as explained in the following table:

Table 127. Report screen: schedule report settings

Setting	Description
Schedule Reports	
Email Recipients	Specify the email addresses of the report recipients, using commas to separate the email addresses.
Frequency	Select one or more of the following check boxes to specify the frequency with which the reports are generated and emailed: • **Hourly**. The report is generated hourly at 3 minutes past the top of the hour. • **Daily**. The report is generated daily at 0:03 a.m. • **Weekly**. The report is generated weekly on Sunday at 0:03 a.m. • **Monthly**. The report is generated monthly on first day of the month at 0:03 a.m.
Reports	Select one or more check boxes to specify the reports that are generated: • **Web Activity**. All reports that are listed in the Web Activity section of the Report screen. • **IPS & Application**. All reports that are listed in the IPS & Application section of the Report screen. • **Email Activity**. All reports that are listed in the Email Activity section of the Report screen. • **System**. All reports that are listed in the System section of the Report screen. **Note:** You can select all check boxes, but you might generate a very large aggregate report. **Note:** Drill-down links (that is, links that provide access to additional charts and tables) are not available in emailed reports.
Report List	
Number of Reports to Keep	Enter the number of reports that the UTM saves. The maximum number is 12.

3. Optional step: To send the reports immediately to the email addresses that are specified in the Email Recipients field, click **Send Now**. (These emailed reports are not saved in the Reports History section of the Reports screen.)
4. Click **Apply** to save your settings.

Managing Saved Reports

After the scheduled report has been generated and emailed, the record of the report is displayed in the Report History section of the Report screen:
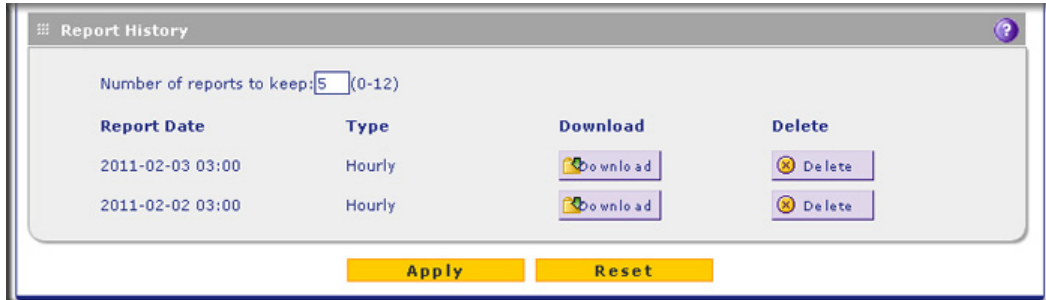
Figure 287. Report, screen 4 of 4

The Report History section shows the generated and emailed reports with their report date and lets you perform the following actions.

- **Specify the number of reports to keep**. To manage the number of reports that you can keep, enter a number from 1 to 12 in the Number of reports to keep field. The default number is 5 reports.

- **Download a report**. Click **Download** next to a report to download the report to your computer.

- **Delete a report**. Click **Delete** next to a report to delete the report.

Use Diagnostics Utilities

The UTM provides diagnostic tools that help you analyze traffic conditions and the status of the network. Two sets of tools are available:

- **Network diagnostic tools**. These tools include a ping utility, traceroute utility, and DNS lookup utility, and the option to display the routing table.

- **Traffic diagnostic tools**. These tools allow you to perform real-time, per-protocol traffic analysis between specific source and destination addresses, and let you generate reports on network usage in your network.

Note: For normal operation, diagnostic tools are not required.

The diagnostic tools are described in the following sections:

- *Use the Network Diagnostic Tools (All UTM Models Except the UTM9S)*
- *Use the Network Diagnostic Tools (UTM9S)*
- *Use the Real-Time Traffic Diagnostics Tool (All UTM Models Except the UTM9S)*

- *Use the Real-Time Traffic Diagnostics Tool (UTM9S)*
- *Gather Important Log Information and Generate a Network Statistics Report (All Models)*

To display the Diagnostics screen, select **Monitoring > Diagnostics**. To facilitate the explanation of the tools, the Diagnostics screen is divided and presented in this manual in three figures.

Use the Network Diagnostic Tools (All UTM Models Except the UTM9S)

This section discusses the Network Diagnostics section and the Perform a DNS Lookup section of the Diagnostics screen of all UTM models except the UTM9S.
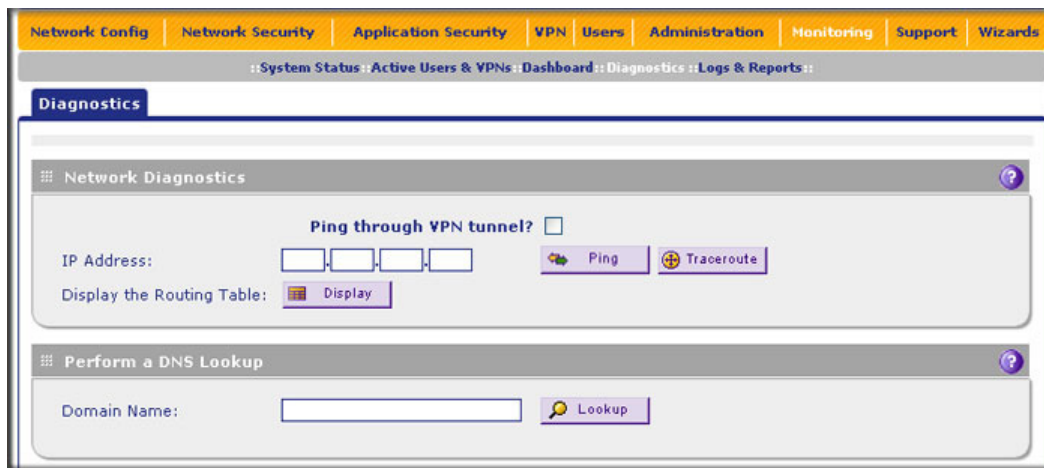
Figure 288. Diagnostics, screen 1a of 3

Send a Ping Packet

Use the ping utility to send a ping packet request in order to check the connection between the UTM and a specific IP address. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results are displayed on a new screen; click **Back** on the browser menu bar to return to the Diagnostics screen.

➢ **To send a ping:**

1. Locate the Network Diagnostics section on the Diagnostics screen. In the IP Address field, enter the IP address that you want to ping.

2. If the specified address is reached through a VPN tunnel, select the **Ping through VPN tunnel** check box.

3. Click the **Ping** button. The results of the ping are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Trace a Route

A traceroute lists all routers between the source (the UTM) and the destination IP address.

➢ **To send a traceroute:**

1. Locate the Network Diagnostics section on the Diagnostics screen. In the IP Address field, enter the IP address for which you want trace the route.

2. Click the **Traceroute** button. The results of the traceroute are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Display the Routing Table

Displaying the internal routing table can assist NETGEAR technical support in diagnosing routing problems.

To display the routing table, locate the Network Diagnostics section on the Diagnostics screen. Next to Display the Routing Table, click the **Display** button. The routing table is shown in the Route Display screen that displays as a pop-up screen.

Look Up a DNS Address

A Domain Name Server (DNS) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a web, FTP, mail, or other server on the Internet, request a DNS lookup to find the IP address.

➢ **To look up a DNS address:**

1. Locate the Perform a DNS Lookup section on the Diagnostics screen. In the Domain Name field, enter a domain name.

2. Click the **Lookup** button. The results of the lookup action are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Use the Network Diagnostic Tools (UTM9S)

This section discusses the Network Diagnostics section and the Perform a DNS Lookup section of the Diagnostics screen of the UTM9S.

Figure 289. Diagnostics, screen 1b of 3

Send a Ping Packet

Use the ping utility to send a ping packet request in order to check the connection between the UTM9S and a specific IP address. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results are displayed on a new screen; click **Back** on the browser menu bar to return to the Diagnostics screen.

 To send a ping:

1. Locate the Network Diagnostics section on the Diagnostics screen. In the IP Address field, enter the IP address that you want to ping.
2. Do one of the following:
   • Make sure that the **Ping through VPN tunnel?** check box is cleared, and then select a gateway from the Select Local Gateway drop-down list. (The Select VPN Tunnel drop-down list is masked out.)
   • Select the the **Ping through VPN tunnel?** check box, and then select a VPN tunnel from the Select VPN Tunnel drop-down list. (The Select Local Gateway drop-down list is masked out.)
3. Click the **Ping** button. The results of the ping are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Trace a Route

A traceroute lists all routers between the source (the UTM9S) and the destination IP address.

 To send a traceroute:

1. Locate the Network Diagnostics section on the Diagnostics screen. In the IP Address field, enter the IP address for which you want trace the route.

2. Click the **Traceroute** button. The results of the traceroute are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Display the Routing Table

Displaying the internal routing table can assist NETGEAR technical support in diagnosing routing problems.

To display the routing table, locate the Network Diagnostics section on the Diagnostics screen. Next to Display the Routing Table, click the **Display** button. The routing table is shown in the Route Display screen that displays as a pop-up screen.

Look Up a DNS Address

A Domain Name Server (DNS) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a web, FTP, mail, or other server on the Internet, request a DNS lookup to find the IP address.

➢ **To look up a DNS address:**

1. Locate the Perform a DNS Lookup section on the Diagnostics screen. In the Domain Name field, enter a domain name.

Click the **Lookup** button. The results of the lookup action are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Use the Real-Time Traffic Diagnostics Tool (All UTM Models Except the UTM9S)

This section discusses the Realtime Traffic Diagnostics section of the Diagnostics screen of all UTM models except the UTM9S.

Figure 290. Diagnostics, screen 2a of 3

You can use the real-time traffic diagnostics tool to analyze traffic patterns with a network traffic analyzer tool. Depending on the network traffic analyzer tool that you use, you can find out which applications are using the most bandwidth, which users use the most bandwidth, how long users are connected, and other information.

➢ **To use the real-time traffic diagnostics tool:**

1. Locate the Realtime Traffic Diagnostics section on the Diagnostics screen. In the Source IP Address field, enter the IP address of the source of the traffic stream that you want to analyze.

2. In the Destination IP Address field, enter the IP address of the destination of the traffic stream that you want to analyze.

3. Click **Start**. You are prompted to save the downloaded traffic information file to your computer; however, do not save the file until you have stopped capturing the traffic flow.

4. When you want to stop capturing the traffic flow, click **Stop**.

5. Select a location to save the captured traffic flow. (The default file name is diagnostics.result.dat.) The file is downloaded to the location that you specify.

6. When the download is complete, browse to the download location that you specified, and verify that the file has been downloaded successfully.

7. Optional: Send the file to NETGEAR technical support for analysis.

Use the Real-Time Traffic Diagnostics Tool (UTM9S)

This section discusses the Realtime Traffic Diagnostics section of the Diagnostics screen of all the UTM9S.
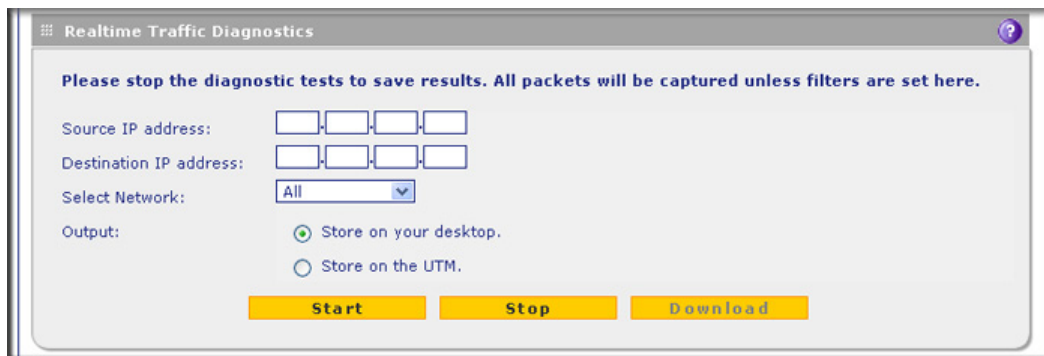
Figure 291. Diagnostics, screen 2b of 3

You can use the real-time traffic diagnostics tool to analyze traffic patterns with a network traffic analyzer tool. Depending on the network traffic analyzer tool that you use, you can find out which applications are using the most bandwidth, which users use the most bandwidth, how long users are connected, and other information.

➢ **To use the real-time traffic diagnostics tool:**

1. Locate the Realtime Traffic Diagnostics section on the Diagnostics screen. In the Source IP Address field, enter the IP address of the source of the traffic stream that you want to analyze.

2. In the Destination IP Address field, enter the IP address of the destination of the traffic stream that you want to analyze.

3. From the Select Network drop-down list, select one of the following components:
    *   All (that is, all interfaces, the slot in which the xDSL module is installed, and all VLANs and WLANs)
    *   A single WAN interface
    *   The slot in which the xDSL module is installed (SLOT-1 or SLOT-2)
    *   A single VLAN or WLAN

4. Specify how the output is saved by selecting either the **Store on your desktop** radio button or the **Store on the UTM** radio button.

5. Click **Start**.

> **Note:** If you select the Store on your desktop radio button, you are prompted to save the traffic information file to your computer; however, do not save the file until you have stopped capturing the traffic flow.

6. When you want to stop capturing the traffic flow, click **Stop**.

7. Take one of the following actions:
    *   If you selected the Store on your desktop radio button, select a location to save the captured traffic flow.
    *   If you selected the Store on the UTM radio button, click **Download**, and then select a location to save the captured traffic flow.

    The default file name is diagnostics.result.dat. The file is downloaded to the location that you specify.

8. When the download is complete, browse to the download location that you specified, and verify that the file has been downloaded successfully.

9. Optional: Send the file to NETGEAR technical support for analysis.

Gather Important Log Information and Generate a Network Statistics Report (All Models)

When you request support, NETGEAR technical support might ask you to collect the debug logs and other information from your UTM.

This section discusses the Gather Important Log Information section, Network Statistics Report section, and Reboot the System section of the Diagnostics screen.
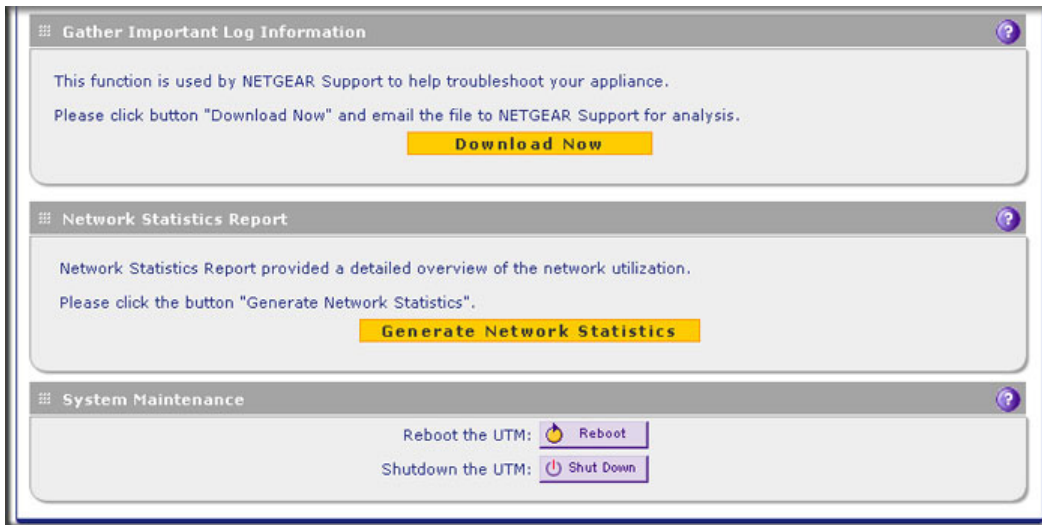
Figure 292. Diagnostics, screen 3 of 3

Gather Important Log Information

➢ **To gather log information about your UTM:**

1. Locate the Gather Important Log Information section on the Diagnostics screen. Click **Download Now**. You are prompted to save the downloaded log information file to your computer. The default file name is importantlog.gpg.

2. When the download is complete, browse to the download location you specified, and verify that the file has been downloaded successfully.

Generate Network Statistics

The network statistic report provides a detailed overview of the network utilization in the UTM managed network environment. The report allows you to see what consumes the most resources on the network.

To generate the Network Statistic Report, locate the Network Statistics Report section on the Diagnostics screen. Click **Generate Network Statistics**. The network statistics report is sent as an email to the recipient that you specified on the Email Notification screen (see *Configure the Email Notification Server* on page 422).

Reboot and Shut Down the UTM

You can perform a remote reboot (restart), for example, when the UTM seems to have become unstable or is not operating normally.

> **Note:** Rebooting breaks any existing connections either to the UTM (such as your management session) or through the UTM (for example, LAN users accessing the Internet). However, when the reboot process is complete, connections to the Internet are automatically reestablished when possible.

To reboot the UTM, locate the Reboot the System section on the Diagnostics screen. Click the **Reboot** button. The UTM reboots. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

> **Note:** See also *Reboot without Changing the Firmware* on page 410.

To shut down the UTM, locate the Reboot the System section on the Diagnostics screen. Click the **Shutdown** button. The UTM shuts down.

WARNING!

You can shut down the UTM using the web management interface, but you cannot start up the UTM using the web management interface.

Monitoring System Access and Performance

490

Troubleshooting and Using Online Support

12

This chapter provides troubleshooting tips and information for the UTM. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the UTM on?

  Go to *Basic Functioning* on page 492.

- Have I connected the UTM correctly?

  Go to *Basic Functioning* on page 492.

- I cannot access the UTM's web management interface.

  Go to *Troubleshoot the Web Management Interface* on page 493.

- A time-out occurs.

  Go to *When You Enter a URL or IP Address, a Time-Out Error Occurs* on page 494.

- I cannot access the Internet or the LAN.

  Troubleshoot the ISP Connection on page 494.

- I have problems with the LAN connection.

  Go to *Troubleshoot a TCP/IP Network Using a Ping Utility* on page 496.

- I want to clear the configuration and start over again.

  Go to *Restore the Default Configuration and Password* on page 498.

- The date or time is not correct.

  Go to *Problems with Date and Time* on page 499.

- I need help from NETGEAR.

  Go to *Use Online Support* on page 499.

> **Note:** The UTM's diagnostic tools are explained in *Use Diagnostics Utilities* on page 482.

Basic Functioning

> **Note:** For descriptions of all LEDs, see *LED Descriptions, UTM5, UTM10, UTM25, UTM50, and UTM150* on page 27 or *LED Descriptions, UTM9S and Modules* on page 28.

> **After you turn on power to the UTM, verify that the following sequence of events occurs:**

1. When power is first applied, verify that the Power LED is on.

2. After approximately 2 minutes, verify that:

   a. The Test LED is no longer lit.

   b. The left LAN port LEDs are lit for any local ports that are connected.

   c. The left WAN port LEDs are lit for any WAN ports that are connected.

   If a port's left LED is lit, a link has been established to the connected device. If a port is connected to a 1000 Mbps device, verify that the port's right LED is green. If the port functions at 100 Mbps, the right LED is amber. If the port functions at 10 Mbps, the right LED is off.

If any of these conditions do not occur, see the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your UTM is turned on, make sure that the power cord is correctly connected to your UTM and that the power supply adapter is correctly connected to a functioning power outlet.

If the error persists, you have a hardware problem and should contact NETGEAR technical support.

Test LED Never Turns Off

When the UTM is powered on, the Test LED turns on for approximately 2 minutes and then turns off when the UTM has completed its initialization. If the Test LED remains on, there is a fault within the UTM.

> **If all LEDs are still on more than several minutes minute after power-up, do the following:**

- Turn the power off, and then turn it on again to see if the UTM recovers.

- Reset the UTM's configuration to factory default settings. Doing so sets the UTM's IP address to **192.168.1.1**. This procedure is explained in *Restore the Default Configuration and Password* on page 498.

If the error persists, you might have a hardware problem and should contact NETGEAR technical support.

LAN or WAN Port LEDs Not On

➢ **If either the LAN LEDs or WAN LEDs do not light when the Ethernet connection is made, check the following:**

- Make sure that the Ethernet cable connections are secure at the UTM and at the hub, router, or workstation.

- Make sure that power is turned on to the connected hub, router, or workstation.

- Be sure that you are using the correct cables:

   When connecting the UTM's WAN ports to one or two devices that provide the Internet connections, use the cables that are supplied with the devices. These cables could be standard straight-through Ethernet cables or Ethernet crossover cables.

Troubleshoot the Web Management Interface

➢ **If you cannot access the UTM's web management interface from a PC on your local network, check the following:**

- Check the Ethernet connection between the PC and the UTM as described in the previous section (*LAN or WAN Port LEDs Not On*).

- Make sure that your PC's IP address is on the same subnet as the UTM. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.1.2 to 192.168.1.254.

   Note: If your PC's IP address is shown as 169.254.x.x:
   Windows and Mac operating systems generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the UTM and reboot your PC.

- If your UTM's IP address has been changed and you do not know the current IP address, reset the UTM's configuration to factory default settings. This sets the UTM's IP address to **192.168.1.1**. This procedure is explained in *Restore the Default Configuration and Password* on page 498.

   Tip: If you do not want to revert to the factory default settings and lose your configuration settings, you can reboot the UTM and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the UTM's LAN interface address.

- Make sure that you are using the SSL https://*address* login rather than the http://*address* login.

- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.

- Try quitting the browser and launching it again.

- Make sure that you are using the correct login information. The factory default login name is admin, and the password is password. Make sure that Caps Lock is off when entering this information.

If the UTM does not save changes you have made in the web management interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.

- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

When You Enter a URL or IP Address, a Time-Out Error Occurs

A number of things could be causing this situation. Try the following troubleshooting steps:

- Check whether other computers on the LAN work correctly. If they do, ensure that your computer's TCP/IP settings are correct. If you use a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses on the WAN ISP Settings screen of the single WAN port models or on one of the WAN ISP Settings screens of the multiple WAN port models. For more information, see *Manually Configure the Internet Connection* on page 71.

- If the computer is configured correctly, but still not working, ensure that the UTM is connected and turned on. Connect to the web management interface, and check the UTM's settings. If you cannot connect to the UTM, see the information in the previous section (*Troubleshoot the Web Management Interface* on page 493).

- If the UTM is configured correctly, check your Internet connection (for example, your modem or router) to make sure that it is working correctly.

Troubleshoot the ISP Connection

If your UTM is unable to access the Internet, you should first determine whether the UTM is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your UTM requests an IP address from the ISP. You can determine whether the request was successful using the web management interface.

> **To check the WAN IP address:**

   1. Launch your browser and navigate to an external site such as www.netgear.com.

   2. Access the web management interface of the UTM's configuration at https://192.168.1.1.

   3. Select **Network Config > WAN Settings**. The WAN Settings screen displays.

   4. In the Action column for the interface for which you want to open the Connection Status screen, click the **Status** button. (For more information, see *View the WAN Ports Status* on page 456.)

   5. Check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your UTM has not obtained an IP address from your ISP.

> **If your UTM is unable to obtain an IP address from the ISP, you might need to force your modem or router to recognize your new UTM by performing the following procedure:**

   1. Turn off the power to the modem or router.

   2. Turn off the power to your UTM.

   3. Wait 5 minutes, and then turn on the power to the modem or router.

   4. When the modem's or router's LEDs indicate that it has reacquired synchronization with the ISP, turn on the power to your UTM.

If your UTM is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your ISP might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.

- If your ISP requires a login, you might have incorrectly set the login name and password.

- Your ISP might check for your PC's host name.
  On the WAN ISP Settings screen of the single WAN port models or on one of the WAN ISP Setting screens of the multiple WAN port models, in the Account Name field, enter the host name, system name, or account name that was assigned to you by your ISP. You might also have to enter the assigned domain name or workgroup name in the Domain Name field, and you might have to enter additional information. For more information, see *Manually Configure the Internet Connection* on page 71.

- Your ISP allows only one Ethernet MAC address to connect to the Internet, and might check for your PC's MAC address. In this case, do one of the following:

  - Inform your ISP that you have bought a new network device, and ask them to use the UTM's MAC address.

  - Configure your UTM to spoof your PC's MAC address. You can do this in the Router's MAC Address section on the WAN Advanced Options screen of the single WAN port models or on one of the WAN Advanced Options screens of the multiple WAN port models. For more information, see *Configure Advanced WAN Options* on page 90.

If your UTM can obtain an IP address, but an attached PC is unable to load any web pages from the Internet:

- Your PC might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. You can configure your PC manually with DNS addresses, as explained in your operating system documentation.

- Your PC might not have the UTM configured as its TCP/IP gateway.

Troubleshoot a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your PC or workstation.

Test the LAN Path to Your UTM

You can ping the UTM from your PC to verify that the LAN path to the UTM is set up correctly.

➢ **To ping the UTM from a PC running Windows 95 or later:**

1. From the Windows toolbar, click **Start** and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the UTM, for example:

   ping 192.168.1.1

3. Click **OK**. A message similar to the following should display:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you will see this message:

   ```
   Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you will see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in *LAN or WAN Port LEDs Not On* on page 493.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and UTM.

- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your UTM and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows Run dialog box, type:

> **ping -n 10 <IP address>**

in which `<IP address>` is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your UTM listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel.

- Check to see that the network address of your PC (the portion of the IP address that is specified by the netmask) is different from the network address of the remote device.

- Check that the modem or router is connected and functioning.

- If your ISP assigned a host name, system name, or account name to your PC, enter that name in the Account Name field on the WAN ISP Settings screen of the single WAN port models or on one of the WAN ISP Settings screens of the multiple WAN port models. You might also have to enter the assigned domain name or workgroup name in the Domain Name field, and you might have to enter additional information. For more information, see *Manually Configure the Internet Connection* on page 71.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you need to configure your UTM to *clone* or *spoof* the MAC address from the authorized PC. You can do this in the Router's MAC Address section on the WAN Advanced Options screen of the single WAN port models or on one of the WAN Advanced Options screens of the multiple WAN port models. For more information, see *Configure Advanced WAN Options* on page 90.

Restore the Default Configuration and Password

To reset the UTM to the original factory default settings, you can use one of the following two methods:

- Press the factory default reset button on the rear panel of the UTM (see *Rear Panel UTM5, UTM10, and UTM25* on page 30, *Rear Panel UTM50 and UTM150* on page 31, or *Rear Panel UTM9S* on page 31) and hold the button for about 8 seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default settings when you do not know the administration password or IP address, you need to use the factory default reset button method.

- On the Backup & Restore Settings screen, next to Revert to factory defaults settings, click the **Default** button:

  a. To display the Backup & Restore Settings screen, select **Administration > Backup & Restore Settings**. The Backup & Restore Settings screen displays:
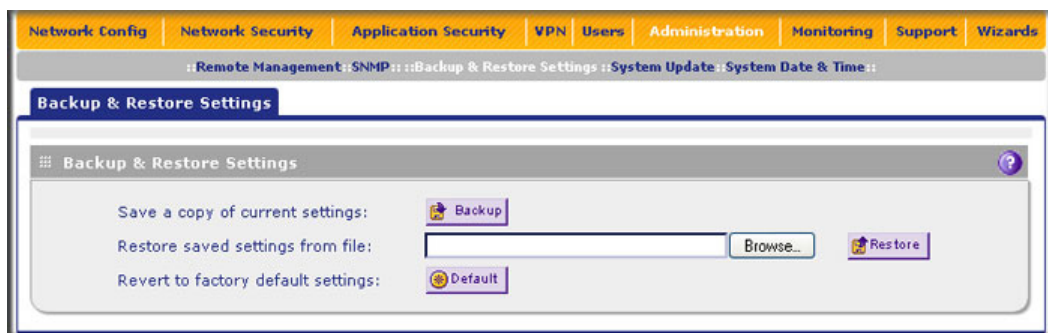
Figure 293.

  b. Click the **Default** button.

The UTM reboots. During the reboot process, the Backup & Restore Settings screen remains visible. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

> ⚠ **WARNING!**
>
> **When you press the hardware factory default reset button or click the software Default button, the UTM settings are erased. All firewall rules, VPN policies, LAN/WAN settings, and other settings are lost. Back up your settings if you intend on using them.**

Note: After rebooting with factory default settings, the UTM's password is **password**, and the LAN IP address is **192.168.1.1**.

Problems with Date and Time

The System Date & Time screen displays the current date and time of day (see *Configure Date and Time Service* on page 412). The UTM uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day.

Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The UTM has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the UTM, wait at least 5 minutes and check the date and time again.

- Time is off by 1 hour. Cause: The UTM does not automatically sense daylight savings time. Go to the System Date & Time screen, and select or clear the **Automatically Adjust for Daylight Savings Time** check box.

Use Online Support

The UTM includes online support tools that allow NETGEAR technical support to securely perform diagnostics of the UTM, and that let you submit suspicious files for analysis by NETGEAR. You can also access the knowledge base and documentation online.

Enable Remote Troubleshooting

One of the advanced features that the UTM provides is online support through a support tunnel. With this feature, NETGEAR technical support staff are able to analyze from a remote location any difficulty you might be experiencing with the UTM and to perform advanced diagnostics. Make sure that ports 443 and 2222 are open on your firewall, and that you have the support key that was given to you by NETGEAR.

➢ **To initiate the support tunnel:**

1. Select **Support > Online Support**. The Online Support screen displays:
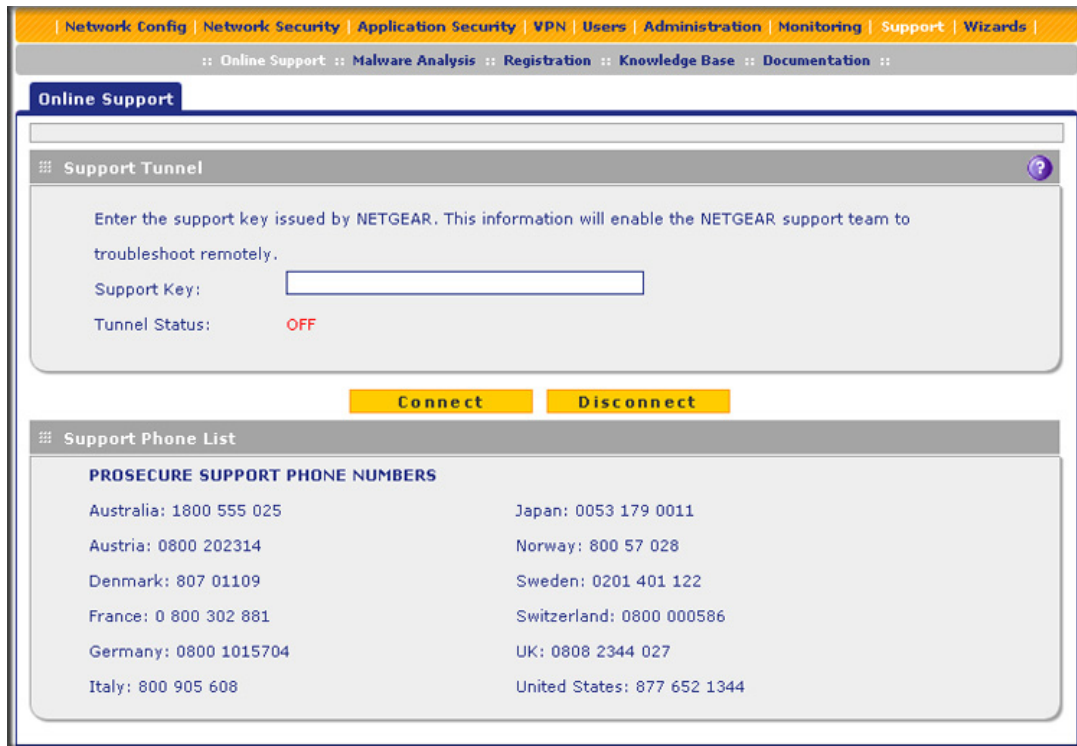
Figure 294.

2. In the Support Key field, enter the support key that was given to you by NETGEAR.

3. Click **Connect**. When the tunnel is established, the tunnel status field displays ON.

To terminate the tunnel, click **Disconnect**. The tunnel status field displays OFF.

If NETGEAR technical support cannot access the UTM remotely, they might ask you to save a log file to your computer and then email it to NETGEAR for analysis (see *Gather Important Log Information* on page 489).

Send Suspicious Files to NETGEAR for Analysis

You can report any undetected malware file or malicious email to NETGEAR for analysis. The file is compressed and password-protected before it is sent.

➢ **To submit a file to NETGEAR for analysis:**

1. Select **Support > Malware Analysis**. The Online Support screen displays:
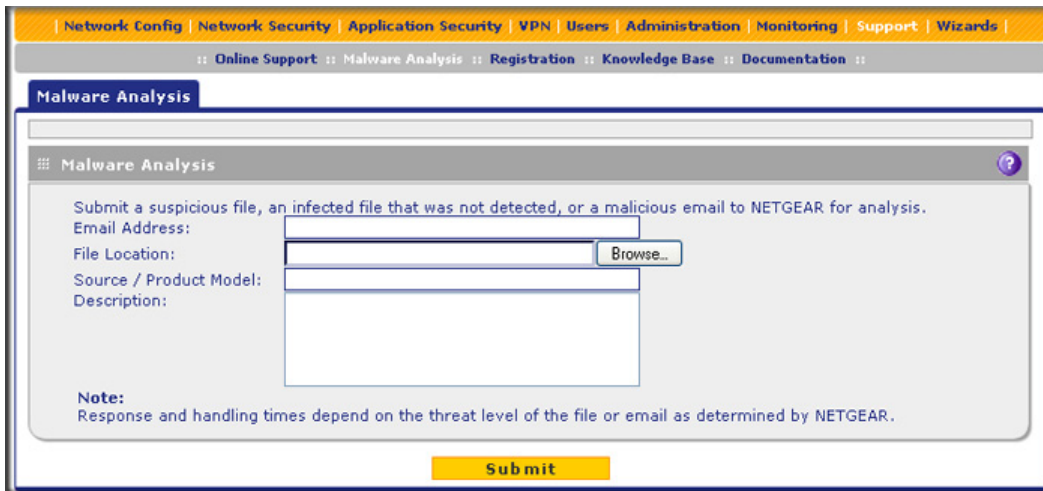
Figure 295.

2. Enter the settings as explained in the following table:

Table 128. Malware Analysis screen settings

Setting	Description
Email Address	The email address of the submitter to enable NETGEAR to contact the submitter if needed.
File Location	Click **Browse** to navigate to the file that you want to submit to NETGEAR.
Source / Product Model	Specify where the file originated (for example, an email address if received through email) and, if known, which product or scan feature (for example, the UTM or a desktop antivirus application) detected the file.
Description	As an option, include a description or any information that is relevant.

3. Click **Submit**.

Access the Knowledge Base and Documentation

To access NETGEAR's knowledge base for the UTM, select **Support > Knowledge Base**. To access NETGEAR's documentation library for your UTM model, select **Support > Documentation**.

xDSL Module for the UTM9S

<div style="text-align:right;">**A**</div>

This appendix describes how to configure the DSL interface of the UTM9SDSL xDSL module that installs in an UTM9S. This appendix includes the following sections:

- *xDSL Module Configuration Tasks*
- *Configure the xDSL Settings*
- *Automatically Detecting and Connecting the Internet Connection*
- *Manually Configure the Internet Connection*
- *Configure the WAN Mode*
- *Configure Secondary WAN Addresses*
- *Configure Dynamic DNS*
- *Configure Advanced WAN Options*

> **Note:** The UTM9S has both WAN interfaces and a DSL interface. For information about configuring the WAN interfaces of the UTM9S, see *Chapter 3, Manually Configuring Internet and WAN Settings*.

xDSL Module Configuration Tasks

Generally, six steps are required to complete the DSL Internet connection of your UTM9S.

➢ **Complete these steps:**

1. **Configure the xDSL settings**. Before you can configure the DSL Internet connection to your ISP, you need to configure the xDSL settings. See *Configure the xDSL Settings* on page 503.

2. **Configure the Internet connection to your ISP**. During this phase, you connect to your ISP. See *Automatically Detecting and Connecting the Internet Connection* on page 505 or *Manually Configure the Internet Connection* on page 508.

3. **Configure the WAN mode**. Select either NAT or classical routing, and select dedicated (single WAN) mode, or, if you also have configured another WAN interface, auto-rollover mode or load balancing mode. For load balancing, you can also select any necessary protocol bindings. See *Configure the WAN Mode* on page 512.

4. **Configure secondary WAN addresses on the WAN port (optional)**. Configure aliases for the WAN port. See *Configure Secondary WAN Addresses* on page 521.

5. **Configure Dynamic DNS on the WAN port (optional)**. Configure your fully qualified domain names during this phase (if required). See *Configure Dynamic DNS* on page 523.

6. **Configure the WAN options (optional)**. Optionally, you can enable the WAN port to respond to a ping, and you can change the factory default MTU size and port speed. However, these are advanced features, and changing them is not usually required. See *Configure Advanced WAN Options* on page 526.

Each of these tasks is detailed separately in this appendix.

> **Note:** For information about how to configure the WAN meter, see *Enable the WAN Traffic Meter* on page 419.

Configure the xDSL Settings

Before you can configure the DSL Internet connection to your ISP, you need to configure the ADSL or VDSL settings and, if required, the ATM multiplexing method. These settings are usually provided by your ISP, but you can autodetect these settings.

> **Note:** Autodetecting the DSL settings takes about 25 minutes.

➢ **To configure the xDSL settings:**

1. Select **Network Config > WAN Settings**. The WAN screen displays (see *Figure 297* on page 505).

2. Click the **Edit** button in the Action column of the SLOT-x interface. The SLOT-x ISP Settings screen displays (see *Figure 298* on page 506).

3. Select the **xDSL Settings** option arrow. The xDLS Settings screen displays:
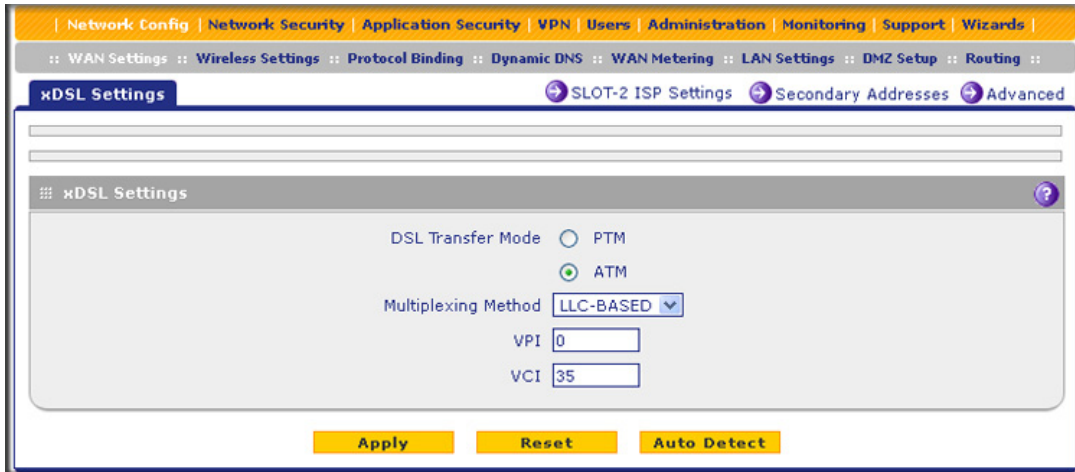
Figure 296.

4. Either click **Auto Detect** or, if you have the correct settings, enter the settings as explained in the following table:

Table 129. xDSL settings

Setting	Description
DSL Transfer Mode	Select one of the following DSL transfer methods: • **PTM**. Packet Transfer Mode (PTM) has a functionality that is similar to packet-switched networking and does not use multiplexing. • **ATM**. Asynchronous Transfer Mode (ATM) uses Asynchronous Time-Division Multiplexing (ATDM) to encode data into small, fixed-sized cells. ATM has a functionality that is similar to circuit-switched networking and small-packet-switched networking. When you select ATM, you also need to configure the multiplexing method, VPI, and VCI.

	Multiplexing Method	Select the VDSL multiplexing method for the ATM mode: • **LLC-BASED**. Multiplexing is based on Logical Link Control (LLC) encapsulation. • **VC-BASED**. Multiplexing is based on use of a virtual circuit (VC).
	VPI	The Virtual Path Identifier (VPI) that is used for the VDSL connection.
	VCI	The Virtual Channel Identifier (VCI) that is used for the VDSL connection.

5. Click **Apply** to save your settings.

Automatically Detecting and Connecting the Internet Connection

To set up your UTM9S for secure Internet connections, the web management interface provides the option to automatically detect the network connection and configure the xDSL port. You can also manually configure the Internet connection and port (see *Manually Configure the Internet Connection* on page 508).

➢ **To automatically configure the WAN port for connection to the Internet:**

1. Select **Network Config > WAN Settings**. The WAN screen displays.

Figure 297.

The xDSL module is installed in one of the two slots (SLOT-1 or SLOT-2). The WAN Settings table displays the following fields:

- **WAN**. The WAN or DSL interface.

- **Status**. The status of the WAN or DSL interface (UP or DOWN).

- **WAN IP**. The IP address of the WAN or DSL interface.

- **Failure Detection Method**. The failure detection method that is active for the WAN or DSL interface. The following methods can be displayed:
  - None
  - DNS Lookup (WAN DNS Servers)
  - DNS Lookup (the configured IP address is displayed)
  - PING (the configured IP address is displayed)

  You can set the failure detection method for the DSL interface on the corresponding WAN Advanced Options screen (see *Configure Auto-Rollover Mode and the Failure Detection Method* on page 514).

- **Action**. The Edit button in the Action column of the SLOT-x entry provides access to the xDSL ISP Settings screen (see *step 2*); the Status button provides access to the Connection Status screen (see *step 4*) for the DSL interface.

2. Click the **Edit** button in the Action column of the SLOT-x entry to automatically configure the connection to the Internet. The SLOT-x ISP Settings screen displays. (The following figure shows the SLOT-2 ISP Settings screen.)
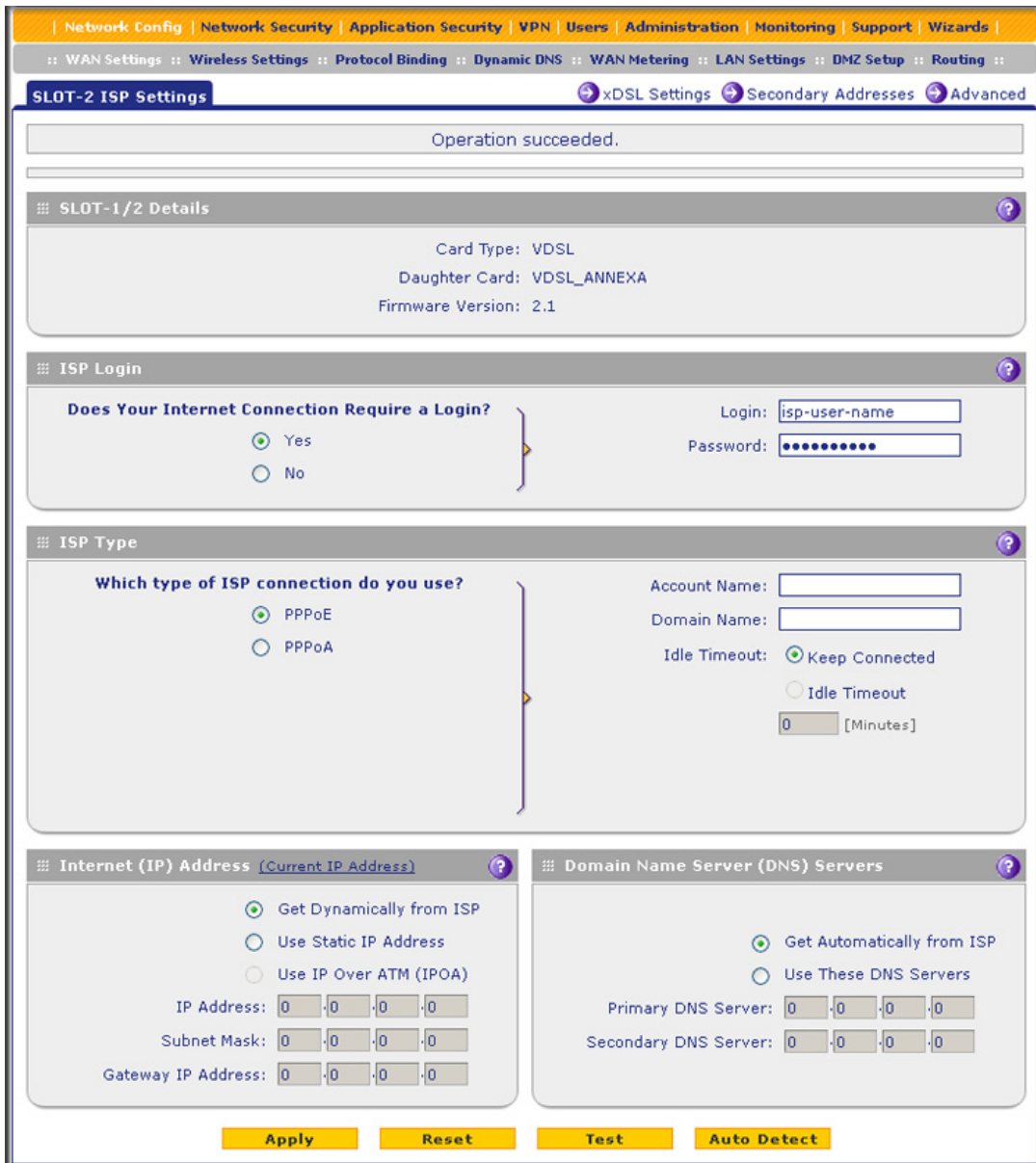
Figure 298.

3. Click the **Auto Detect** button at the bottom of the screen. The autodetect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support.

The autodetect process returns one of the following results:

- If the autodetect process is successful, a status bar at the top of the screen displays the results (for example, *DHCP service detected*).

- If the autodetect process senses a connection method that requires input from you, it prompts you for the information. All methods with their required settings are explained in the following table:

Table 130. Internet connection methods

Connection method	Manual data input required
DHCP (Dynamic IP)	No data is required.
PPPoA	Login, password, account name, and domain name. **Note:** PPPoA is supported on the UTM9S only.
PPPoE	Login, password, account name, and domain name.
Fixed (Static) IP	IP address, subnet mask, and gateway IP address, and related data supplied by your ISP.

- If the autodetect process does not find a connection, you are prompted either to check the physical connection between the xDSL module and the telephone line or to check your UTM9S's MAC address. For more information, see *Configure the xDSL Settings* on page 503, *Configure the WAN Mode* on page 512, and *Troubleshoot the ISP Connection* on page 494.

4. To verify the connection:

    a. Return to the WAN screen by selecting **Network Config > WAN Settings**.

    b. Click the **Status** button in the Action column of the SLOT-x entry to display the Connection Status pop-up screen.
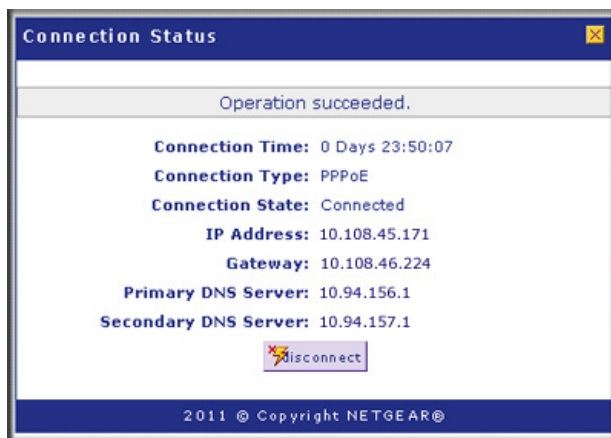
Figure 299.

The Connection Status screen should show a valid IP address and gateway. If the configuration was not successful, skip ahead to *Manually Configure the Internet Connection* on page 508, or see *Troubleshoot the ISP Connection* on page 494.

Note: If the configuration process was successful, you are connected to the Internet through the DSL interface that you just configured.

Note: For more information about the WAN Connection Status screen, see *View the WAN Ports Status* on page 456.

If the automatic ISP configuration is successful, you can skip ahead to *Configure the WAN Mode* on page 512.

If the automatic ISP configuration fails, you can attempt a manual configuration as described in *Manually Configure the Internet Connection* on this page, or see *Troubleshoot the ISP Connection* on page 494.

Set the UTM's MAC Address

Each computer or router on your network has a unique 48-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. The default is set to Use Default Address on the WAN Advanced Options screens. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then you need to enter that address on the WAN Advanced Options screen for the DSL interface (see *Configure Advanced WAN Options* on page 526).

Manually Configure the Internet Connection

Unless your ISP automatically assigns your configuration through DHCP, you need to obtain configuration parameters from your ISP to manually establish an Internet connection over the DSL interface. The necessary parameters for various connection types are listed in *Table 130* on page 507.

➢ **To manually configure the WAN ISP settings for the DSL interface:**

1. Select **Network Config > WAN Settings**. The WAN screen displays:

Figure 300.

2. Click the **Edit** button in the Action column of the SLOT-x interface. The SLOT-x ISP Settings screen displays (see *Figure 298* on page 506).

---

3. Locate the ISP Login section on the screen:

Figure 301.

In the ISP Login section, select one of the following options:

- If your ISP requires an initial login to establish an Internet connection, select **Yes**. (The default is No.)
- If a login is not required, select **No**, and ignore the Login and Password fields.

4. If you selected Yes, enter the login name in the Login field and the password in the Password field. This information is provided by your ISP.

5. In the ISP Type section of the screen, select the type of ISP connection that you use from the two listed options. By default, PPPoE is selected, as shown in the following figure:
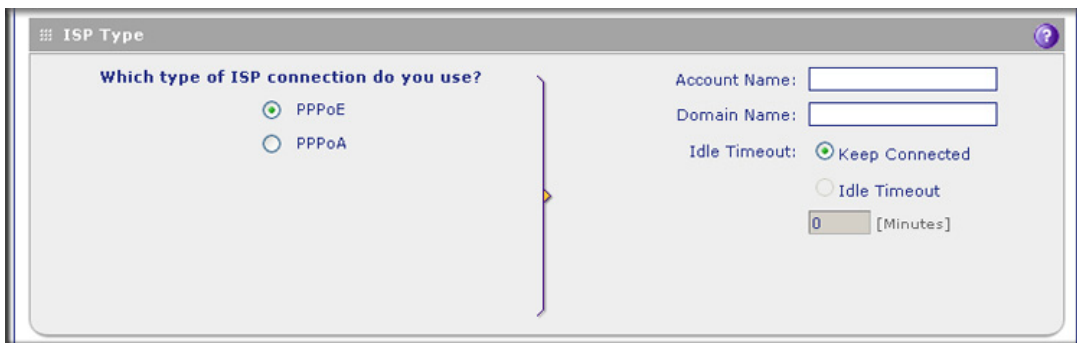
Figure 302.

6. If your connection is Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA), your ISP requires an initial login. Enter the settings as explained in the following table:

Table 131. PPPoE and PPPoA settings

Setting	Description	
PPPoE	If your ISP uses PPPoE for login, select this radio button, and enter the following settings:	
	Account Name	The account name for the PPPoE connection.
	Domain Name	The name of your ISP's domain or your domain name if your ISP has assigned you one. You can leave this field blank.

Table 131. PPPoE and PPPoA settings (continued)

Setting	Description	
PPPoE (continued)	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Timeout** radio button and, in the time-out field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in. **Note:** When you use a PPPoE connection and select the Idle Timeout radio button, you cannot configure load balancing (see *Configure Load Balancing* on page 518). To use load balancing on a PPPoE connection, select the **Keep Connected** radio button. When you have configured load balancing, the Idle Timeout radio button and time-out field are masked out.
PPPoA	If your ISP uses PPPoA for login, select this radio button, and enter the following settings:	
	Account Name	The account name for the PPPoA connection.
	Domain Name	The name of your ISP's domain or your domain name if your ISP has assigned you one. You can leave this field blank.
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Timeout** radio button and, in the time-out field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in. **Note:** When you use a PPPoA connection and select the Idle Timeout radio button, you cannot configure load balancing (see *Configure Load Balancing* on page 518). To use load balancing on a PPPoA connection, select the **Keep Connected** radio button. When you have configured load balancing, the Idle Timeout radio button and time-out field are masked out.

7. In the Internet (IP) Address section of the screen (see the following figure), configure the IP address settings as explained in the following table. Click the **Current IP Address** link to see the currently assigned IP address.
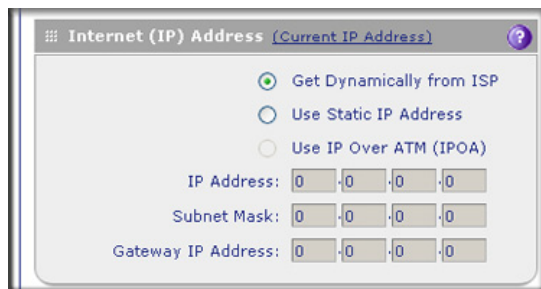
Table 132. Internet IP address settings

Setting	Description	
Get Dynamically from ISP	If your ISP has not assigned you a static IP address, select the **Get Dynamically from ISP** radio button. The ISP automatically assigns an IP address to the UTM9S using DHCP network protocol.	
Use Static IP Address	If your ISP has assigned you a fixed (static or permanent) IP address, select the **Use Static IP Address** radio button, and enter the following settings:	
	IP Address	Static IP address assigned to you. This address identifies the UTM9S to your ISP.
	Subnet Mask	The subnet mask is usually provided by your ISP.
	Gateway IP Address	The IP address of the ISP's gateway is usually provided by your ISP.
Use IP Over ATM (IPOA)	If your ISP uses IP over ATM (IPoA), select the **Use IP Over ATM (IPOA)** radio button, and enter the following settings:	
	IP Address	The IP address assigned to you. This address identifies the UTM9S to your ISP.
	Subnet Mask	The subnet mask is usually provided by your ISP.
	Gateway IP Address	The IP address of the ISP's gateway is usually provided by your ISP.

8. In the Domain Name Server (DNS) Servers section of the screen (see the following figure), specify the DNS settings as explained in the following table.

Figure 303.

Table 133. DNS server settings

Setting	Description
Get Automatically from ISP	If your ISP has not assigned any Domain Name Server (DNS) addresses, select the **Get Automatically from ISP** radio button.

Table 133. DNS server settings (continued)

Setting	Description	
Use These DNS Servers	If your ISP has assigned DNS addresses, select the **Use These DNS Servers** radio button. Make sure that you fill in valid DNS server IP addresses in the fields. Incorrect DNS entries might cause connectivity issues.	
	Primary DNS Server	The IP address of the primary DNS server.
	Secondary DNS Server	The IP address of the secondary DNS server.

9. Click **Test** to evaluate your entries. The UTM9S attempts to make a connection according to the settings that you entered.

10. Click **Apply** to save any changes to the SLOT-x ISP settings. (Or click **Reset** to discard any changes and revert to the previous settings.)

When you are finished, click the **Logout** link in the upper right of the web management interface, or proceed to additional setup and management tasks.

Configure the WAN Mode

The UTM9S in which an xDSL module is installed supports both Ethernet WAN interfaces and an xDSL WAN interface. For information about how to configure the WAN interfaces, see *Chapter 3, Manually Configuring Internet and WAN Settings*.

If you have configured a WAN interface in addition to the DSL interface, the UTM9S can be configured on a mutually exclusive basis for either auto-rollover (for increased system reliability) or load balancing (for maximum bandwidth efficiency). If you do not select load balancing, you need to specify the DSL interface or one WAN interface as the primary interface.

- **Load balancing mode**. The UTM9S distributes the outbound traffic equally among the DSL and WAN interfaces that are functional. The UTM9S supports weighted load balancing and round-robin load balancing (see *Configure Load Balancing and Optional Protocol Binding* on page 517).

> **Note:** Scenarios could arise when load balancing needs to be bypassed for certain traffic or applications. If certain traffic needs to travel on the DSL interface or a specific WAN interface, configure protocol binding rules for that interface. The rule should match the desired traffic.

- **Primary WAN mode**. The DSL interface (or a WAN interface) is made the primary interface. The other interfaces are disabled.
- **Auto-rollover mode**. The selected DSL or WAN interface is defined as the primary link, and another interface needs to be defined as the rollover link. Because there are three

interfaces on the UTM9S (one DSL and two WAN interfaces), the one remaining interface is disabled. As long as the primary link is up, all traffic is sent over the primary link. When the primary link goes down, the rollover link is brought up to send the traffic. When the primary link comes back up, traffic automatically rolls back to the original primary link.

If you want to use a redundant ISP link for backup purposes, select the DSL or WAN interface that needs to function as the primary link for this mode. Ensure that the backup interface has also been configured and that you configure the WAN failure detection method on the WAN Advanced Options screen to support auto-rollover (see *Configure Auto-Rollover Mode and the Failure Detection Method* on page 514).

Whichever WAN mode you select, you also need to select either NAT or classical routing, as explained in the following sections.

> **WARNING!**
>
> **When you change the WAN mode, the UTM9S restarts. If you change from primary WAN mode to load balancing mode, or the other way around, the interface through which you can access the UTM9S might change. Take note of the IP addresses of the interfaces before you change the WAN mode.**

Configure Network Address Translation

Network Address Translation (NAT) allows all PCs on your LAN to share a single public Internet IP address. From the Internet, there is only a single device (the UTM9S) and a single IP address. PCs on your LAN can use any private IP address range, and these IP addresses are not visible from the Internet.

Note the following about NAT:

- The UTM9S uses NAT to select the correct PC (on your LAN) to receive any incoming data.
- If you have only a single public Internet IP address, you need to use NAT (the default setting).
- If your ISP has provided you with multiple public IP addresses, you can use one address as the primary shared address for Internet access by your PCs, and you can map incoming traffic on the other public IP addresses to specific PCs on your LAN. This one-to-one inbound mapping is configured using an inbound firewall rule.

> **WARNING!**
>
> **Changing the WAN mode from classical routing to NAT causes all LAN WAN and DMZ WAN inbound rules to revert to default settings.**

➢ **To configure NAT:**

1. Select **Network Config > WAN Settings > WAN Mode**. The WAN Mode screen displays (see *Figure 304* on page 515).

2. In the NAT (Network Address Translation) section of the screen, select the **NAT** radio button.

3. Click **Apply** to save your settings.

Configure Classical Routing

In classical routing mode, the UTM9S performs routing, but without NAT. To gain Internet access, each PC on your LAN needs to have a valid static Internet IP address.

If your ISP has allocated a number of static IP addresses to you, and you have assigned one of these addresses to each PC, you can choose classical routing. Or, you can use classical routing for routing private IP addresses within a campus environment.

To view the status of the WAN ports, you can view the Router Status screen (see *View the System Status* on page 439).

⚠️ **WARNING!**

Changing the WAN mode from NAT to classical routing causes all LAN WAN and DMZ WAN inbound rules to revert to default settings.

➢ **To configure classical routing:**

1. Select **Network Config > WAN Settings > WAN Mode**. The WAN Mode screen displays (see *Figure 304* on page 515).

2. In the NAT (Network Address Translation) section of the screen, select the **Classical Routing** radio button.

3. Click **Apply** to save your settings.

Configure Auto-Rollover Mode and the Failure Detection Method

To use a redundant ISP link for backup purposes, ensure that the backup DSL or WAN interface has already been configured. Then select the DSL or WAN interface that should function as the primary link for this mode, and configure the WAN failure detection method on the WAN Mode screen to support auto-rollover.

When the UTM9S is configured in auto-rollover mode, it uses the selected WAN failure detection method to detect the status of the primary link connection at regular intervals. Link failure is detected in one of the following ways:

• DNS queries sent to a DNS server

• Ping request sent to an IP address

- None (no failure detection is performed)

From the primary interface, DNS queries or ping requests are sent to the specified IP address. If replies are not received after a specified number of retries, the primary interface is considered down, and a rollover to the backup interface occurs. When the primary interface comes back up, another rollover occurs from the backup interface back to the primary interface. The WAN failure detection method that you select applies only to the primary interface, that is, it monitors the primary link only.

Configure Auto-Rollover Mode

➢ **To configure auto-rollover mode:**

1. Select **Network Config > WAN Settings** > **WAN Mode**. The WAN Mode screen displays:
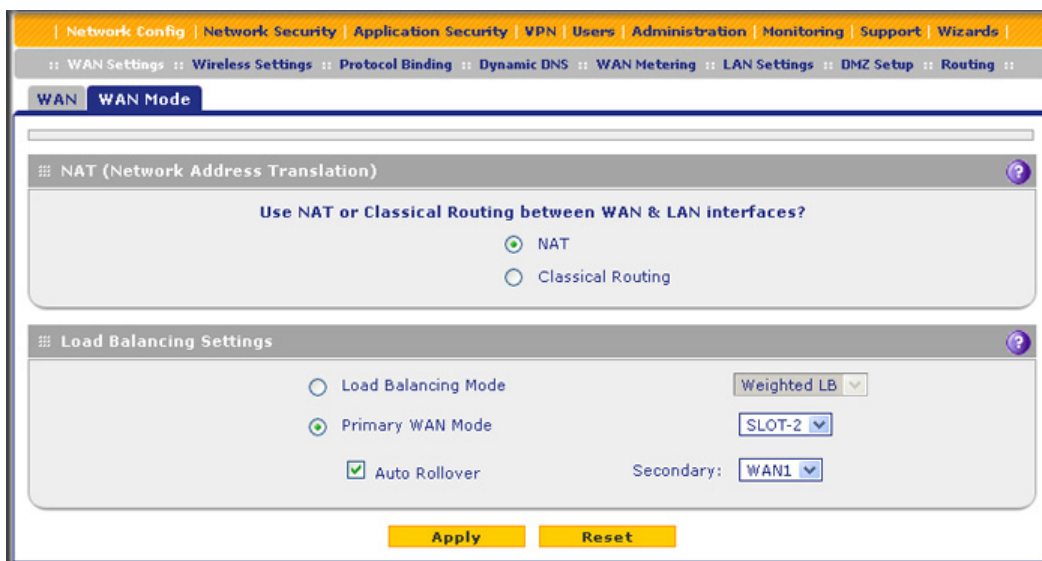
Figure 304.

2. In the Load Balancing Settings section of the screen, configure the following settings:
   a. Select the **Primary WAN Mode** radio button.
   b. From the corresponding drop-down list on the right, select the DSL interface or a WAN interface to function as the primary WAN interface. If you select the DSL interface, both WAN interfaces become disabled; if you select a WAN interface, both the DSL interface and the other WAN interface become disabled.
   c. Select the **Auto Rollover** check box.
   d. From the corresponding drop-down list on the right, select a WAN interface or the DSL interface to function as the backup interface.

   Note: Ensure that the backup interface is configured before enabling auto-rollover mode.

3. Click **Apply** to save your settings.

Configure the Failure Detection Method

➢ **To configure the failure detection method:**

1. Select **Network Config > WAN Settings**. The WAN screen displays (see *Figure 297* on page 505).

2. Click the **Edit** button in the Action column of the interface that you selected as the primary interface (see *Figure 298* on page 506, which shows the SLOT-2 ISP Settings screen as an example).

3. Click the **Advanced** option arrow at the upper right of the screen. The WAN Advanced Options screen displays for the interface that you selected. (For an image of the entire screen, see *Figure 312* on page 527, which shows the WAN Advanced Options screen for the DSL interface.)

4. Locate the Failure Detection Method section on the screen (see the following figure). Enter the settings as explained in the following table.
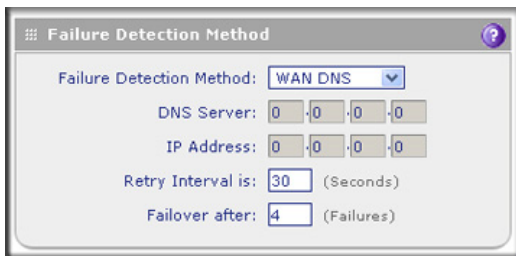
Figure 305.

Table 134. Failure detection method settings

Setting	Description	
WAN Failure Detection Method Select a failure detection method from the drop-down list. DNS queries or pings are sent through the interface that is being monitored. The retry interval and number of failover attempts determine how quickly the UTM9S switches from the primary link to the backup link in case the primary link fails, or when the primary link comes back up, switches back from the backup link to the primary link.		
WAN DNS	DNS queries are sent to the DNS server that is configured in the Domain Name Server (DNS) Servers section of the WAN ISP screen (see *Manually Configure the Internet Connection* on page 508).	
Custom DNS	DNS queries are sent to the specified DNS server.	
	DNS Server	The IP address of the DNS server.
Ping	Pings are sent to a server with a public IP address. This server should not reject the ping request and should not consider ping traffic to be abusive.	
	IP Address	The IP address of the ping server.

Table 134. Failure detection method settings (continued)

Setting	Description
Retry Interval is	The retry interval in seconds. The DNS query or ping is sent periodically after every test period. The default test period is 30 seconds.
Failover after	The number of failover attempts. The primary WAN interface is considered down after the specified number of queries have failed to elicit a reply. The backup interface is brought up after this situation has occurred. The failover default is 4 failures.

Note: The default time to roll over after the primary interface fails is 2 minutes. The minimum test period is 30 seconds, and the minimum number of tests is 4.

5. Click **Apply** to save your settings.

Note: You can configure the UTM to generate a WAN status log and email this log to a specified address (see *Configure Logging, Alerts, and Event Notifications* on page 422).

Configure Load Balancing and Optional Protocol Binding

To use multiple ISP links simultaneously, configure load balancing. In load balancing mode, the DSL interface or any WAN interface carries any outbound protocol unless protocol binding is configured.

When a protocol is bound to a particular interface, all outgoing traffic of that protocol is directed to the bound interface. For example, if the HTTPS protocol is bound to the DSL interface and the FTP protocol is bound to the WAN1 interface, then the UTM9S automatically routes all outbound HTTPS traffic from the computers on the LAN through the DSL interface. All outbound FTP traffic is routed through the WAN1 interface.

Protocol binding addresses two issues:

- Segregation of traffic between links that are not of the same speed.
  High-volume traffic can be routed through the DSL interface connected to a high-speed link, and low-volume traffic can be routed through a WAN interface connected to a low-speed link.

- Continuity of source IP address for secure connections.
  Some services, particularly HTTPS, cease to respond when a client's source IP address changes shortly after a session has been established.

Configure Load Balancing

> **To configure load balancing:**

1. Select **Network Config > WAN Settings > WAN Mode**. The WAN Mode screen displays:
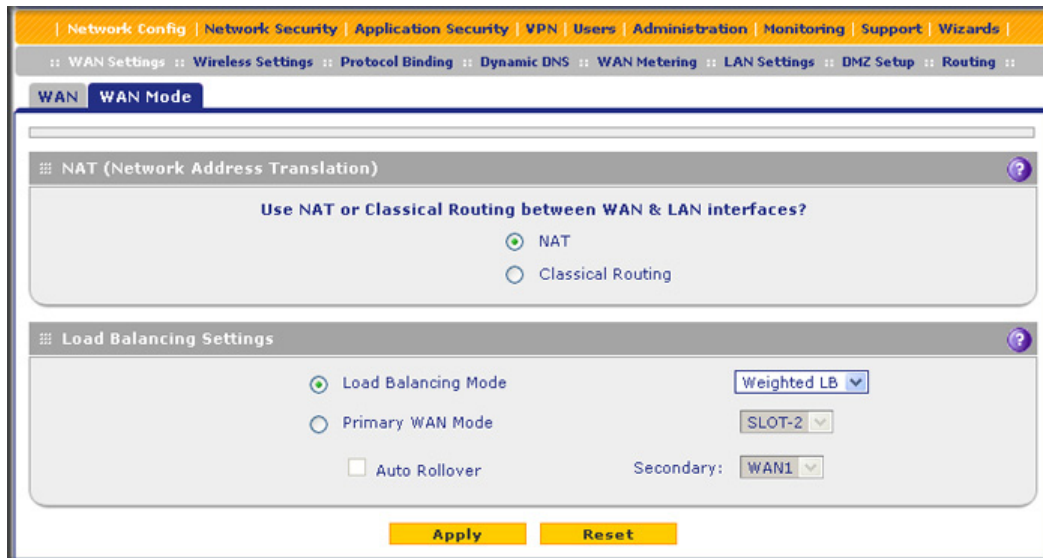
Figure 306.

> **Note:** You cannot configure load balancing when you use a PPPoE or PPPoA connection and have selected the Idle Timeout radio button on the WAN ISP Settings screen (single WAN port models) or on one of the WAN ISP Settings screens (multiple WAN port models); to use load balancing on a PPPoE or PPPoA connection, select the **Keep Connected** radio button. For more information, see *Figure 302* on page 509 and the accompanying PPPoE and PPPoA information in *Table 131* on page 509.

---

2. In the Load Balancing Settings section of the screen, configure the following settings:

  a. Select the **Load Balancing Mode** radio button.

  b. From the corresponding drop-down list on the right, select one of the following load balancing methods:

- **Weighted LB**. With weighted load balancing, balance weights are calculated based on DSL or WAN link speed and available DSL or WAN bandwidth. This is the default setting and the most efficient load-balancing algorithm.

- **Round-robin**. With round-robin load balancing, new traffic connections are sent over a DSL or WAN link in a serial method irrespective of bandwidth or link speed. For example if the DSL, WAN1, and WAN2 interfaces are active in round-robin load balancing mode, an HTTP request could first be sent over the DSL interface,

then a new FTP session could start on the WAN1 interface, and then any new connection to the Internet could be made on the WAN2 interface. This load-balancing method ensures that a single interface does not carry a disproportionate distribution of sessions.

3. Click **Apply** to save your settings.

Configure Protocol Binding (Optional)

➢ **To configure protocol binding and add protocol binding rules:**

1. Select **Network Config > Protocol Binding**. The Protocol Bindings screen displays. (The following figure shows two examples in the Protocol Bindings table.)
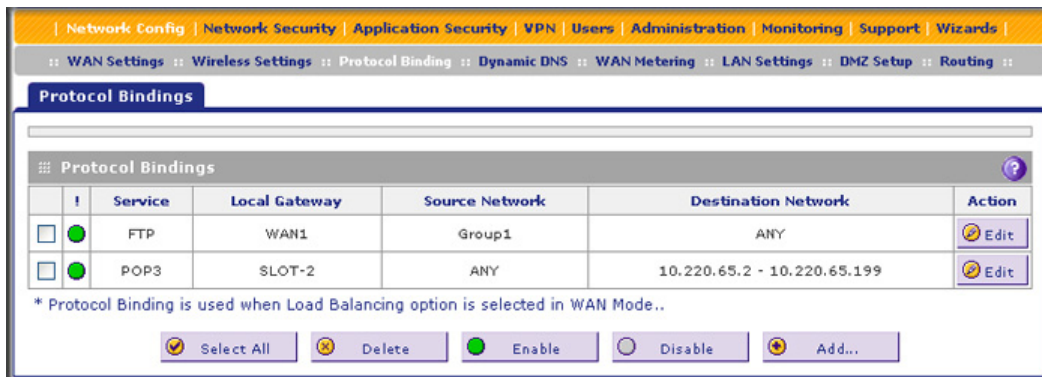
Figure 307.

The Protocol Bindings table displays the following fields:

- **Check box**. Allows you to select the protocol binding rule in the table.
- **Status icon**. Indicates the status of the protocol binding rule:
  - **Green circle**. The protocol binding rule is enabled.
  - **Gray circle**. The protocol binding rule is disabled.
- **Service**. The service or protocol for which the protocol binding rule is set up.
- **Local Gateway**. The WAN interface to which the service or protocol is bound.
- **Source Network**. The computers on your network that are affected by the protocol binding rule.
- **Destination Network**. The Internet locations (based on their IP address) that are covered by the protocol binding rule.
- **Action**. The Edit button provides access to the Edit Protocol Binding screen for the corresponding service.

2. Click the **Add** table button below the Protocol Bindings table. The Add Protocol Binding screen displays:

Figure 308.

3. Configure the protocol binding settings as explained in the following table:

Table 135. Add Protocol Binding screen settings

Setting	Description	
Service	From the drop-down list, select a service or application to be covered by this rule. If the service or application does not appear in the list, you need to define it using the Services screen (see *Service-Based Rules* on page 123).	
Local Gateway	From the drop-down list, select the DSL interface or one of the WAN interfaces.	
Source Network	The source network settings determine which computers on your network are affected by this rule. Select one of the following options from the drop-down list:	
	Any	All devices on your LAN.
	Single address	In the Start IP field, enter the IP address to which the rule is applied.
	Address Range	In the Start IP field and End IP field, enter the IP addresses for the range to which the rule is applied.
	Group 1–Group 8	If this option is selected, the rule is applied to the devices that are assigned to the selected group. **Note:** You can also assign a customized name to a group (see *Change Group Names in the Network Database* on page 110).
Destination Network	The destination network settings determine which Internet locations (based on their IP address) are covered by the rule. Select one of the following options from the drop-down list:	
	Any	All Internet IP address.
	Single address	In the Start IP field, enter the IP address to which the rule is applied.
	Address range	In the Start IP field and End IP field, enter the IP addresses for the range to which the rule is applied.

4. Click **Apply** to save your settings. The protocol binding rule is added to the Protocol Bindings table. The rule is automatically enabled, which is indicated by the ! status icon, a green circle.

➢ **To edit a protocol binding:**

1. On the Protocol Bindings screen (see *Figure 307* on page 519), in the Protocol Bindings table, click the **Edit** table button to the right of the binding that you want to edit. The Edit Protocol Binding screen displays. This screen shows the same fields as the Add Protocol Binding screen (see the previous figure).

2. Modify the settings as explained in the previous table.

3. Click **Apply** to save your settings.

➢ **To enable, disable, or delete one or more protocol bindings:**

1. On the Protocol Bindings screen (see *Figure 307* on page 519), select the check box to the left of each protocol binding that you want to enable, disable, or delete, or click the **Select All** table button to select all bindings.

2. Click one of the following table buttons:
    *   **Enable**. Enables the binding or bindings. The ! status icon changes from a gray circle to a green circle, indicating that the selected binding or bindings are enabled. (By default, when a binding is added to the table, it is automatically enabled.)
    *   **Disable**. Disables the binding or bindings. The ! status icon changes from a green circle to a gray circle, indicating that the selected binding or bindings are disabled.
    *   **Delete**. Deletes the binding or bindings.

Configure Secondary WAN Addresses

You can set up a single WAN Ethernet port to be accessed through multiple IP addresses by adding aliases to the port. An alias is a secondary WAN address. One advantage is, for example, that you can assign different virtual IP addresses to a web server and an FTP server, even though both servers use the same physical IP address. You can add several secondary IP addresses to a single WAN port.

After you have configured secondary WAN addresses, these addresses are displayed on the following firewall rule screens:

*   In the WAN Destination IP Address drop-down lists of the following inbound firewall rule screens:
    -   Add LAN WAN Inbound Service screen
    -   Add DMZ WAN Inbound Service screen
*   In the NAT IP drop-down lists of the following outbound firewall rule screens:
    -   Add LAN WAN Outbound Service screen
    -   Add DMZ WAN Outbound Service screen

For more information about firewall rules, see *Use Rules to Block or Allow Specific Kinds of Traffic* on page 122).

It is important that you ensure that any secondary DSL addresses are different from the primary DSL, WAN, LAN, and DMZ IP addresses that are already configured on the UTM9S. However, primary and secondary DSL addresses can be in the same subnet. The following is an example of correctly configured IP addresses:

- Primary DSL IP address. 10.118.0.1 with subnet 255.255.255.0
- Secondary DSL IP address. 10.118.24.1 with subnet 255.255.255.0
- Primary WAN1 IP address. 10.215.74.1 with subnet 255.255.255.0
- Secondary WAN1 IP address. 10.215.81.1 with subnet 255.255.255.0
- DMZ IP address. 192.168.10.1 with subnet 255.255.255.0
- Primary LAN IP address. 192.168.1.1 with subnet 255.255.255.0
- Secondary LAN IP address. 192.168.2.1 with subnet 255.255.255.0

➢ **To add a secondary WAN address to the DSL interface:**

1. Select **Network Config > WAN Settings**. The WAN screen displays (see *Figure 297* on page 505).
2. Click the **Edit** button in the Action column of the SLOT-x entry. The WAN ISP Settings screen displays (see *Figure 298* on page 506, which shows the SLOT-2 ISP Settings screen as an example).
3. Click the **Secondary Addresses** option arrow at the upper right of the screen. The SLOT-x Secondary Addresses screen displays (see the following figure, which shows the SLOT-2 Secondary Addresses screen as an example, and which includes one entry in the List of Secondary WAN addresses table).
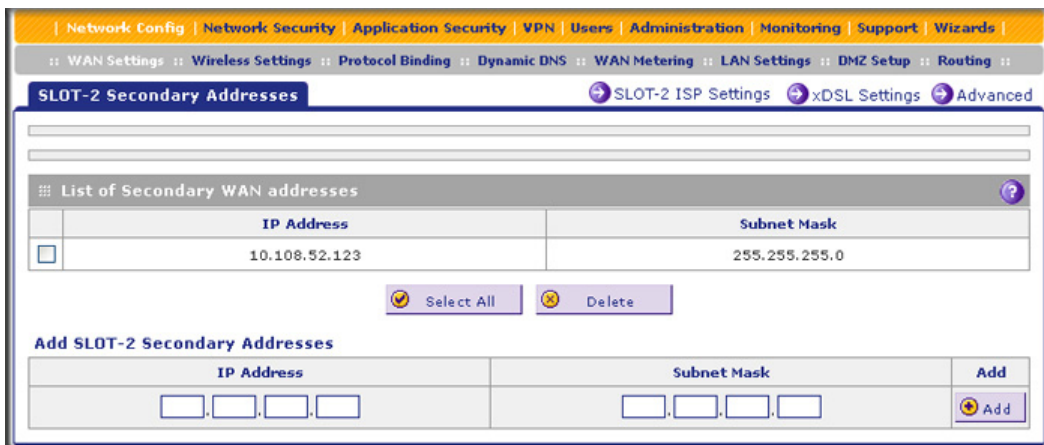
Figure 309.

The List of Secondary WAN addresses table displays the secondary LAN IP addresses added for the DSL interface.

4. In the Add SLOT-x Secondary Addresses section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the DSL interface.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.

5. Click the **Add** table button in the rightmost column to add the secondary IP address to the List of Secondary WAN addresses table.

   Repeat *step 4* and *step 5* for each secondary IP address that you want to add to the List of Secondary WAN addresses table.

➢ **To delete one or more secondary addresses:**

1. In the List of Secondary WAN addresses table, select the check box to the left of each address that you want to delete, or click the **Select All** table button to select all addresses.

2. Click the **Delete** table button.

Configure Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows devices with varying public IP addresses to be located using Internet domain names. To use DDNS, you need to set up an account with a DDNS provider such as DynDNS.org, TZO.com, Oray.net, or 3322.org. (Links to DynDNS, TZO, Oray, and 3322 are provided for your convenience as option arrows on the DDNS configuration screens.) The UTM9S firmware includes software that notifies DDNS servers of changes in the DSL IP address, so that the services running on this network can be accessed by others on the Internet.

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently—hence, the need for a commercial DDNS service, which allows you to register an extension to its domain, and restores DNS requests for the resulting fully qualified domain name (FQDN) to your frequently changing IP address.

After you have configured your account information on the UTM9S, when your ISP-assigned IP address changes, your UTM9S automatically contacts your DDNS service provider, logs in to your account, and registers your new IP address.

Consider the following:

- For auto-rollover mode, you need an FQDN to implement features such as exposed hosts and virtual private networks regardless of whether you have a fixed or dynamic IP address.

- For load balancing mode, you might still need an FQDN either for convenience or if you have a dynamic IP address.

> **Note:** If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the DDNS service does not work because private addresses are not routed on the Internet.

➢ To configure DDNS:

1. Select **Network Config > Dynamic DNS**. The Dynamic DNS screen displays (see the following figure).

   The WAN Mode section on the screen reports the currently configured WAN mode (for example, Single Port WAN1, Load Balancing, or Auto Rollover). Only those options that match the configured WAN mode are accessible on the screen.

2. Click the submenu tab for your DDNS service provider:
   - **Dynamic DNS** for DynDNS.org (which is shown in the following figure)
   - **DNS TZO** for TZO.com
   - **DNS Oray** for Oray.net
   - **3322 DDNS** for 3322.org

Figure 310.

3. Click the **Information** option arrow in the upper right of a DNS screen for registration information.

Figure 311.

4. Access the website of the DDNS service provider, and register for an account (for example, for DynDNS.org, go to *http://www.dyndns.com/*).

5. Configure the DDNS service settings for the DSL interface as explained in the following table:

Table 136. DNS service settings

Setting	Description	
SLOT-x (Dynamic DNS Status: ...)		
Change DNS to (DynDNS, TZO, Oray, or 3322)	Select the **Yes** radio button to enable the DDNS service. The fields that display on the screen depend on the DDNS service provider that you have selected. Enter the following settings:	
	Host and Domain Name	The host and domain name for the DDNS service.
	Username or User Email Address	The user name or email address for DDNS server authentication.
	Password or User Key	The password that is used for DDNS server authentication.
	Use wildcards	If your DDNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
	Update every 30 days	If your WAN IP address does not change often, you might need to force a periodic update to the DDNS service to prevent your account from expiring. If the **Update every 30 days** check box displays, select it to enable a periodic update.

6. Click **Apply** to save your configuration.

Configure Advanced WAN Options

The advanced options include configuring the maximum transmission unit (MTU) size, the port speed, and the UTM9S's MAC address, and setting a rate limit on the traffic that is being forwarded by the UTM9S.

> **Note:** You can also configure the failure detection method for the auto-rollover mode on the Advanced screen. This procedure is discussed in *Configure the Failure Detection Method* on page 516.

➢ **To configure advanced WAN options:**

1. Select **Network Config > WAN Settings**.
2. Click the **Edit** button in the Action column of the SLOT-x entry. The SLOT-x ISP Settings screen displays (see *Figure 298* on page 506, which shows the SLOT-2 ISP Settings screen as an example).

3. Click the **Advanced** option arrow in the upper right of the screen. The SLOT-x Advanced Options screen displays. (The following figure shows the SLOT-2 Advanced Options screen as an example.)
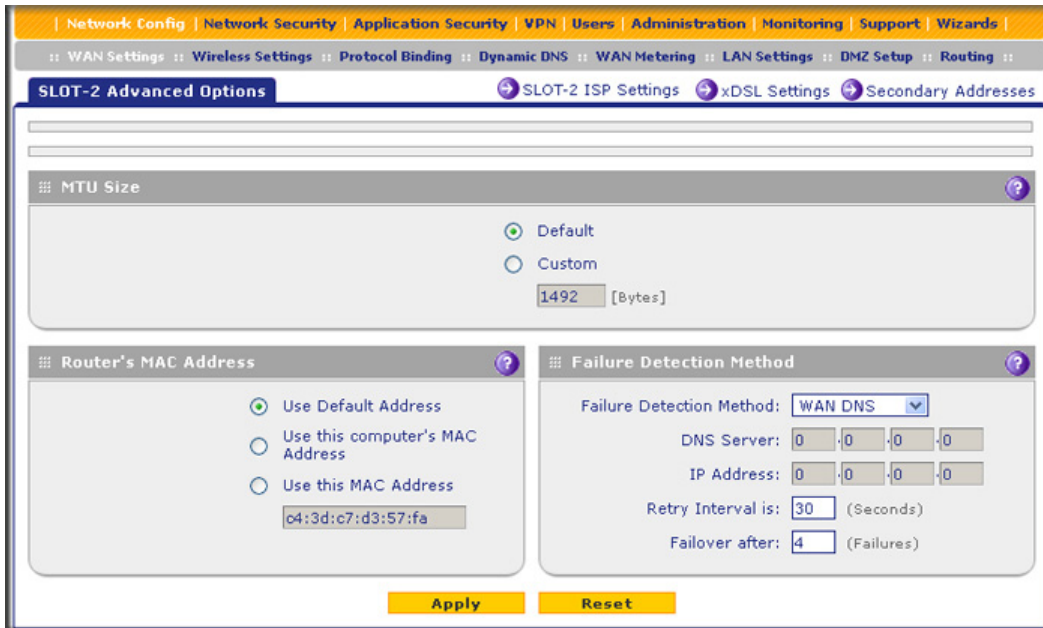
Figure 312.

4. Enter the settings as explained in the following table:

Table 137. Advanced DSL settings

Setting	Description
MTU Size Make one of the following selections:	
Default	Select the **Default** radio button for the normal maximum transmit unit (MTU) value. For most Ethernet networks this value is 1500 bytes, or 1492 bytes for PPPoE connections.
Custom	Select the **Custom** radio button, and enter an MTU value in the Bytes field. For some ISPs, you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
Router's MAC Address Make one of the following selections:	
Use Default Address	Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. To use the UTM9S's own MAC address, select the **Use Default Address** radio button.
Use this computer's MAC Address	Select the **Use this computer's MAC Address** radio button to allow the UTM9S to use the MAC address of the computer you are now using to access the web management interface. This setting is useful if your ISP requires MAC authentication.

Table 137. Advanced DSL settings (continued)

Setting	Description
Use this MAC Address	Select the **Use this MAC Address** radio button, and manually enter the MAC address in the field next to the radio button. You would typically enter the MAC address that your ISP is requiring for MAC authentication. **Note:** The format for the MAC address is 01:23:45:67:89:AB (numbers 0–9 and either uppercase or lowercase letters A–F). If you enter a MAC address, the existing entry is overwritten.
Failure Detection Method See *Configure the Failure Detection Method* on page 516, including *Table 134* on page 516.	

5. Click **Apply** to save your changes.

> ⚠️ **WARNING!**
>
> **Depending on the changes that you made, when you click Apply, the UTM9S restarts, or services such as HTTP and SMTP might restart.**

Additional WAN-Related Configuration Tasks

- If you have not done so already, configure the WAN interfaces of the UTM9S (see *Chapter 3, Manually Configuring Internet and WAN Settings*).

- If you want the ability to manage the UTM9S remotely, enable remote management (see *Configure Remote Management Access* on page 399). If you enable remote management, NETGEAR strongly recommend that you change your password (see *Change Passwords and Administrator and Guest Settings* on page 397).

- You can set up the traffic meter for the DSL interface, if you wish. See *Enable the WAN Traffic Meter* on page 419.

Wireless Module for the UTM9S

B

This appendix describes how to configure the wireless features of the UTM9SWLSN wireless module that is installed in a UTM9S. This appendix includes the following sections:

- *Overview of the Wireless Module*
- *Configure the Basic Radio Settings*
- *Wireless Data Security Options*
- *Wireless Security Profile*
- *Configure the Access Point*
- *Configure a Wireless Distribution System*
- *Configure Advanced Radio Settings*
- *Configure Advanced Profile and WMM QoS Priority Settings*
- *Test Basic Wireless Connectivity*

Before you set up the wireless features that are described in this appendix, connect the UTM9S and get the Internet connection working. The UTM9S should work with an Ethernet or DSL WAN connection, or with both. In planning your wireless network, consider the level of security required.

⚠️ **WARNING!**

If you are configuring the wireless settings from a wireless computer and you change the wireless module's SSID, channel, or wireless security settings, you will lose your wireless connection when you click Apply. You then need to change the wireless settings of your computer to match the wireless module's new settings.

Overview of the Wireless Module

The wireless module provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) through an antenna. Typically, an individual in-building wireless access point provides

a maximum connectivity area of about a 500-foot radius. The wireless module can support a small group of wireless users—typically 5 to 20 users.

The wireless module integrates a 2.4-GHz radio and a 5-GHz radio. One radio can be active to provide wireless connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. The 2.4-GHz radio supports 802.11b/g/n modes and Greenfield mode; the 5-GHz radio supports 802.11a/n modes and Greenfield mode.

The wireless module supports one access point and one security profile with Wi-Fi Multimedia (WMM) QoS priority, WMM Power Save, and Wireless Distribution System (WDS). Future releases might support additional virtual access points (VAPs) and security profiles. You can insert one wireless module only in the UTM9S.

Configuration Order

Configure the wireless features according to the order of the following sections:

1. *Configure the Basic Radio Settings*
2. *Configure and Enable Wireless Security Profiles*
3. *Configure the Access Point*
4. (Optional) *Configure a Wireless Distribution System*
5. (Optional) *Configure Advanced Radio Settings*
6. (Optional) *Configure Advanced Profile and WMM QoS Priority Settings*

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the UTM9S. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to connect to the wireless module. For complete performance specifications, see the data sheet on the ProSecure UTM series home page at *http://prosecure.netgear.com/products/prosecure-utm-series/index.php*.

For best results, place your UTM9S according to the following general guidelines:

- Near the center of the area in which your wireless devices will operate.
- In an elevated location such as a high shelf where the wirelessly connected devices have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves ovens, and 2.4-GHz cordless phones.

- Away from large metal surfaces or water.

- Placing the antennas in a vertical position provides the best side-to-side coverage. Placing the antennas in a horizontal position provides the best up-and-down coverage.

- If you are using multiple wireless access points, it is better if the wireless module and an adjacent wireless access point use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent wireless access points is five channels (for example, use channels 1 and 6, or 6 and 11, or 1 and 11).

- The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Configure the Basic Radio Settings

The default wireless mode is 802.11ng. You can change the wireless mode, country, and many other radio settings on the Radio Settings screen (described in this section) and on the Advanced Wireless screen (see *Configure Advanced Radio Settings* on page 549). The default radio settings should work well for most configurations.

> **Note:** To configure radio settings, you first need to disable the access point.

➢ **To configure the basic radio settings:**

1. Select **Network Config > Wireless Settings > Radio Settings**. The Radio Settings screen displays:
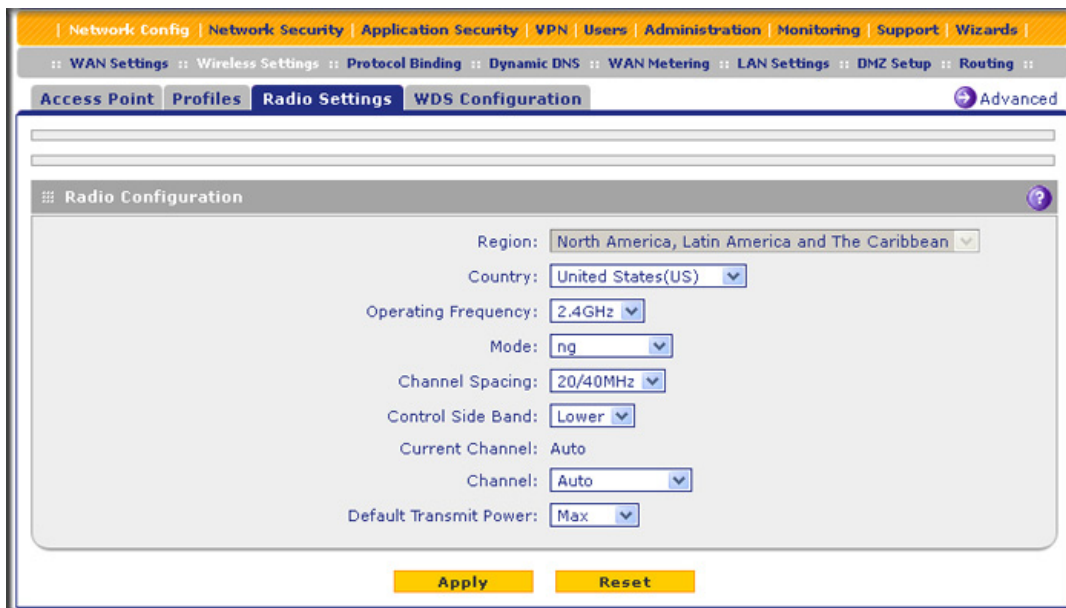
Figure 313.

2. Specify the settings as explained the following table:

Table 138. Radio Settings screen settings

Field	Descriptions	
Region	This is a preconfigured field that you cannot change.	
Country	Specify a country by making a selection from the drop-down list.	
Operating Frequency	Specify the radio's operating frequency by making a selection from the drop-down list: • **2.4GHz** • **5GHz**	
Mode	The wireless modes that you can select depend on the radio's operating frequency that you select.	
	2.4 GHz	Specify the wireless mode in the 2.4-GHz band by making a selection from the drop-down list: • **g and b**. In addition to 802.11b- and 802.11g-compliant devices, 802.11n-compliant devices can connect to the wireless access point because they are backward compatible. • **g only**. 802.11g- and 802.11n-compliant devices can connect to the wireless access point, but 802.11n-compliant devices function below their capacity in 802.11g mode. 802.11b-compliant devices cannot connect. • **ng**. This is the default setting. 802.11g- and 802.11n-compliant devices can connect to the wireless access point. 802.11b-compliant devices cannot connect. • **GreenField**. Only 802.11n-compliant devices can connect to the wireless access point, *and* 802.1b- and 802.11g-compliant devices cannot recognize the wireless access point, which might cause interference. Therefore, use Greenfield mode only when you are sure that there are no or very few 802.1b- and 802.11g-compliant devices in the wireless coverage area.
	5 GHz	Specify the wireless mode in the 5-GHz band by making a selection from the drop-down list: • **a only**. 802.11a- and 802.11n-compliant devices can connect to the wireless access point, but 802.11n-compliant devices function below their capacity in 802.11a mode. • **na**. This is the default setting. 802.11a- and 802.11n-compliant devices can connect to the wireless access point. • **GreenField**. Only 802.11n-compliant devices can connect to the wireless access point, *and* 802.1a -compliant devices cannot recognize the wireless access point, which might cause interference. Therefore, use Greenfield mode only when you are sure that there are no or very few 802.1a-compliant devices in the wireless coverage area.

Table 138. Radio Settings screen settings (continued)

Field	Descriptions
Channel Spacing **Note:** na, ng, and Greenfield modes only. This is a fixed field for a, b, and g modes.	For the na, ng, and Greenfield modes only, specify the channel spacing by making a selection from the drop-down list: • **20/40MHz**. Select this option to improve the performance. Some legacy devices (that is, devices that function only in a, b, or g mode) can operate only in 20 MHz. • **20MHz**. Select this option if your network includes legacy devices. This is the default setting. **Note:** The channel spacing is fixed at 20 MHz for the a, b, and g modes.
Control Side Band **Note:** na, ng, and Greenfield modes only	For the na, ng, and Greenfield modes, when you have selected a channel spacing of 20/40 MHz, you also need to select the control side band from the drop-down list. The extension channel that is specified by the control side band is four channels above or below the main channel. • **Lower**. The radio can use a lower channel as its extension channel. Use this setting when your main channel is in the 5–11 range for the 2.4-GHz operating frequency or the 5–13 range for the 5-GHz frequency. Lower is the default setting. • **Upper**. The radio can use a higher channel as its extension channel. Use this setting when your main channel is in the 1–7 range for the 2.4-GHz operating frequency or the 1–9 range for the 5-GHz frequency. **Note:** This field is not applicable when the channel spacing is set to 20 MHz.
Current Channel	This is a nonconfigurable field that shows the current channel if you have selected Auto from the Channel drop-down list.
Channel	Specify the channel you wish to use on your wireless LAN by making a selection from the drop-down list. The wireless channels and frequencies depend on the country and wireless mode. The default setting is Auto. **Note:** It should not be necessary to change the wireless channel unless you notice interference in the network (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see *Operating Frequency (Channel) Guidelines* following this table. **Note:** For more information about available channels and frequencies, see *Physical and Technical Specifications* on page 601.
Default Transmit Power	Specify the transmission power by making a selection from the drop-down list: • **Max** (this is the default setting.) • **75%** • **50%** • **25%** • **12.5%** • **Mi**n

⚠️ **WARNING!**

> **When you have changed the country settings, the wireless module (*not* the UTM9S) will reboot when you click Apply.**

3. Click **Apply** to save your settings.

Operating Frequency (Channel) Guidelines

You should not need to change the operating frequency (channel) unless you notice interference problems, or are setting up the UTM9S near another wireless access point. Observe the following guidelines:

- Wireless access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available in the 2.4-GHz operating frequency and 13 channels in the 5-GHz operating frequency.

- If you are using multiple wireless access points, it is better if adjacent wireless access points use different channels to reduce interference. The recommended channel spacing between adjacent wireless access points is 5 channels (for example, in 2.4-GHz operating frequency, use channels 1 and 6, or 6 and 11).

- In infrastructure mode, wireless devices normally scan all channels, looking for a wireless access point. If more than one wireless access point can be used, the one with the strongest signal is used. This can happen only when the wireless access points use the same SSID. The wireless module functions in infrastructure mode by default.

Wireless Data Security Options

Indoors, computers can connect over 802.11n wireless networks at a maximum range of 300 feet. Typically, a UTM9S inside a building works best with wireless devices within a 100-foot radius. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless module provides highly effective wireless security features that are covered in detail in this appendix. Deploy the security features appropriate to your needs.

Wireless Data Security Options

Range: Up to 500 feet RADIUS

1. No security: Easy but no security
2. MAC Access List: No data security
3. WEP: Secure but vulnerable
4. WPA or WPA-PSK: Strong security
5. WPA2 or WPA2-PSK: Very strong security

UTM9S
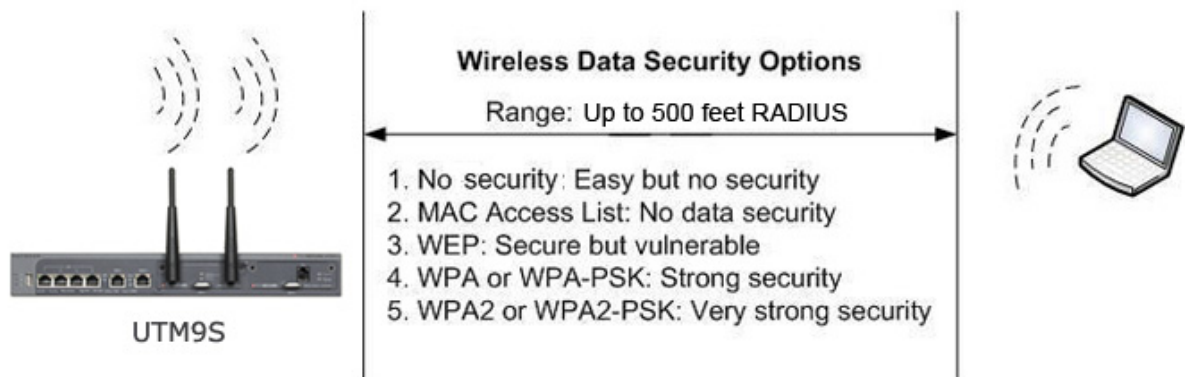
Figure 314.

There are several ways you can enhance the security of your wireless network:

• **Restrict access based by MAC address**. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the wireless module. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For information about how to restrict access by MAC address, see *Restrict Wireless Access by MAC Address* on page 545.

• **Turn off the broadcast of the wireless network name (SSID)**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network discovery feature of some products, such as Windows XP, but the data is still exposed. For information about how to turn of broadcast of the SSID, see *Configure and Enable Wireless Security Profiles* on page 538.

• **WEP**. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP shared key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.

> **Note:** On the UTM9S, WEP is not supported when the radio functions in 802.11n wireless mode (802.11n, 802.11ng, 802,11na, or Greenfield).

For information about how to configure WEP, see *Configure and Enable Wireless Security Profiles* on page 538.

• **WPA**. Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) or a combination of TKIP and Advanced Encryption Standard (AES) encryption. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. The wireless module supports WPA with a pre-shared key (PSK), RADIUS, or a combination of PSK and RADIUS.

For more information about how to configure WPA, see *Configure and Enable Wireless Security Profiles* on page 538.

- **WPA2**. Wi-Fi Protected Access version 2 (WPA2) data encryption provides strong data security with AES encryption. WPA2 provides the most reliable security. Use WPA2 only if all clients in your network support WPA2. The wireless module supports WPA2 with PSK, RADIUS, or a combination of PSK and RADIUS.

  For more information about how to configure WPA2, see *Configure and Enable Wireless Security Profiles* on page 538.

- **WPA+WPA2 mixed mode**. This mode supports data encryption with a combination of TKIP and AES for both WPA and WPA2 clients. The very strong authentication along with dynamic per frame rekeying of WPA2 make it virtually impossible to compromise. The wireless module supports WPA+WPA2 with PSK, RADIUS, or a combination of PSK and RADIUS.

  For more information about how to configure WPA+WPA2 mixed mode, see *Configure and Enable Wireless Security Profiles* on page 538.

Note: TKIP provides only legacy (slower) rates of operation. NETGEAR recommends WPA2 with AES to make use of 802.11n rates and speed.

Wireless Security Profile

The security profile lets you configure the security settings for the SSID on the wireless module. The wireless module supports one security profile (BSSID) that you can configure from the Profiles screen (see *Configure and Enable Wireless Security Profiles* on page 538).

To configure the security profile, specify a name for the SSID, type of security with authentication and data encryption, and whether or not the SSID is broadcast.

- **Network authentication**
  The wireless module is set by default as an open system with no authentication. When you configure network authentication, bear in mind that older wireless adapters might not support WPA or WPA2. Windows XP, Windows 2000 with Service Pack 3, and Windows Vista do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

  For information about the types of network authentication that the wireless module supports, see *Configure and Enable Wireless Security Profiles* on page 538.

- **Data encryption**
  Select the data encryption that you want to use. The available options depend on the network authentication setting described earlier (otherwise, the default is None). The data

---

encryption settings are explained in *Configure and Enable Wireless Security Profiles* on page 538.

Here are some concepts and guidelines regarding the SSID:

- A basic service set (BSS) is a group of wireless devices and a single wireless access point, all using the same security profile or service set identifier (BSSID). The actual identifier in the BSSID is the MAC address of the wireless radio. (A wireless radio can have multiple MAC addresses, one for each security profile.)

- An extended service set (ESS) is a group of wireless devices, all using the same identifier (ESSID).

- Different devices within an ESS can use different channels. To reduce interference, adjacent devices should use different channels.

- Roaming is the ability of wireless devices to connect wirelessly when they physically move from one BSS to another one within the same ESS. The wireless device automatically changes to the wireless access point with the least interference or best performance.

Before You Change the SSID, WEP, and WPA Settings

For a new wireless network, print or copy the following form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the Country/Region correctly as the first step.

_____

Store this information in a safe place:

- **SSID**
  The service set identifier (SSID) identifies the wireless local area network. You can customize it by using up to 32 alphanumeric characters. Write your SSID on the line.

  SSID: _____

  The SSID in the wireless access point is the SSID you configure on the wireless adapter card. All wireless nodes in the same network need to be configured with the same SSID.

- **WEP key size, key format, authentication type, and passphrase**
  Choose the key size by circling one: 64, 128, or 256 bits.
  Choose the key format by circling one: ASCII or HEX.
  Choose the authentication type by circling one: Open or Shared.

  Passphrase: _____

  Note: If you select shared key, the other devices in the network will not connect unless they are set to shared key and have the same keys in the same positions as those in the security profile on the wireless module.

- **WPA-PSK (Pre-Shared Key) and WPA2-PSK**
  Record the WPA-PSK passphrase:

  WPA-PSK passphrase: _____

Record the WPA2-PSK passphrase:

WPA2-PSK passphrase: _____

- **WPA RADIUS settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary _____ Secondary _____

  Port: _____

  Shared secret: _____

- **WPA2 RADIUS settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary _____ Secondary _____

  Port: _____

  Shared secret: _____

_____

Configure and Enable Wireless Security Profiles

➢ **To configure the wireless security profile:**

1. Select **Network Config > Wireless Settings > Profiles**. The Profiles screen displays:
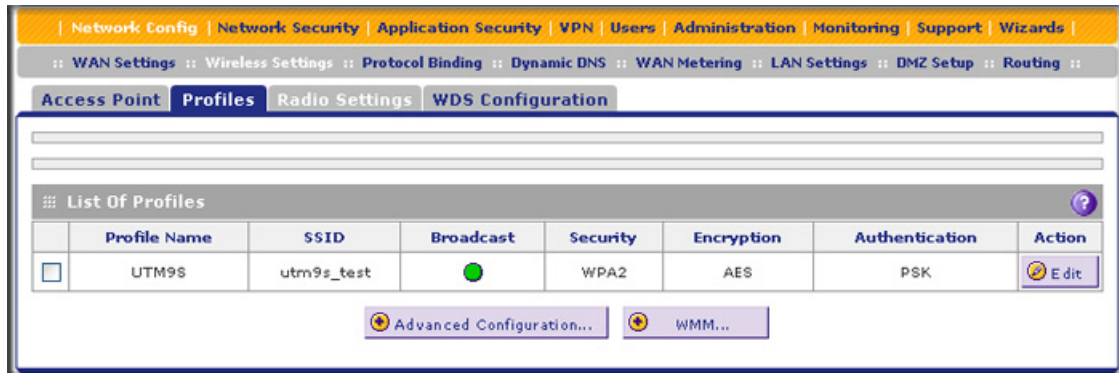
Figure 315.

The following table explains the fields of the Profile screen:

Table 139. Profiles screen settings

Field	Description
Profile Name	The unique name of the security profile that makes it easy to recognize the profile. The default name is UTM9S. You cannot change this name.
SSID	The wireless network name (SSID) for the security profile.

Table 139. Profiles screen settings (continued)

Field	Description
Broadcast	Indicates whether or not the SSID is broadcast. A green circle indicates that the SSID is broadcast; a gray circle indicates that it is not.
Security	The configured security method for the security profile.
Encryption	The configured encryption method for the security profile.
Authentication	The configured authentication method for the security profile.

2. Click the **Edit** table button in the Action column. The Edit Profile screen displays:

Figure 316.

3. Specify the settings as explained in the following table:

Table 140. Edit Profile screen settings

Field	Description
Profile Configuration	
Profile Name	The name for the wireless security profile is UTM9S. You cannot change this name.
SSID	The wireless network name (SSID) for the wireless security profile. There is no default SSID name.
Broadcast SSID	Select the check box to enable the wireless access point to broadcast its SSID, allowing wireless clients that have a null (blank) SSID to adopt the wireless access point's SSID. To prevent the SSID from being broadcast, clear the check box.

Security	**Note:** Before you configure security, you might want to read *Wireless Data Security Options* on page 534.
	
	Specify the wireless security by making a selection from the drop-down list:
	• **OPEN**. This is the default setting. An open system has no authentication and no encryption, and therefore no security configuration. However, you *can* use an open system with encryption. To do so, select **WEP** from the Security drop-down list. In the WEP Index and Keys section of the screen, take the following steps:
	    - Select **Open System** authentication.
	    - Select the encryption.
	    - Enter a passphrase and generate a key, or enter a key manually.
	• **WEP**. To configure WEP, take the following steps in the WEP Index and Keys section of the screen:
	    - Select **Shared Key** authentication.
	    - Select the encryption.
	    - Enter a passphrase and generate a key, or enter a key manually.
	• **WPA**. To configure WPA, select the encryption and authentication. The remaining configuration depends on the selected authentication:
	    - For WPA-PSK, select a password.
	    - For WPA with RADIUS, configure the RADIUS server settings.
	    - For WPA with PSK+RADIUS, select a password and configure the RADIUS server settings.
	• **WPA2**. To configure WPA2, select the encryption and authentication. The remaining configuration depends on the selected authentication:
	    - For WPA2-PSK, select a password.
	    - For WPA2 with RADIUS, configure the RADIUS server settings. As an option, you can enable RADIUS preauthentication.
	    - For WPA2 with PSK+RADIUS, select a password and configure the RADIUS server settings. As an option, you can enable RADIUS preauthentication.

Table 140. Edit Profile screen settings (continued)

Field	Description

Security (continued)	• **WPA+WPA2**. To configure WPA, select the encryption and authentication. The remaining configuration depends on the selected authentication:
	   - For WPA+WPA2 with PSK, select a password.
	   - For WPA+WPA2 with RADIUS, configure the RADIUS server settings.
	   - For WPA+WPA2 with PSK+RADIUS, select a password and configure the RADIUS server settings.

Encryption
 	
Note: WPA, WPA2, and WPA+WPA2 only.
	The encryption that you can select depends on the type of WPA security that you have selected:
	• **WPA**. You can select the following types of encryption from the drop-down list:
	   - TKIP
	   - TKIP+AES
	• **WPA2**. The encryption is AES.
	• **WPA+WPA2**. The encryption is TKIP+AES.

Authentication **Note:** WPA, WPA2, and WPA+WPA2 only.	For WPA, WPA2, and WPA+WPA2 only, specify the authentication by making a selection from the drop-down list: • **PSK** • **RADIUS** • **PSK+RADIUS**
WPA Password **Note:** WPA, WPA2, and WPA+WPA2 only.	For WPA, WPA2, and WPA+WPA2 only, if you have selected PSK or PSK+RADIUS authentication, enter a pre-shared key or password. The password length needs to be between 8 and 63 characters (inclusive).
Enable Pre-Authentication **Note:** WPA2 only.	For WPA2 only, if you have selected RADIUS authentication, configure preauthentication by selecting the check box. Preauthentication allows a client to roam from one access point to another access point without having to be reauthenticated.
Radius Server Settings **Note:** These settings apply to WPA, WPA2, and WPA+WPA2 only if you have selected RADIUS or PSK+RADIUS authentication.	
Server Name / IP Address	The IP address or FQDN of the RADIUS server.
Radius Port	The port number on the UTM9S that is used to connect to the RADIUS server. The default port number is 1812.
Shared Key	The shared key that is required for the UTM9S to connect to the RADIUS server.
Key Life Time	This period in seconds after which the encryption key is changed. The default period is 3600 seconds. Short periods are more secure than long periods but can slow down the authentication time.

Table 140. Edit Profile screen settings (continued)

Field	Description
WEP Index and Keys	
Authentication	Specify the authentication by making a selection from the drop-down list: • **Open System**. Select this option to use WEP encryption without authentication. • **Shared Key**. Select this option to use WEP authentication and encryption with a shared key (passphrase).
Encryption	Select the encryption key size by making a selection from the drop-down list: • **64-bit WEP**. Standard WEP encryption, using 40/64-bit encryption. • **128-bit WEP**. Standard WEP encryption, using 104/128-bit encryption. • **256-bit WEP**. Standard WEP encryption, using 232/256-bit encryption.
Passphrase	Enter a passphrase. The passphrase can have a maximum of 64 characters. The secret passphrase allows you to automatically generate the keys by clicking **Generate**.
Encryption Key (Key1–Key4)	Specify the active key by selecting one of the four radio buttons. Only one key can be the active key. Either enter a key manually or generate the key automatically by clicking **Generate**. The length of the key depends on the selected encryption: • **64-bit WEP**. A key length of 5 ASCII or 10 hexadecimal characters. • **128-bit WEP**. A key length of 13 ASCII or 26 hexadecimal characters. • **256-bit WEP**. A key length of 29 ASCII or 58 hexadecimal characters. **Note:** Wireless stations need to use the key to access the wireless access point.

4. Click **Apply** to save your settings. The profile is updated in the List of Profiles table.

WARNING!

If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the wireless module from a wired computer to make further changes.

Configure the Access Point

The wireless access point provides the following features:

• Capability to turn off the wireless access point during scheduled vacations and office shutdowns, on evenings, or on weekends. This a green feature that allows you to save energy.
• MAC address access control list that lets you add another level of security.
• Capability to monitor the wireless access point and its connected clients.

> **To configure the wireless access point:**

1. Select **Network Config > Wireless Settings > Access Point**. The Access Point screen displays. (The following figure shows some examples.)
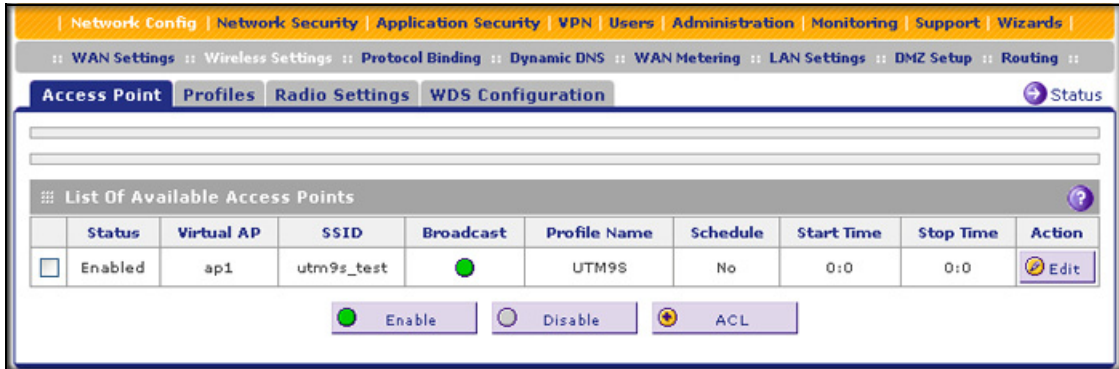
Figure 317.

The following table explains the fields of the Access Point screen:

Table 141. Access Point screen settings

Item	Description
Status	The status of the access point (Enabled or Disabled).
Virtual AP	The name for the virtual access point (VAP) is ap1. You cannot change this name.
SSID	The wireless network name (SSID) for the security profile that is allocated to the access point.
Broadcast	Indicates whether or not the SSID is broadcast. A green circle indicates that the SSID is broadcast; a gray circle indicates that it is not.
Profile Name	The security profile that is allocated to the access point.
VLAN	The VLAN to which the access point is allocated.
Active Time	Indicates whether or not the timer for the access point is activated (No or Yes).
Start Time	The start time for the timer.
Stop Time	The stop time for the timer.

2. Click the **Edit** table button in the Action column. The Edit Access Point screen displays:
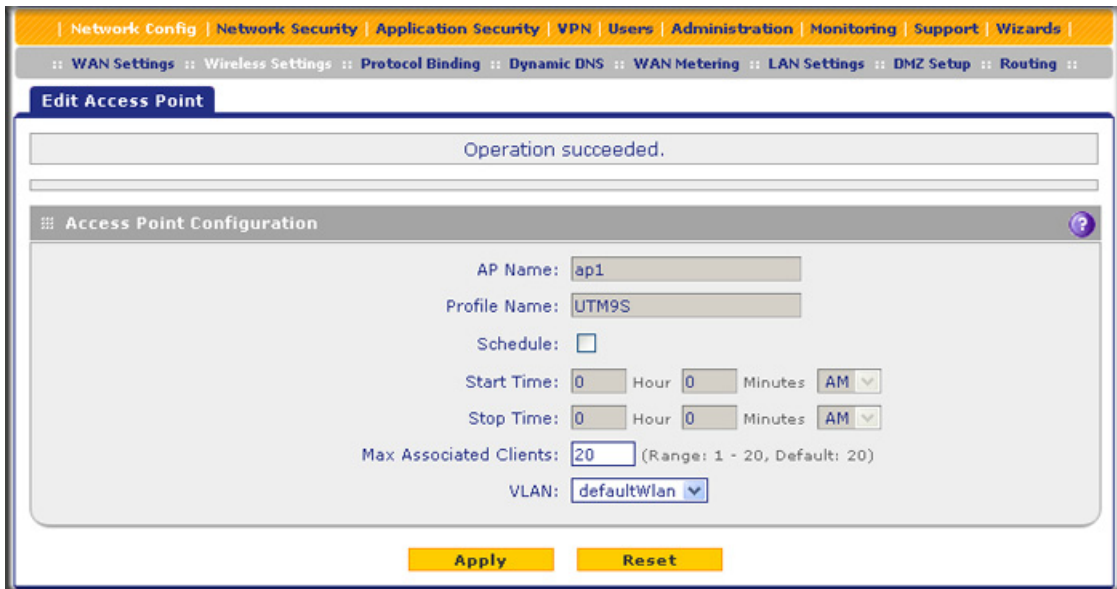
Figure 318.

3. Specify the settings as explained in the following table:

Table 142. Edit Access Point screen settings

Settings	Description
AP Name	The name for the access point is ap1. You cannot change this name.
Profile Name	The name for the profile is UTM9S. You cannot change this name.
Schedule	To enable the timer, select the **Schedule** check box. When the timer is enabled, the access point is turned off from the start time until the stop time. To disable the timer, clear the check box.
Start Time	Specify the start hour in the Hours field and the start minute in the Minutes field, and then select **AM** or **PM** from the drop-down list.
Stop Time	Specify the stop hour in the Hours field and the stop minute in the Minutes field, and then select **AM** or **PM** from the drop-down list.
Max Associated Clients	Enter the maximum number (1 to 20) of clients that can be associated with the access point.
VLAN	From the drop-down list, select the VLAN to which the access point should be allocated. The default VLAN is defaultWLAN. For information about how to configure VLANs, see *Configure a VLAN Profile* on page 98.

4. Click **Apply** to save your settings. The access point is updated in the List Of Available Access Points table.

➢ **To enable or disable the access point:**

1. On the Access Point screen (see *Figure 317* on page 543), select the check box to the left of the access point.

2. Click one of the following table buttons:
   - **Enable**. Enables the access point and allows wireless clients to make a connection.
   - **Disable**. Disables the access point and prevents wireless clients from making a connection.

Restrict Wireless Access by MAC Address

For increased security, you can restrict access to an SSID by allowing access to only specific computers or wireless stations based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot connect to the wireless access point. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

> **Note:** For wireless adapters, you can usually find the MAC address printed on the wireless adapter.

➤ **To allow or restrict access based on MAC addresses:**

1. Select **Network Config > Wireless Settings > Access Point**. The Access Point screen displays (see *Figure 317* on page 543).
2. Select the check box to the left of the access point.
3. Under the List Of Available Access Points table, click the **ACL** button. The MAC Address Filtering screen displays. (The following figure shows some examples.)
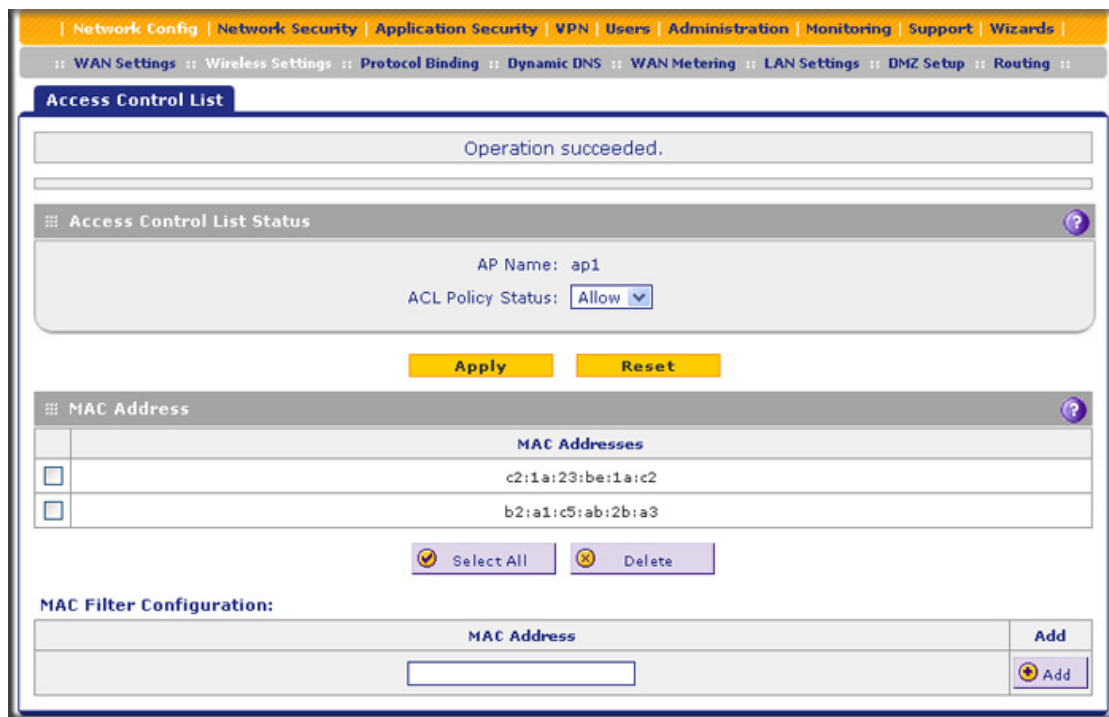
Figure 319.

4. Enter a MAC address in the MAC Address field.

5. Click **Apply** to add the MAC address to the MAC Address table on the MAC Address Filtering screen.

6. Repeat *step 4* and *step 5* for any other MAC addresses that you want to add to the MAC Address table.

7. From the ACL Policy Status drop-down list, select if access control is enabled, and if so, how the MAC addresses in the MAC Address table are treated:

   • **Open**. Access control is disabled. All MAC addresses, including the ones in the MAC Address table, are allowed access.

   • **Allow**. Only the MAC addresses in the MAC Address table are allowed access. All other MAC addresses are denied access.

   • **Deny**. The MAC addresses in the MAC Address table are denied access. All other MAC addresses are allowed access.

8. Click **Apply** to save your settings.

⚠ **WARNING!**

When configuring the wireless module in the UTM9S from a wireless computer whose MAC address is not in the access control list and when the ACL policy status is set to deny access, you will lose your wireless connection when you click Apply. You then need to access the UTM9S from a wired computer or from a wireless computer that is on the access control list to make any further changes.

➢ **To remove one or more MAC addresses from the table:**

1. In the MAC Address table, select the check box to the left of each MAC address that you want to delete, or click the **Select All** table button to select all MAC addresses.

2. Click the **Delete** table button.

View the Access Point Status and Connected Clients

➢ **To view the status of the access point and the clients that are connected to it:**

1. Select **Network Config > Wireless Settings > Access Point**. The Access Point screen displays (see *Figure 317* on page 543).

2. Click the **Status** option arrow in the upper right of the Access Point screen. The Access Point Status screen displays:
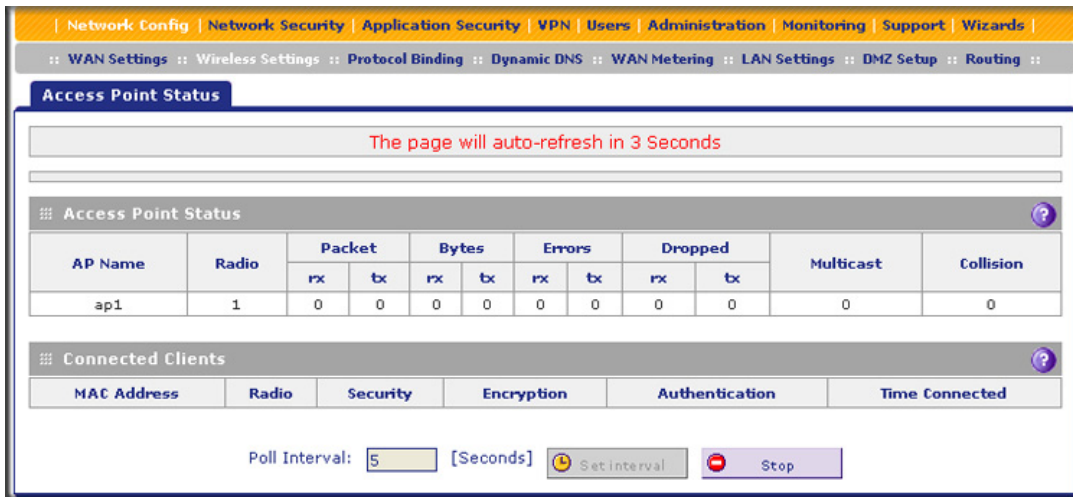
Figure 320.

The following table explains the fields of the Access Point Status screen.

To change the poll interval period, enter a new value in the Poll Interval field, and then click **Set interval**. To stop polling, click **Stop**.

Table 143. Access Point Status screen fields

Item	Description
AP Statistics	
AP Name	The name for the virtual access point (VAP) is ap1.
Packets	The number of received (Rx) and transmitted (Tx) packets on the access point in bytes.
Bytes	The number of received (Rx) and transmitted (Tx) bytes on the access point.
Errors	The number of received (Rx) and transmitted (Tx) errors on the access point.
Dropped	The number of received (Rx) and transmitted (Tx) dropped packets on the access point.
Multicast	The number of received (Rx) and transmitted (Tx) multicast packets on the access point.
Collisions	The number of signal collisions that have occurred on the access point. A collision occurs when the access point attempts to send data at the same time as a wireless station that is connected to the access point.
Connected Clients	
MAC Address	The MAC address of the client.
Radio	The radio to which the client is connected (2.4GHz or 5GHz).
Security	The type of security that the client is using (Open, WEP, WPA, WPA2, or WPA+WPA2).
Encryption	The type of encryption that the client is using (None, TKIP, AES, or TKIP+AES).

Table 143. Access Point Status screen fields (continued)

Item	Description
Authentication	The type of encryption that the client is using (Open, PSK, RADIUS, or PSK+RADIUS).
Time Connected	The period in minutes since the connection was established between the access point and the client..

Configure a Wireless Distribution System

The UTM9S can function as a station (peer) in a Wireless Distribution System (WDS). WDS enables expansion of a wireless network through two or more access points that are interconnected and that use the same radio channel and security mode.

WDS is supported in any of the security modes (see *Wireless Security Profile* on page 536). If you configure the access point for WEP, then WDS works in WEP mode; if you configure the access point for WPA2, then WDS works in WPA2 mode, and so on. If you configure mixed encryption (TKIP+AES, which is supported in WPA and WPA+WPA2 security modes), WDS uses AES because it is the stronger encryption method.

To configure WDS, you need to know the MAC addresses of the wireless peers, and you need to use a common WPA password or WEP key on all peers. (You enter the WPA password or WEP key in the WPA Password field on the WDS Configuration screen.) You can configure up to a maximum of four WDS peers.

➢ **To enable and configure WDS:**

1. Select **Network Config > Wireless Settings > WDS Configuration**. The WDS Configuration screen displays:

Figure 321.

2. Select the **Enable WDS** check box.

3. In the WPA Password field, enter a password between 8 and 63 characters.

4. Click **Apply** to save your settings.

5. Enter a MAC address of a peer in the MAC Address field.

6. Click **Apply** to add the MAC address to the WDS Peers table.

7. Repeat *step 5* and *step 6* for any other MAC addresses that you want to add to the MAC Address table.

➢ **To configure WDS on a peer:**

1. Configure the same wireless security that you have configured on the UTM9S.

2. Enter the MAC address of the UTM9S's access point, which is displayed on the WDS Configuration screen of the UTM9S.

3. Enter the same WPA password or WEP key that you have entered on the WDS Configuration screen of the UTM9S.

> **Note:** Make sure that you use the same wireless security configuration on all WDS peers.

➢ **To remove one or more MAC addresses from the WDS Peers table:**

1. In the WDS Peers table, select the check box to the left of each MAC address that you want to delete, or click the **Select All** table button to select all MAC addresses.

2. Click the **Delete** table button.

Configure Advanced Radio Settings

➢ **To configure advanced radio settings:**

1. Select **Network Config > Wireless Settings > Radio Settings**. The Radio Settings screen displays (see *Figure 313* on page 531).

2. Click the **Advanced** option arrow in the upper right of the Radio Settings screen. The Advanced Wireless screen displays:
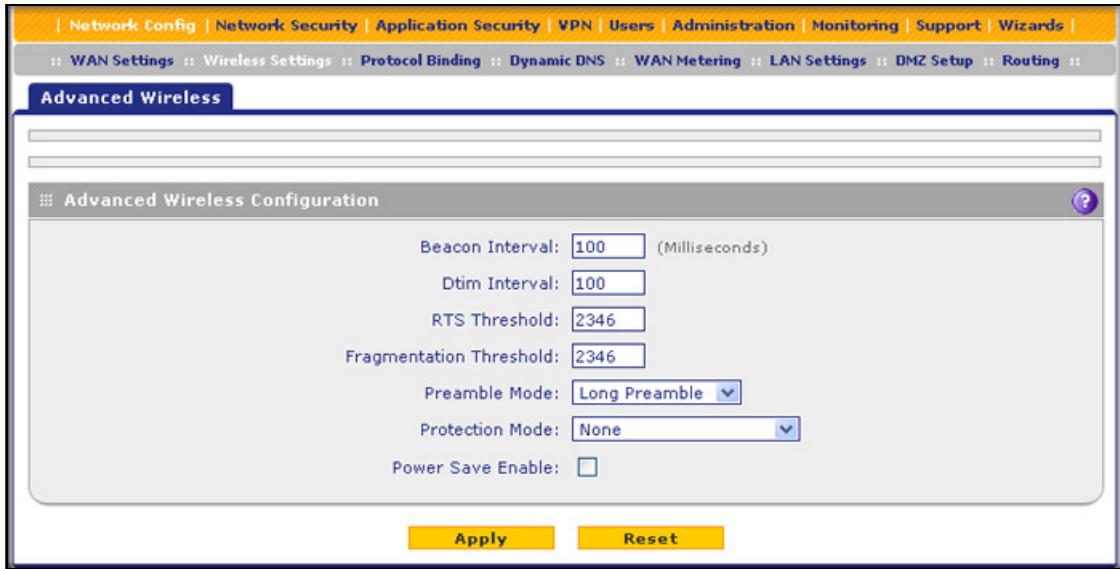
Figure 322.

3. Specify the settings as explained in the following table:

Table 144. Advanced Wireless screen settings

Setting	Description
Beacon Interval	Enter an interval between 40 ms and 3500 ms for each beacon transmission, which allows the wireless module to synchronize the wireless network. The default setting is 100 ms.
DTIM Interval	Enter the Delivery Traffic Indication Message (DTIM) interval, also referred to as the data beacon rate, which indicates the period for the beacon DTIM in multiples of beacon intervals. This value needs to be between 1 and 255. The default setting is 2.
RTS Threshold	Enter the Request to Send (RTS) threshold. The default setting is 2346 bytes. If the packet size is equal to or less than the RTS threshold, the wireless module uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism, and the data frame is transmitted immediately after the silence period. If the packet size is larger than the RTS threshold, the wireless module uses the CSMA with Collision Avoidance (CSMA/CA) mechanism. In this situation, the transmitting station sends an RTS packet to the receiving station and waits for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data. This method improves the performance but reduces the throughput.
Fragmentation Threshold	Enter the maximum packet size that is used for the fragmentation of data packets. Packets that are larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation threshold needs to be an even number. The default setting is 2346 bytes.

Table 144. Advanced Wireless screen settings (continued)

Setting	Description
Preamble Mode	Specify the preamble mode by making a selection from the drop-down list: • **Long**. A long transmit preamble might provide a more reliable connection or a slightly longer range. This is the default mode. • **Short**. A short transmit preamble gives better performance.
Protection Mode	Specify the CTS-to-self protection mode (CTS stands for Clear to Send) by making a selection from the drop-down list: • **None**. CTS-to-self protection mode is disabled. This is the default mode. • **CTS-To-Self-Protection**. CTS-to-self protection mode is enabled. This mode increases the performance but reduces the throughput slightly.
Power Save Enable	To enable the Wi-Fi Multimedia (WMM) Power Save feature, select the **Power Save Enable** check box. This feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission. Clear the check box to disable the feature, which is the default setting.

4. Click **Apply** to save your settings.

Configure Advanced Profile and WMM QoS Priority Settings

Advanced Profile Settings

The advanced profile settings let you configure advanced WPA and WPA2 settings and related RADIUS settings.

➢ **To configure advanced profile settings:**

1. On the Profiles screen (see *Figure 315* on page 538), select the check box to the left of the profile.

2. Under the List Of Profiles table, click the **Advanced Configuration** button. The Advanced Configuration screen displays:
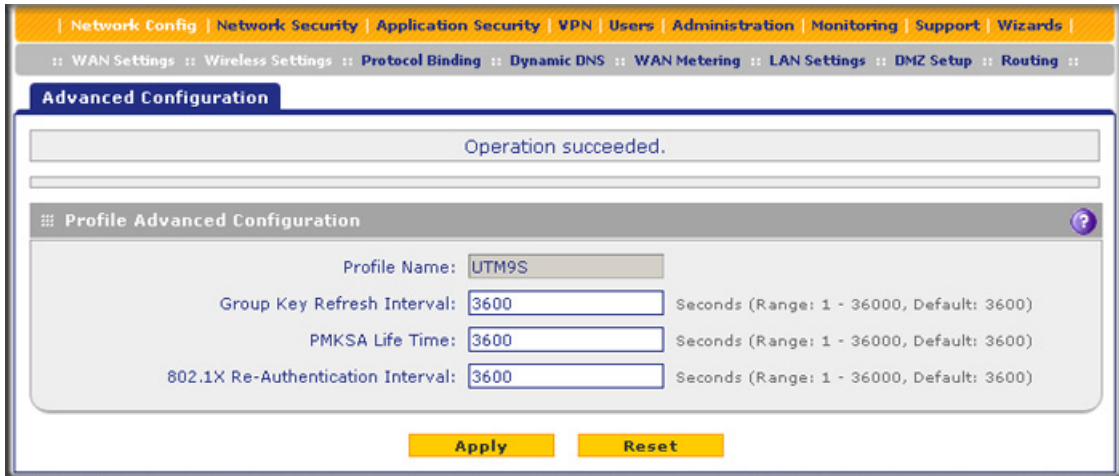
Figure 323.

3. Specify the advanced profile settings as explained the following table:

Table 145. Advanced profile settings

Field	Descriptions
Profile Name	The name for the wireless security profile is UTM9S. You cannot change this name.
Group Key Refresh Interval	**Note:** This field applies only if you have configured the profile for WPA or WPA2 security. Specify the time-out interval in seconds (1–36000) after which group keys are generated. The default interval is 3600 seconds.
PMKSA Life Time	**Note:** This field applies only if you have configured the profile for WPA2 security and RADIUS or PSK+RADIUS authentication. Pairwise Master Key Security Association (PMKSA) caching is used to store the master keys that are derived from a successful RADIUS authentication. When a client has been authenticated by the RADIUS server and then attempts to reconnect within the specified PMKSA lifetime interval, the RADIUS authentication is skipped. This feature prevents a long RADIUS authentication process when the client attempts to reconnect. Specify the lifetime in seconds (1–36000) after which the master keys time out. The default interval is 3600 seconds.
802.1X Re-Authentication Interval	**Note:** This field applies only if you have configured the profile for WPA or WPA2 security and RADIUS or PSK+RADIUS authentication. Specify the time-out interval in seconds (1–36000) after which the wireless clients need to reauthenticate with the RADIUS server. The default interval is 3600 seconds.

4. Click **Apply** to save your settings.

WMM QoS Priority Settings

Wi-Fi Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients also need to support WMM.

By enabling WMM, you allow Quality of Service (QoS) control for upstream traffic flowing from a wireless client to the UTM9S and for downstream traffic flowing from the UTM9S to a wireless client.

WMM defines the following four queues in decreasing order of priority:

- **Voice (Queue 4)**. The highest priority queue with minimum delay, which makes it ideal for applications like VoIP and streaming media.

- **Video (Queue 3)**. The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue.

- **Best Effort (Queue 2)**. The medium priority queue with medium delay is given to this queue. Most standard IP application use this queue.

- **Background (Queue 1)**. Low priority queue with high throughput. Applications, such as FTP, that are not time-sensitive but require high throughput can use this queue.

Differentiated Services (DiffServ) QoS packet matching lets you map each Differentiated Services Code Point (DSCP) value (0 to 63) to one queue (1, 2, 3, or 4). You can map different DSCP values to the same queue. Based on the DSCP value in a packet's IP header, the packet is placed in the queue to which you mapped the DSCP value.

➢ **To enable and configure WMM QoS priority settings:**

1. On the Profiles screen (see *Figure 315* on page 538), select the check box to the left of the profile.
2. Under the List Of Profiles table, click the **WMM** button. The WMM screen displays:
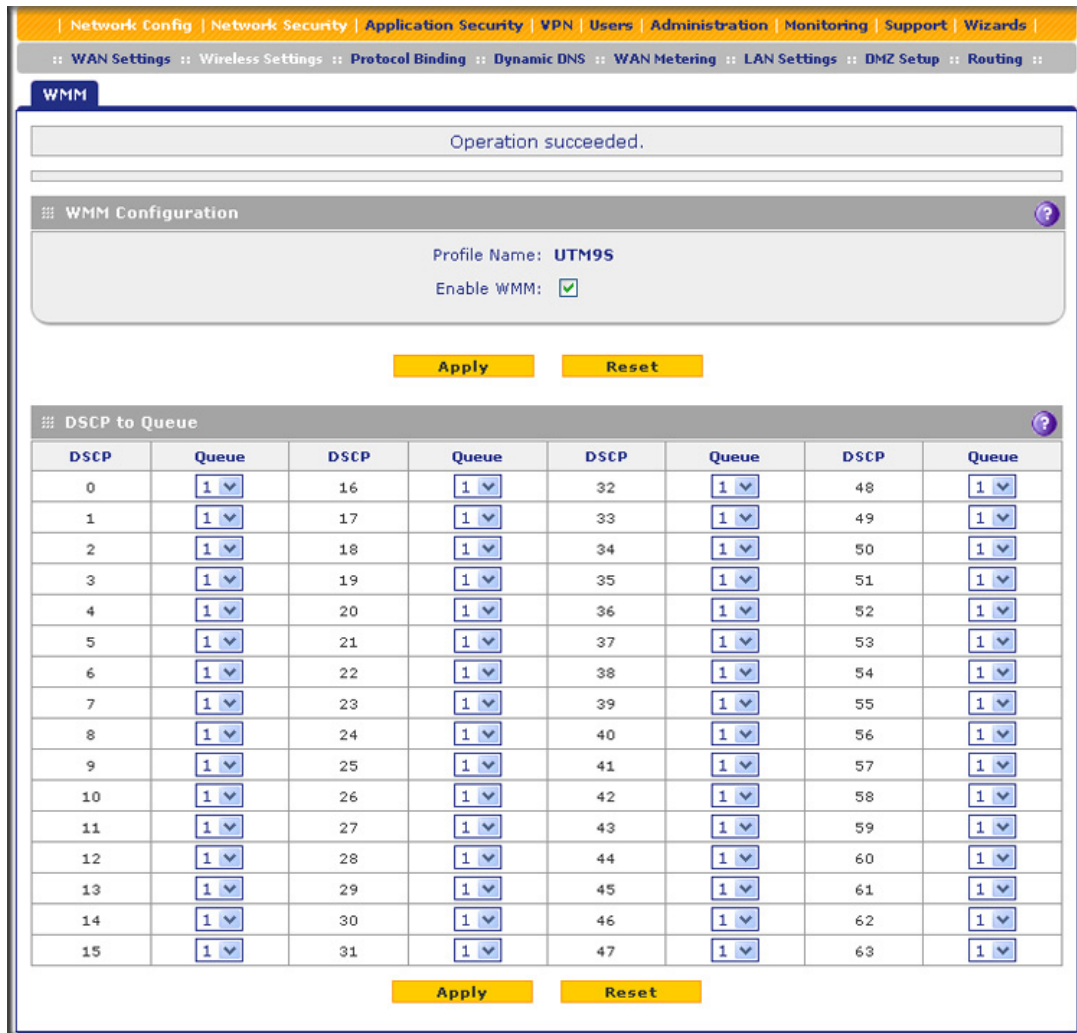
Figure 324.

3. Select the **Enable WMM** check box.

4. Click **Apply** to save your settings.

5. In the DSCP to Queue table, from the drop-down lists, select a WMM queue for each DSCP value that you want to use in a QoS profile.

6. Click **Apply** to save your settings.

Test Basic Wireless Connectivity

After you have configured the wireless module as explained in the previous sections, test your wireless clients for connectivity before you place the UTM9S at its permanent position.

> ➢ **To test for wireless connectivity:**

1. Configure the 802.11b/g/n or 802.11a/n wireless clients so that they all have the same SSID that you have configured on the wireless access point. Make sure that the wireless mode on the wireless access point supports the wireless capacity of the wireless clients. (For example, 802.11b-compliant devices cannot connect to the wireless access point if the wireless mode is set to ng.)

2. Verify that your wireless clients have a link to the wireless access point. If you have enabled the DHCP server on the UTM9S (see *Configure a VLAN Profile* on page 98) and have assigned a VLAN to the wireless access point, verify that your wireless clients are able to obtain an IP address through DHCP from the UTM9S.

3. Verify network connectivity by using a browser such as Internet Explorer 6.0 or later or Mozilla Firefox 1.5 or later to browse the Internet, or check for file and printer access on your network.

If you have trouble connecting to the wireless module, try to connect without security by selecting **OPEN** from the Security drop-down list on the Edit Profiles screen. If that does not help you to solve the connection problem, see *Chapter 12, Troubleshooting and Using Online Support*.

Network Planning for Dual WAN Ports (Multiple WAN Port Models Only)

C

This appendix describes the factors to consider when planning a network using a firewall that has dual WAN ports. This appendix does not apply to single WAN port models.

This appendix contains the following sections:

- *What to Consider Before You Begin*
- *Overview of the Planning Process*
- *Inbound Traffic*
- *Virtual Private Networks*

What to Consider Before You Begin

The UTM is a powerful and versatile solution for your networking needs. The information in this section can help you to understand the configuration choices that are available to you, and can make the configuration process easier.

Consider the following information before you begin:

1. Plan your network.
   a. Determine whether you will use one or both WAN ports. For one WAN port, you might need a fully qualified domain name either for convenience or to remotely access a dynamic WAN IP address.
   b. If you intend to use both WAN ports, determine whether you will use them in auto-rollover mode for increased system reliability or load balancing mode for maximum bandwidth efficiency. See the topics in this appendix for more information. Your decision has the following implications:
      - Fully qualified domain name (FQDN)
        - For auto-rollover mode, you will need an FQDN to implement features such as exposed hosts and virtual private networks.
        - For load balancing mode, you might still need an FQDN either for convenience or to remotely access a dynamic WAN IP address.
      - Protocol binding
        - For auto-rollover mode, protocol binding does not apply.

- For load balancing mode, decide which protocols should be bound to a specific WAN port.
- You can also add your own service protocols to the list.

2. Set up your accounts.

   a. Obtain active Internet services such as cable or DSL broadband accounts, and locate the Internet service provider (ISP) configuration information.

   - In this manual, the WAN side of the network is presumed to be provisioned as shown in the following figure, with two ISPs connected to the UTM through separate physical facilities.

   - Each WAN port needs to be configured separately, whether you are using a separate ISP for each WAN port or you are using the same ISP to route the traffic of both WAN ports.

   - If your ISP charges by the volume of data traffic each month, consider enabling the UTM's traffic meter to monitor or limit your traffic.
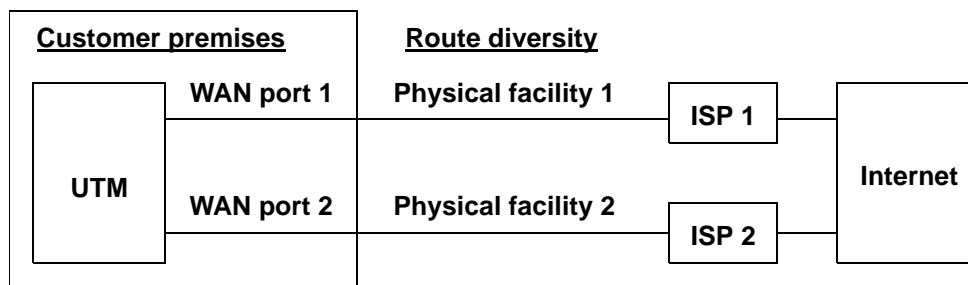
Figure 325.

   b. Contact a Dynamic DNS service and register FQDNs for one or both WAN ports.

3. Plan your network management approach.

   - The UTM is capable of being managed remotely, but this feature needs to be enabled locally after each factory default reset.

     NETGEAR strongly advises you to change the default management password to a strong password before enabling remote management.

   - You can choose a variety of WAN options if the factory default settings are not suitable for your installation. These options include enabling a WAN port to respond to a ping, and setting MTU size, port speed, and upload bandwidth.

4. Prepare to physically connect the firewall to your cable or DSL modems and a computer. Instructions for connecting the UTM are in the *ProSecure Unified Threat Management UTM Installation Guide*.

Cabling and Computer Hardware Requirements

For you to use the UTM in your network, each computer needs to have an Ethernet network interface card (NIC) installed and needs to be equipped with an Ethernet cable. If the

computer will connect to your network at 100 Mbps or higher speeds, you need to use a Category 5 (Cat 5) cable.

Computer Network Configuration Requirements

The UTM integrates a web management interface. To access the configuration screens on the UTM, you need to use a Java-enabled web browser that supports HTTP uploads such as Microsoft Internet Explorer 6 or later, Mozilla Firefox 3 or later, or Apple Safari 3 or later with JavaScript and cookies, and you need to have SSL enabled. Free browsers are readily available for Windows, Macintosh, or UNIX/Linux.

For the initial connection to the Internet and configuration of the UTM, you need to connect a computer to the UTM, and the computer needs to be configured to automatically get its TCP/IP configuration from the UTM through DHCP.

The cable or DSL modem broadband access device needs to provide a standard 10 Mbps (10BASE-T) Ethernet interface.

Internet Configuration Requirements

Depending on how your ISP set up your Internet accounts, you will need the following Internet configuration information to connect UTM to the Internet:

- Host and domain names
- One or more ISP login names and passwords
- ISP Domain Name Server (DNS) addresses
- One or more fixed IP addresses (also known as static IP addresses)

Where Do I Get the Internet Configuration Information?

There are several ways you can gather the required Internet connection information.

- Your ISPs provide all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide you with it, or, if you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
    - For Windows 95/98/ME, open the Network Control Panel, select the TCP/IP entry for the Ethernet adapter, and click **Properties**. Record all the settings for each tab.
    - For Windows 2000/XP/Vista, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click **Properties**. Record all the settings for each tab.
    - For Macintosh computers, open the TCP/IP or Network Control Panel. Record all the settings for each section.

After you have located your Internet configuration information, you might want to record the information in the following section.

Internet Connection Information

Print these pages with the Internet connection information. Fill in the configuration settings that are provided to you by ISP.

- **ISP login name**: The login name and password are case-sensitive and need to be entered exactly as given by your ISP. For AOL customers, the login name is the primary screen name. Some ISPs use your full email address as the login name. The service name is not required by all ISPs. If you connect using a login name and password, then fill in the following:

  Login name: _____

  Password: _____

  Service name: _____

- **Fixed or static IP address**: If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

  Fixed or static Internet IP address: _____._____._____._____

  Gateway IP address: _____._____._____._____

  Subnet mask: _____._____._____._____

- **ISP DNS server addresses**: If you were given DNS server addresses, fill in the following:

  Primary DNS server IP address: _____._____._____._____

  Secondary DNS server IP address: _____._____._____._____

- **Host and domain names**: Some ISPs use a specific host or domain name like CCA7324-A or home. If you have not been given host or domain names, you can use the following examples as a guide:

  - If your main email account with your ISP is aaa@yyy.com, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
  - If your ISP's mail server is mail.xxx.yyy.com, then use **xxx.yyy.com** as the domain name.

  ISP host name: _____

  ISP domain name: _____

- **Fully qualified domain name**: Some organizations use a fully qualified domain name (FQDN) from a Dynamic DNS service provider for their IP addresses.

  Dynamic DNS service provider: _____

  FQDN: _____

Overview of the Planning Process

The areas that require planning when you use a firewall that has dual WAN ports such as the UTM include the following:

- Inbound traffic (port forwarding, port triggering)
- Outbound traffic (protocol binding)
- Virtual private networks (VPNs)

The two WAN ports can be configured on a mutually exclusive basis to either of the following:

- Auto-rollover for increased reliability
- Load balance for outgoing traffic

These various types of traffic and auto-rollover or load balancing all interact to make the planning process more challenging:

- **Inbound traffic**. Unrequested incoming traffic can be directed to a PC on your LAN rather than being discarded. The mechanism for making the IP address public depends on whether the dual WAN ports are configured for auto-rollover or load balancing.

- **Virtual private networks**. A virtual private network (VPN) tunnel provides a secure communication channel either between two gateway VPN firewalls or between a remote PC client and gateway VPN firewall. As a result, the IP address of at least one of the tunnel endpoints needs to be known in advance in order for the other tunnel endpoint to establish (or reestablish) the VPN tunnel.

Note: When the UTM's WAN port rolls over, the VPN tunnel collapses and needs to be reestablished using the new WAN IP address. However, you can configure automatic IPSec VPN rollover to ensure that an IPSec VPN tunnel is reestablished.

- **Dual WAN ports in auto-rollover mode**. Rollover for a UTM with dual WAN ports is different from a single WAN port gateway configuration when you specify the IP address. Only one WAN port is active at a time, and when it rolls over, the IP address of the active WAN port always changes. Therefore, the use of a fully qualified domain name (FQDN) is always required, even when the IP address of each WAN port is fixed.
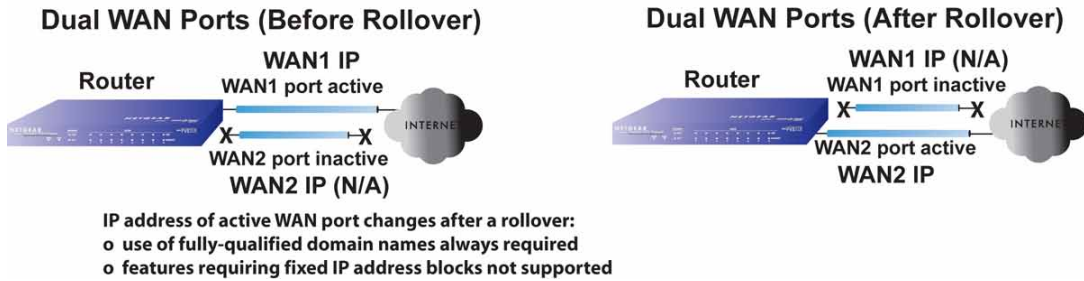
Figure 326.

Features such as multiple exposed hosts are not supported in auto-rollover mode because the IP address of each WAN port needs to be in the identical range of fixed addresses.

- **Dual WAN ports in load balancing mode**. Load balancing for a UTM with dual WAN ports is similar to a single WAN gateway configuration when you specify the IP address. Each IP address is either fixed or dynamic based on the ISP: You need to use FQDNs when the IP address is dynamic, but FQDNs are optional when the IP address is static.
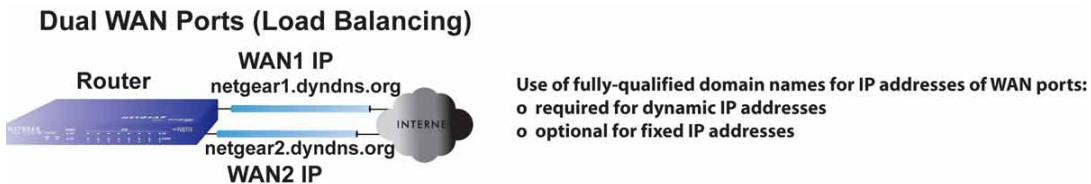
Figure 327.

Inbound Traffic

Incoming traffic from the Internet is usually discarded by the UTM unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can configure the UTM to forward it to one or more LAN hosts on your network.

The addressing of the UTM's dual WAN port depends on the configuration being implemented.

Table 146. IP addressing requirements for exposed hosts in dual WAN port systems

Configuration and WAN IP address		Single WAN port (reference case)	Dual WAN port cases	
			Rollover mode	Load balancing mode
Inbound traffic • Port forwarding • Port triggering	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

Inbound Traffic to a Single WAN Port System

The Internet IP address of the UTM's WAN port needs to be known to the public so that the public can send incoming traffic to the exposed host when this feature is supported and enabled.

In the single WAN case, the WAN's Internet address is either fixed IP or an FQDN if the IP address is dynamic.

Figure 328.

Inbound Traffic to a Dual WAN Port System

The IP address range of the UTM's WAN port needs to be both fixed and public so that the public can send incoming traffic to the multiple exposed hosts when this feature is supported and enabled.

Inbound Traffic: Dual WAN Ports for Improved Reliability

In a dual WAN port auto-rollover configuration, the WAN port's IP address will always change when a rollover occurs. You need to use an FQDN that toggles between the IP addresses of the WAN ports (that is, WAN1 or WAN2).
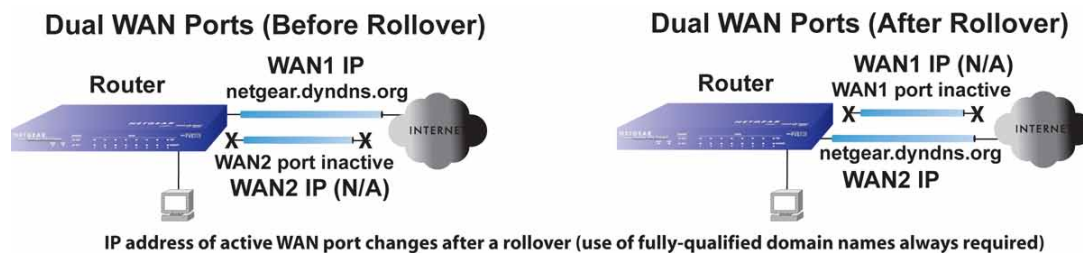
Figure 329.

Inbound Traffic: Dual WAN Ports for Load Balancing

In a dual WAN port load-balancing configuration, the Internet address of each WAN port is either fixed if the IP address is fixed or an FQDN if the IP address is dynamic (see the following figure).

Note: Load balancing is implemented for outgoing traffic and not for incoming traffic. Consider making one of the WAN port Internet addresses public and keeping the other one private in order to maintain better control of WAN port traffic.
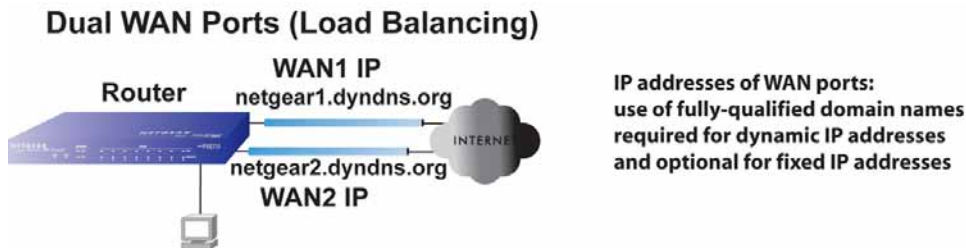
Figure 330.

Virtual Private Networks

When implementing virtual private network (VPN) tunnels, you need to use a mechanism for determining the IP addresses of the tunnel endpoints. The addressing of the firewall's dual WAN port depends on the configuration being implemented.

Table 147. IP addressing requirements for VPNs in dual WAN port systems

Configuration and WAN IP address		Single WAN port configurations (reference cases)	Dual WAN port configurations	
			Rollover Mode[1]	Load balancing mode
VPN Road Warrior (Client-to-Gateway)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Telecommuter (Client-to-Gateway through a NAT Router)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

1. After a rollover, all tunnels need to be reestablished using the new WAN IP address.

For a single WAN gateway configuration, use an FQDN when the IP address is dynamic and either an FQDN or the IP address itself when the IP address is fixed. The situation is different in dual WAN port gateway configurations.

- **Dual WAN ports in auto-rollover mode**. A dual WAN port auto-rollover gateway configuration is different from a single WAN port gateway configuration when you specify

the IP address of the VPN tunnel endpoint. Only one WAN port is active at a time, and when it rolls over, the IP address of the active WAN port always changes. Therefore, the use of an FQDN is always required, even when the IP address of each WAN port is fixed.

Note: When the UTM's WAN port rolls over, the VPN tunnel collapses and need to be reestablished using the new WAN IP address. However, you can configure automatic IPSec VPN rollover to ensure that an IPSec VPN tunnel is reestablished.
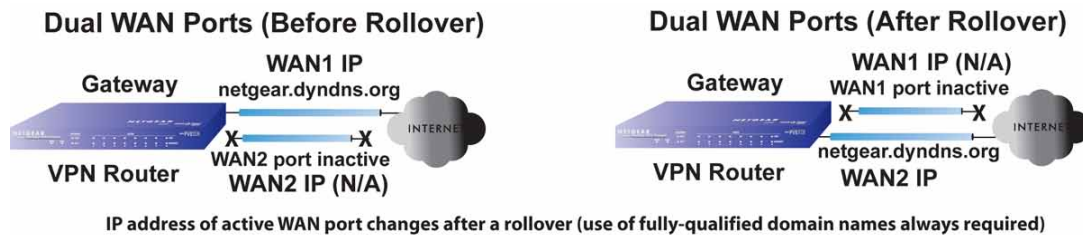
Figure 331.

- **Dual WAN ports in load balancing mode**. A dual WAN port load balancing gateway configuration is the same as a single WAN port configuration when you specify the IP address of the VPN tunnel endpoint. Each IP address is either fixed or dynamic based on the ISP: You need to use FQDNs when the IP address is dynamic, and FQDNs are optional when the IP address is static.
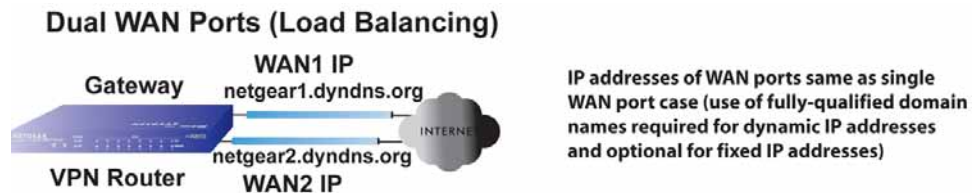
Figure 332.

VPN Road Warrior (Client-to-Gateway)

The following situations exemplify the requirements for a remote PC client with no firewall to establish a VPN tunnel with a gateway VPN firewall such as an UTM:

- Single-gateway WAN port
- Redundant dual-gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Road Warrior: Single-Gateway WAN Port (Reference Case)

In a single WAN port gateway configuration, the remote PC client initiates the VPN tunnel because the IP address of the remote PC client is not known in advance. The gateway WAN port needs to function as the responder.
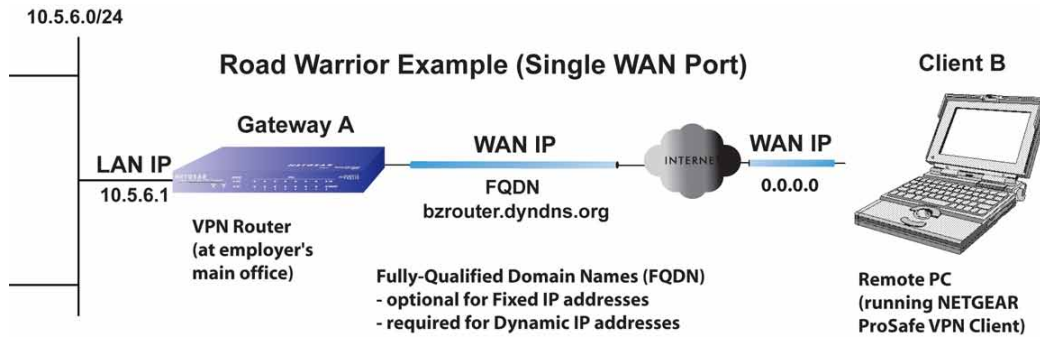
Figure 333.

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, an FQDN needs to be used. If the IP address is fixed, an FQDN is optional.

VPN Road Warrior: Dual-Gateway WAN Ports for Improved Reliability

In a dual WAN port auto-rollover gateway configuration, the remote PC client initiates the VPN tunnel with the active WAN port (port WAN1 in the following figure) because the IP address of the remote PC client is not known in advance. The gateway WAN port needs to function as a responder.
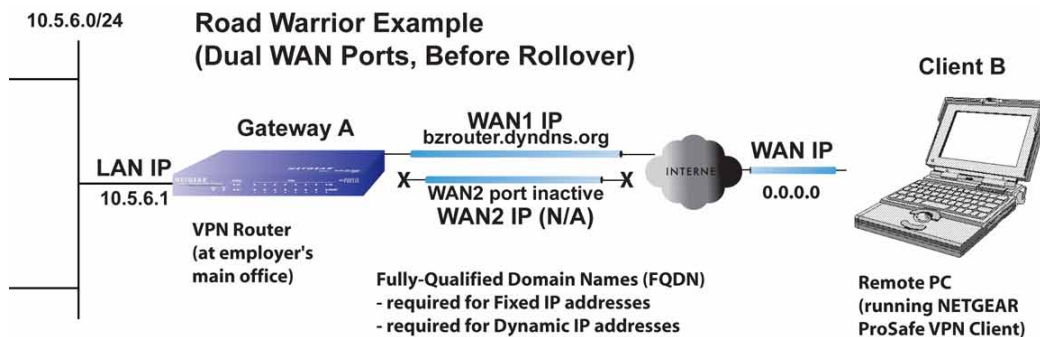
Figure 334.

The IP addresses of the WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN port could be either WAN1 or WAN2 (that is, the IP address of the active WAN port is not known in advance).

After a rollover of the WAN port has occurred, the previously inactive gateway WAN port becomes the active port (port WAN2 in the following figure) and the remote PC client needs to reestablish the VPN tunnel. The gateway WAN port needs to function as the responder.
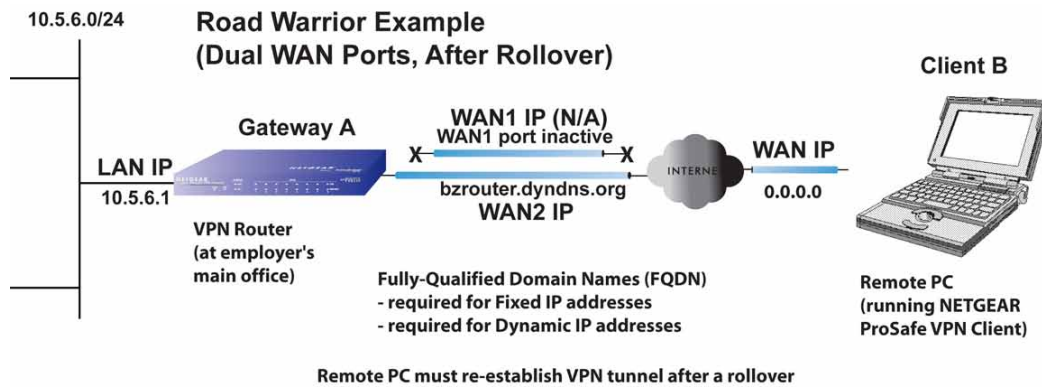
Figure 335.

The purpose of the FQDN in this case is to toggle the domain name of the gateway firewall between the IP addresses of the active WAN port (that is, WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or reestablish a VPN tunnel.

VPN Road Warrior: Dual-Gateway WAN Ports for Load Balancing

In a dual WAN port load balancing gateway configuration, the remote PC initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the active WAN port is not known in advance. The selected gateway WAN port needs to function as the responder.
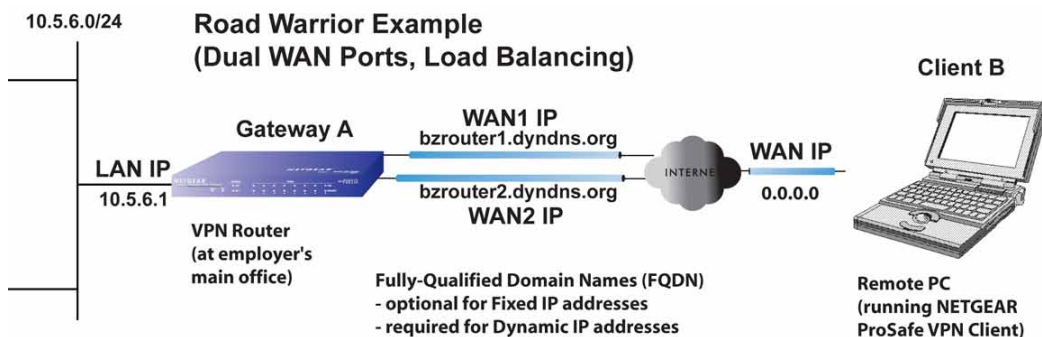
Figure 336.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Gateway-to-Gateway

The following situations exemplify the requirements for a gateway VPN firewall such as an UTM to establish a VPN tunnel with another gateway VPN firewall:

- Single-gateway WAN ports
- Redundant dual-gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Gateway-to-Gateway: Single-Gateway WAN Ports (Reference Case)

In a configuration with two single WAN port gateways, either gateway WAN port can initiate the VPN tunnel with the other gateway WAN port because the IP addresses are known in advance.
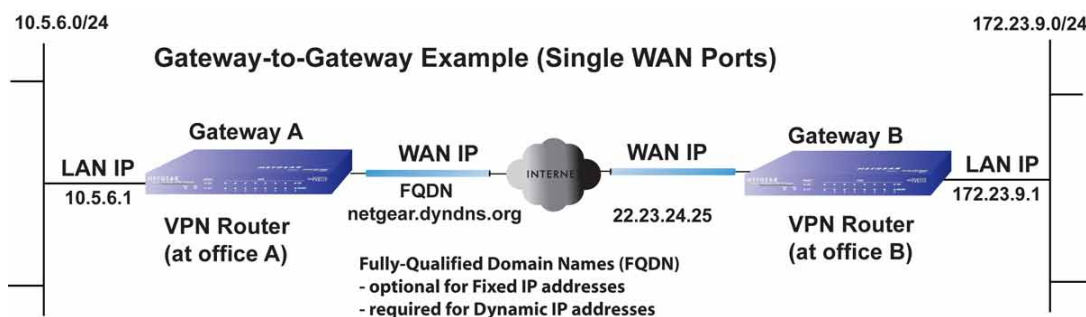
Figure 337.

The IP address of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use a FQDN. If an IP address is fixed, an FQDN is optional.

VPN Gateway-to-Gateway: Dual-Gateway WAN Ports for Improved Reliability

In a configuration with two dual WAN port VPN gateways that function in auto-rollover mode, either of the gateway WAN ports at one end can initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to balance the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance. In this example (see
the following figure), port WAN_A1 is active and port WAN_A2 is inactive at Gateway A; port WAN_B1 is active and port WAN_B2 is inactive at Gateway B.
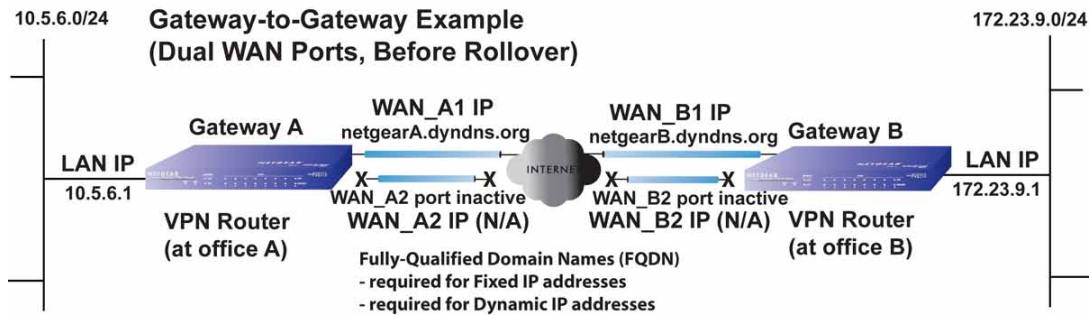
Figure 338.

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN ports could be either WAN_A1, WAN_A2, WAN_B1, or WAN_B2 (that is, the IP address of the active WAN ports is not known in advance).

After a rollover of a gateway WAN port, the previously inactive gateway WAN port becomes the active port (port WAN_A2 in the following figure), and one of the gateways needs to reestablish the VPN tunnel.
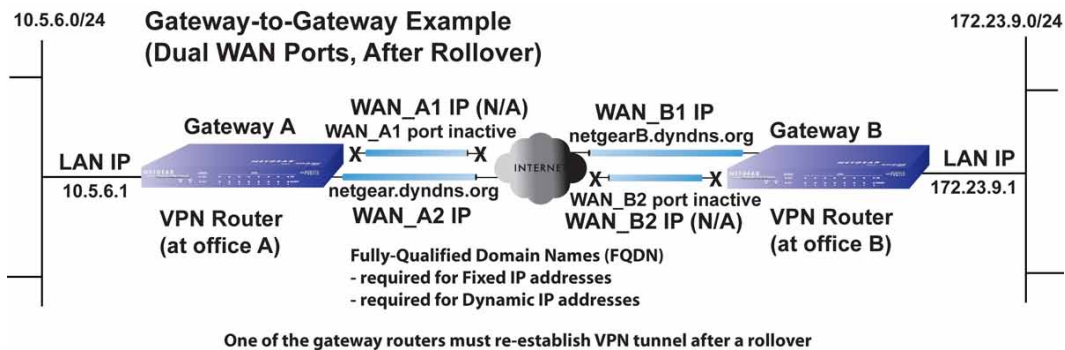
Figure 339.

The purpose of the FQDNs is to toggle the domain name of the rolled-over gateway between the IP addresses of the active WAN port (that is, WAN_A1 and WAN_A2 in the previous figure) so that the other end of the tunnel has a known gateway IP address to establish or reestablish a VPN tunnel.

VPN Gateway-to-Gateway: Dual-Gateway WAN Ports for Load Balancing

In a configuration with two dual WAN port VPN gateways that function in load balancing mode, either of the gateway WAN ports at one end can be programmed in advance to initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to manage the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance.
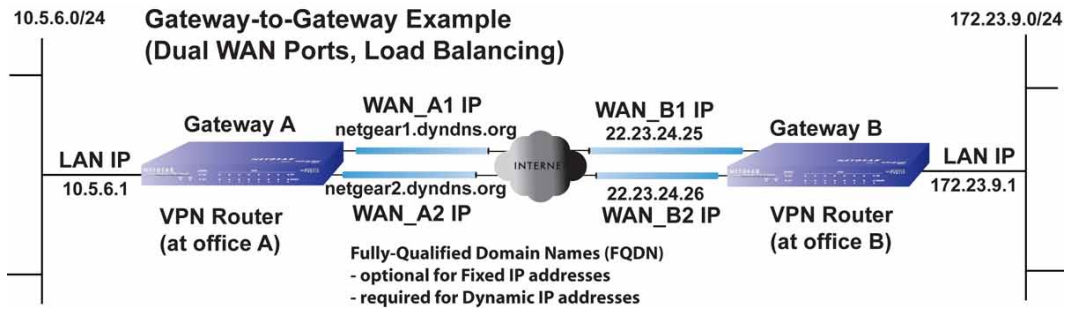
Figure 340.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Telecommuter (Client-to-Gateway through a NAT Router)

> **Note:** The telecommuter case assumes that the home office has a dynamic IP address and NAT router.

The following situations exemplify the requirements for a remote PC client connected to the Internet with a dynamic IP address through a NAT router to establish a VPN tunnel with a gateway VPN firewall such as an UTM at the company office:

- Single-gateway WAN port
- Redundant dual-gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Telecommuter: Single-Gateway WAN Port (Reference Case)

In a single WAN port gateway configuration, the remote PC client at the NAT router initiates the VPN tunnel because the IP address of the remote NAT router is not known in advance. The gateway WAN port needs to function as the responder.
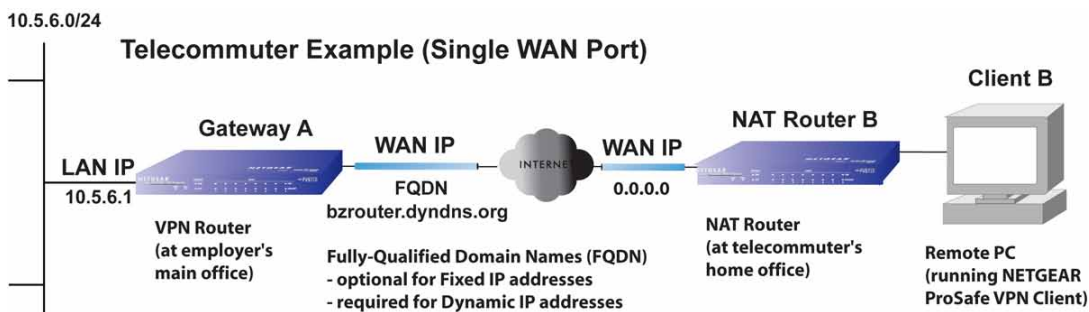
Figure 341.

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, you need to use an FQDN. If the IP address is fixed, an FQDN is optional.

VPN Telecommuter: Dual-Gateway WAN Ports for Improved Reliability

In a dual WAN port auto-rollover gateway configuration, the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in the following figure) because the IP address of the remote NAT router is not known in advance. The gateway WAN port needs to function as the responder.

Figure 342.

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN port could be either WAN1 or WAN2 (that is, the IP address of the active WAN port is not known in advance).

After a rollover of the WAN port has occurred, the previously inactive gateway WAN port becomes the active port (port WAN2 in the following figure), and the remote PC needs to reestablish the VPN tunnel. The gateway WAN port needs to function as the responder.
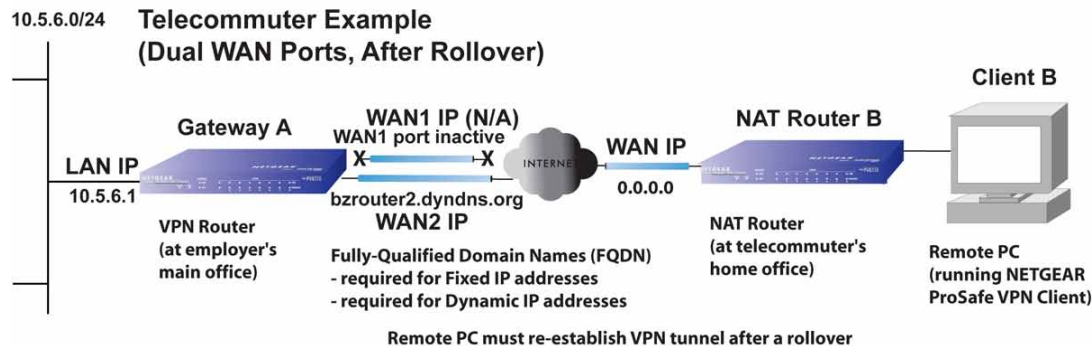
Figure 343.

The purpose of the FQDN is to toggle the domain name of the gateway between the IP addresses of the active WAN port that is, WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or reestablish a VPN tunnel.

VPN Telecommuter: Dual-Gateway WAN Ports for Load Balancing

In a dual WAN port load balancing gateway configuration, the remote PC client initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote NAT router is not known in advance. The selected gateway WAN port needs to function as the responder.
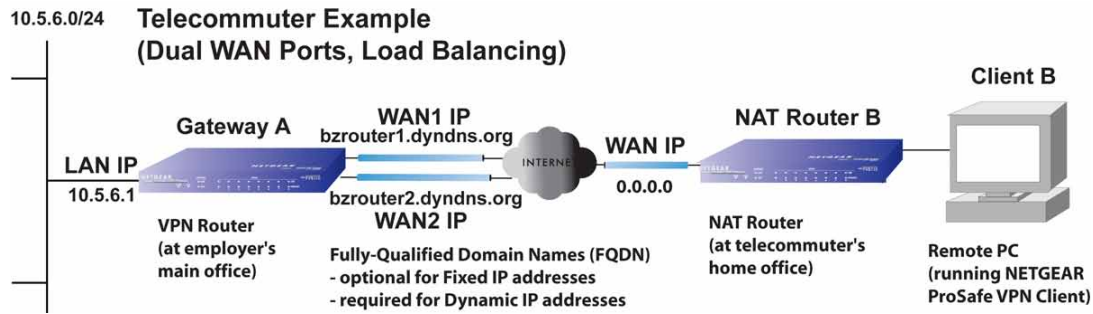
Figure 344.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

ReadyNAS Integration

D

This appendix describes how to set up a UTM9S with a NETGEAR ReadyNAS. This appendix includes the following sections:

- *Supported ReadyNAS Models*
- *Install the UTM9S Add-On on the ReadyNAS*
- *Connect to the ReadyNAS on the UTM9S*

Supported ReadyNAS Models

The following ReadyNAS models are supported for integration with the UTM9S:

- ReadyNAS 1500
- ReadyNAS 2100
- ReadyNAS 3100
- ReadyNAS 3200
- ReadyNAS 4200
- ReadyNAS Ultra 2/Plus
- ReadyNAS Ultra 4/Plus
- ReadyNAS Ultra 6/Plus
- ReadyNAS Pro 2
- ReadyNAS Pro 4
- ReadyNAS Pro 6
- ReadyNAS Pro Business Edition
- ReadyNAS Pro Pioneer Edition
- ReadyNAS NVX
- ReadyNAS NVX Pioneer Edition

Install the UTM9S Add-On on the ReadyNAS

➢ **To install the UTM9S add-on on the ReadyNAS:**

1. Start a web browser.

2. In the address field, enter the IP address of the ReadyNAS, for example, enter **https://192.168.168.168**. The ReadyNAS web management interface displays.

3. In the User Name field, type **admin**; in the Password field, type **netgear1**.

4. Select **Add-ons > Add New**.
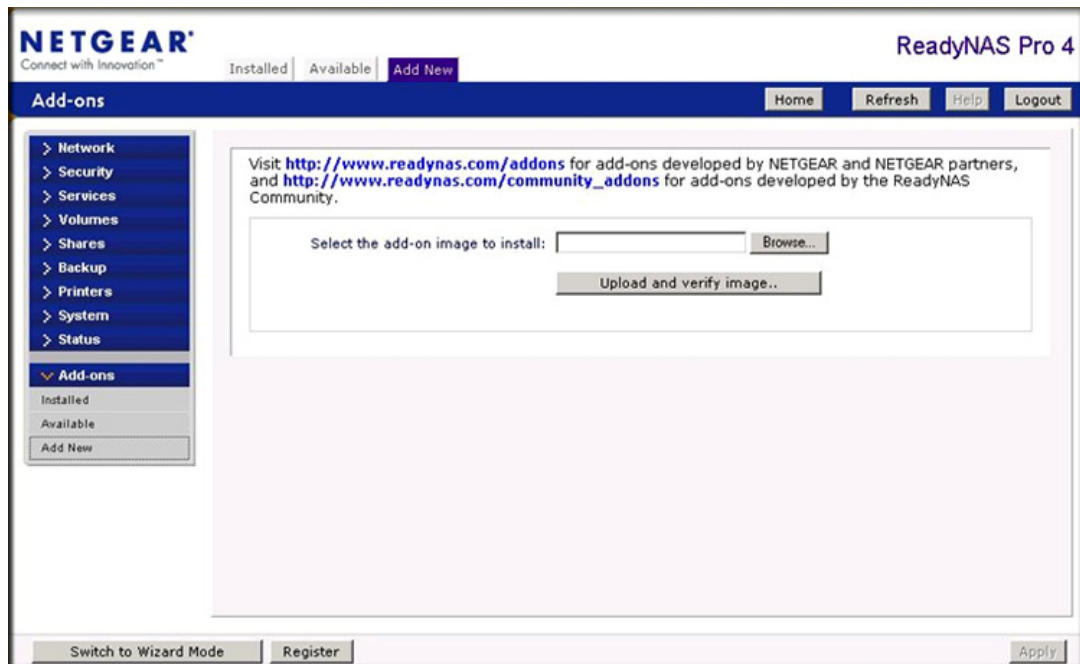
Figure 345.

5. Click **Browse**. Navigate to and select the UTM9S add-on image.

6. Click **Upload and verify image**. When the upload is finished and the image has been verified, the screen adjusts.
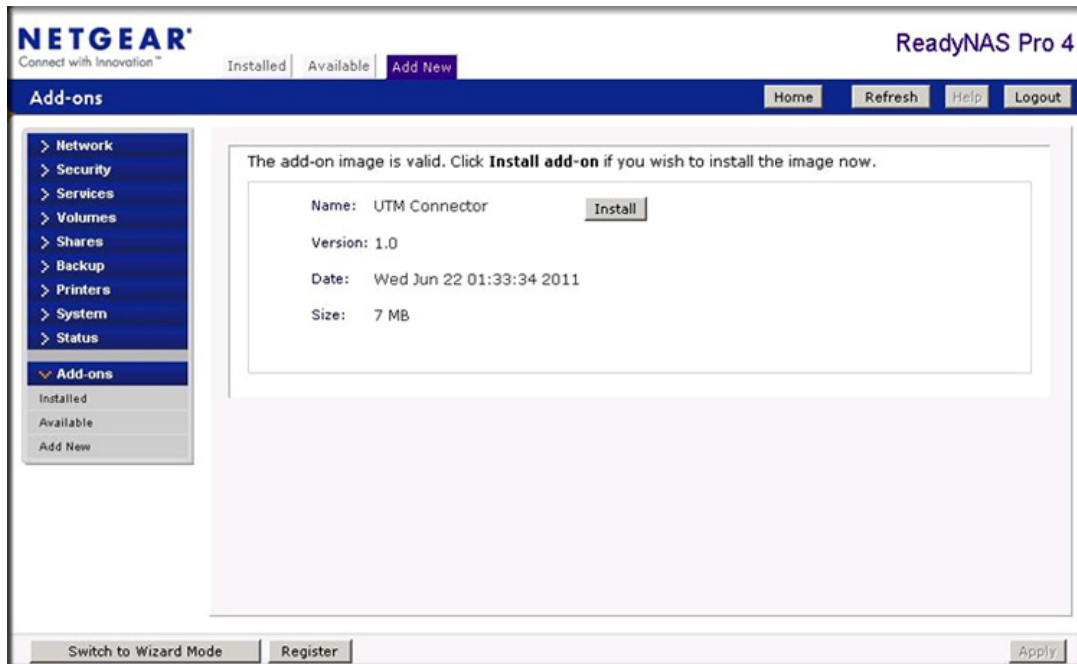
Figure 346.

7. Click **Install**.

8. **Select Add-ons > Installed**.
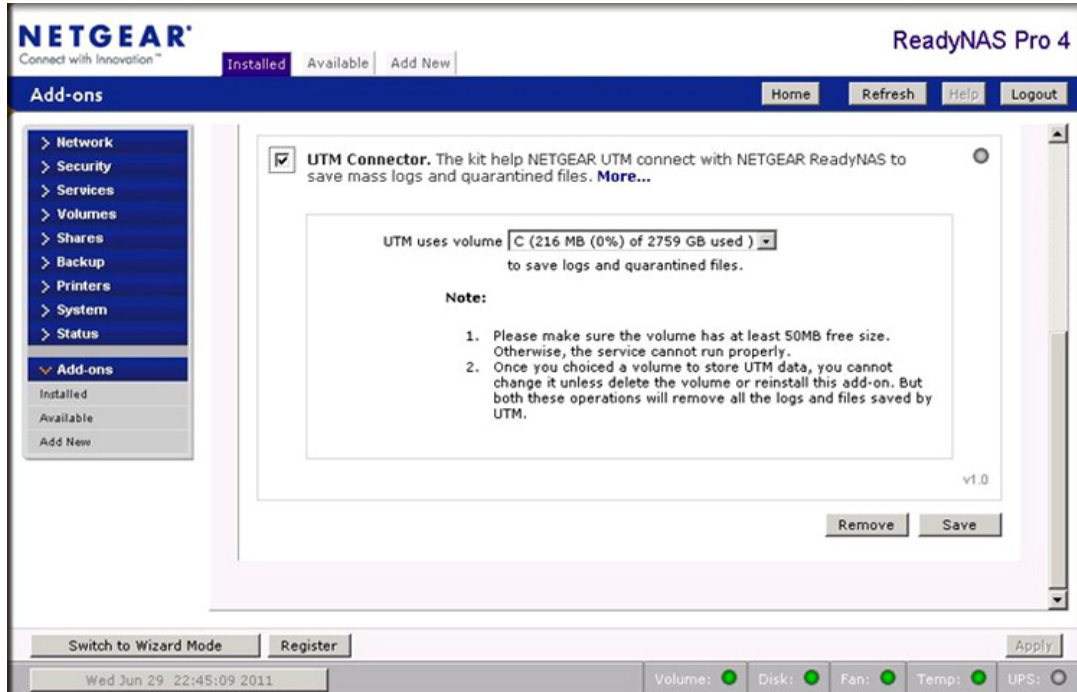
Figure 347.

9. Select the **UTM Connector** check box to enable the UTM connection.

10. Click **Save**. The status indicator shows green.
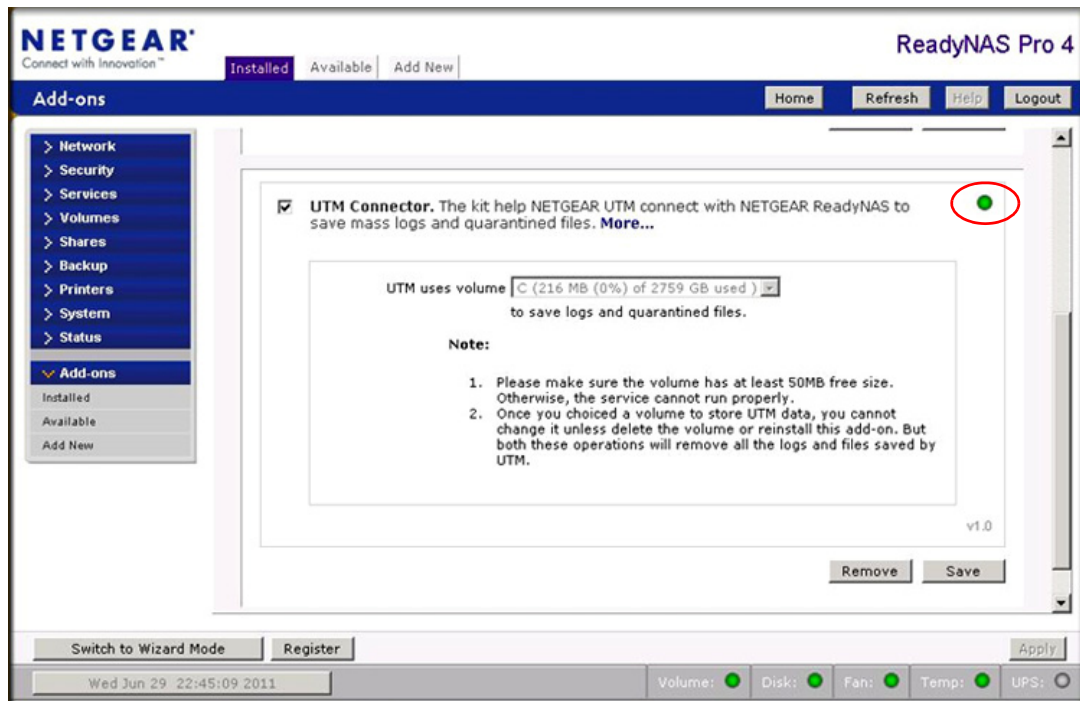
Figure 348.

Connect to the ReadyNAS on the UTM9S

➢ **To connect to the ReadyNAS on the UTM9S:**

1. Select **Administration > ReadyNAS Integration**. The ReadyNAS Integration screen displays:
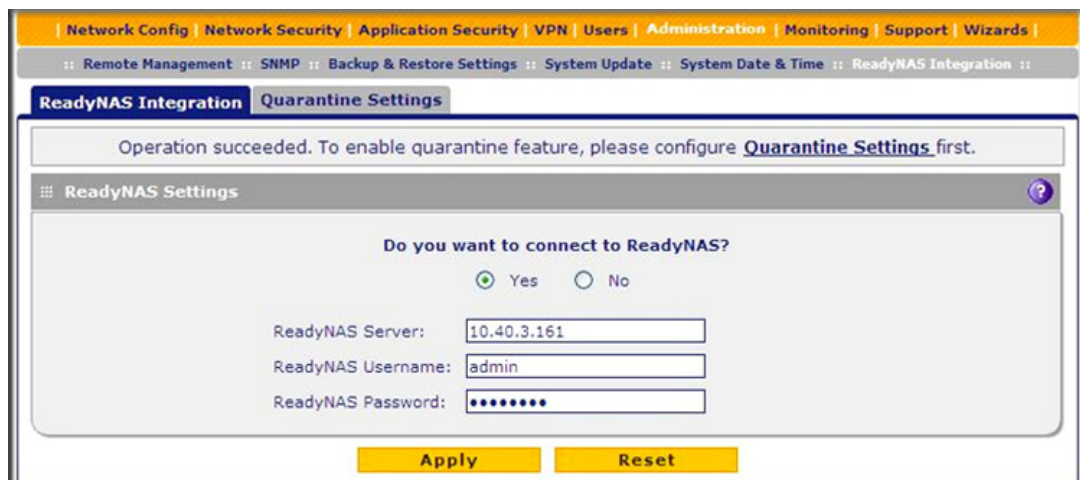
Figure 349.

2. To connect to the ReadyNAS, click the **Yes** radio button.

ReadyNAS Integration

575

3. Enter the settings as explained in the following table:

Table 148. ReadyNAS Integration screen settings

Setting	Description
ReadyNAS Server	The IP address of the ReadyNAS server.
ReadyNAS Username	The user name to access the ReadyNAS. By default, the user name is admin.
ReadyNAS Password	The password to access the ReadyNAS. By default, the password is netgear1.

4. Click **Apply** to save your settings.

5. Select **Administration > Quarantine Settings**. The Quarantine Settings screen displays:
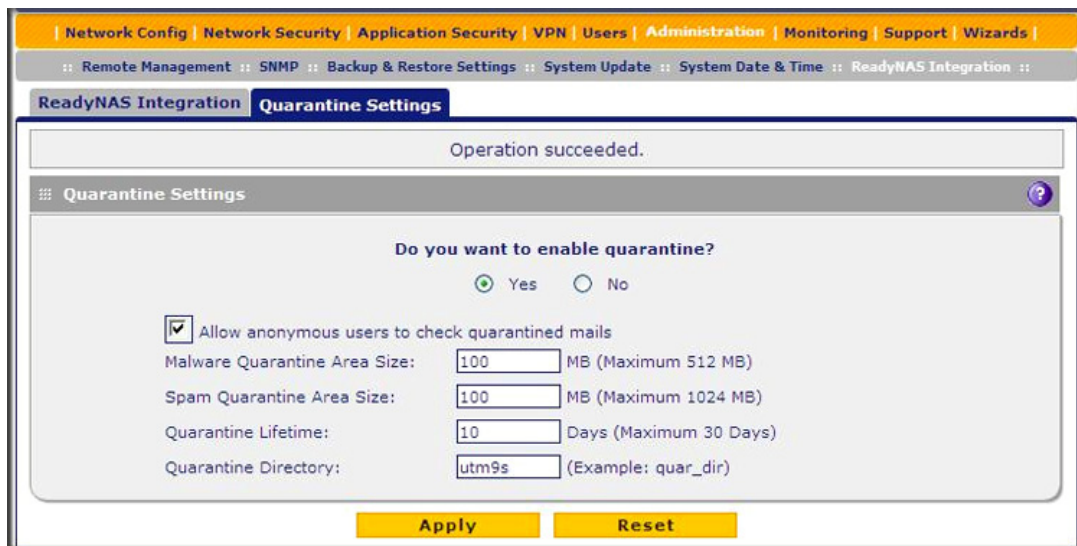
Figure 350.

6. To enable quarantine files to be saved to the ReadyNAS, click the **Yes** radio button. (For information about how to configure the quarantine settings, see *Configure the Quarantine Settings* on page 416).

7. Click **Apply** to save your settings.

8. Select **Monitoring > System Status**. The System Status screen displays. When the UTM9S connects with the ReadyNAS, the ReadyNAS Status and Quarantine Status fields in the Status section of the screen show NORMAL in green font. The following figure shows the top of the System Status screen only.
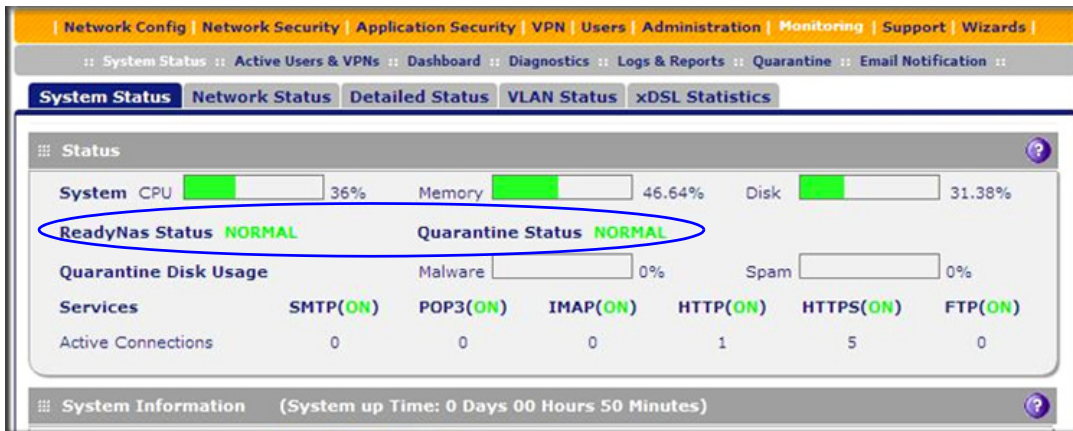
Figure 351.

Two-Factor Authentication

E

This appendix provides an overview of two-factor authentication, and an example of how to implement the WiKID solution. This appendix contains the following sections:

Why Do I Need Two-Factor Authentication?

In today's market, online identity theft and online fraud continue to be one of the fast-growing cybercrime activities used by many unethical hackers and cybercriminals to steal digital assets for financial gains. Many companies and corporations are losing millions of dollars and running into risks of revealing their trade secrets and other proprietary information as a result of these cybercrime activities. Security threats and hackers have become more sophisticated, and user names, encrypted passwords, and the presence of firewalls are no longer enough to protect the networks from being compromised. IT professionals and security experts have recognized the need to go beyond the traditional authentication process by introducing and requiring additional factors in the authentication process. NETGEAR has also recognized the need to provide more than just a firewall to protect the networks. NETGEAR has implemented a more robust authentication system known as two-factor authentication (2FA or T-FA) to help address the fast-growing network security issues.

What Are the Benefits of Two-Factor Authentication?

- **Stronger security**. Passwords cannot efficiently protect the corporate networks because attackers can easily guess simple passwords or users cannot remember complex and unique passwords. One-time passcode (OTP) strengthens and replaces the need to remember complex password.

- **No need to replace existing hardware**. Two-factor authentication can be added to existing NETGEAR products through a firmware upgrade.

- **Quick to deploy and manage**. The WiKID solution integrates seamlessly with the NETGEAR SSL and VPN firewall products.

- **Proven regulatory compliance**. Two-factor authentication has been used as a mandatory authentication process for many corporations and enterprises worldwide.

What Is Two-Factor Authentication?

Two-factor authentication is a security solution that enhances and strengthens security by implementing multiple factors of the authentication process that challenge and confirm the users' identities before they can gain access to the network. There are several factors that are used to validate the users to make sure that you are who you say you are. These factors are:

- Something you know—for example, your password or your PIN.
- Something you have—for example, a token with generated passcode that is 6 to 8 digits in length.
- Something you are—for example, biometrics such as fingerprints or retinal prints.

This appendix focuses on and discusses only the first two factors, something you know and something you have. This security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you have. A common example of two-factor authentication is a bank (ATM) card that has been issued by a bank institute:

- The PIN to access your account is *something you know.*
- The ATM card is *something you have.*

You need to have both of these factors to gain access to your bank account. Similar to the way ATM cards work, access to the corporate networks and data can also be strengthened using a combination of multiple factors such as a PIN and a token (hardware or software) to validate the users and reduce the incidence of online identity theft.

NETGEAR Two-Factor Authentication Solutions

NETGEAR has implemented 2 two-factor authentication solutions from WiKID. WiKID is the software-based token solution. So instead of using only Windows Active Directory or LDAP as the authentication server, administrators now have the option to use WiKID to perform two-factor authentication on NETGEAR SSL and VPN firewall products.

The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), which is time-synchronized with the authentication server, is generated and sent to the user after the validity of a user credential has been confirmed by the server.

The request-response architecture is capable of self-service initialization by end users, dramatically reducing implementation and maintenance costs.

➢ **To use WiKID (for end users):**

1. Launch the WiKID token software, enter the PIN that has been provided (*something the user know*s), and then click **Continue** to receive the OTP from the WiKID authentication server:

Figure 352.

2. A one-time passcode (*something the user has*) is generated.
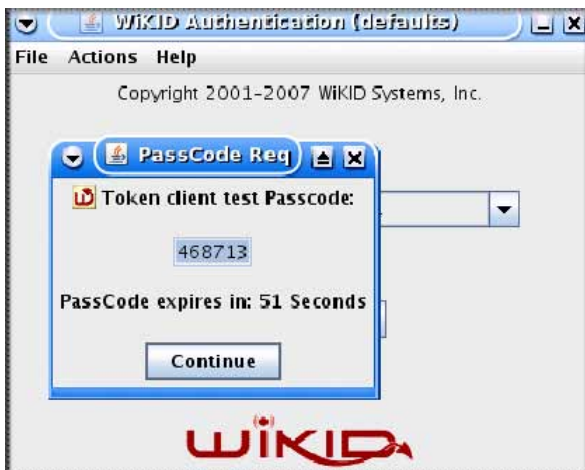
Figure 353.

Note: The one-time passcode is time-synchronized to the authentication server so that the OTP can be used only once and needs to be used before the expiration time. If a user does not use this passcode before it expires, the user needs to go through the request process again to generate a new OTP.

---

3. Proceed to the 2 Factor Authentication login screen and enter the one-time passcode as the login password.
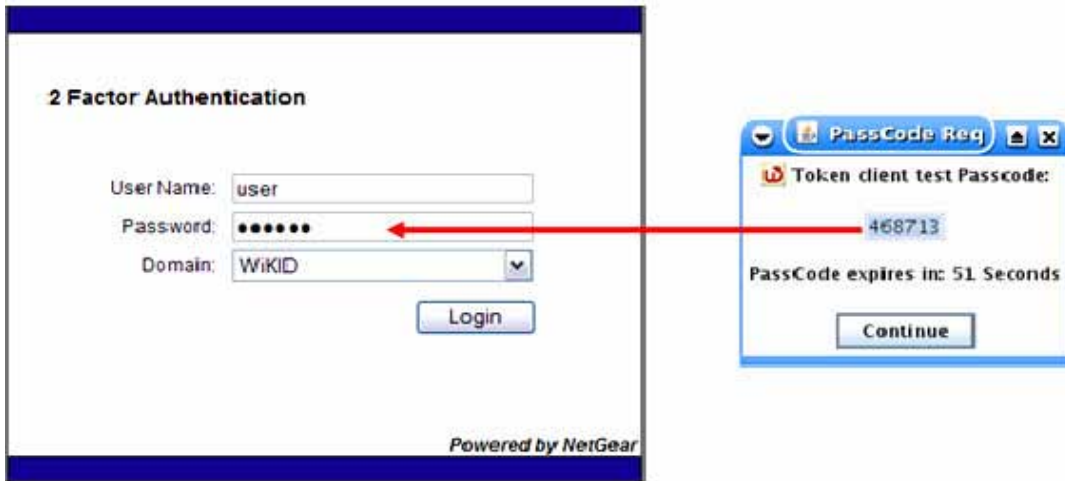
Figure 354.

System Logs and Error Messages

F

This appendix provides examples and explanations of system logs and error message. When applicable, a recommended action is provided. This appendix contains the following sections:

- *System Log Messages*
- *Content-Filtering and Security Logs*
- *Routing Logs*

This appendix uses the log message terms that are described in the following table:

Table 149. Log message terms

Term	Description
[UTM]	System identifier.
[kernel]	Message from the kernel.
CODE	Protocol code (for example, protocol is ICMP, type 8) and CODE=0 means successful reply.
DEST	Destination IP address of the machine to which the packet is destined.
DPT	Destination port.
IN	Incoming interface for packet.
OUT	Outgoing interface for packet.
PROTO	Protocol used.
SELF	Packet coming from the system only.
SPT	Source port.
SRC	Source IP address of machine from which the packet is coming.
TYPE	Protocol type.

System Log Messages

This section describes log messages that belong to one of the following categories:

- Logs that are generated by traffic that is meant for the UTM.
- Logs that are generated by traffic that is routed or forwarded through the UTM.
- Logs that are generated by system daemons: the NTP daemon, the WAN daemon, and others daemons.

System Startup

This section describes log messages generated during system startup.

Table 150. System logs: system startup

Message	Jan 1 15:22:28 [UTM] [ledTog] [SYSTEM START-UP] System Started
Explanation	Logs that are generated when the system is started.
Recommended Action	None.

Reboot

This section describes log messages generated during a system reboot.

Table 151. System logs: reboot

Message	Nov 25 19:42:57 [UTM] [reboot] Rebooting in 3 seconds
Explanation	Logs that are generated when the system is rebooted from the web management interface.
Recommended Action	None.

Service Logs

This section describes log messages generated during firmware updates and other service-related events.

Table 152. System logs: service

Message	2008-12-31 23:59:48 error Firmware update failed! Either the subscription is not yet registered, or has expired.
Explanation	Logs that are generated when a firmware update fails or succeeds. The message shows the date and time, and the event. **Note:** The service log includes miscellaneous service messages.
Recommended Action	None.

NTP

This section describes log messages generated by the NTP daemon during synchronization with the NTP server. The fixed time and date before NTP synchronizes with any of the servers is Fri 1999 Dec 31 19:13:00.

Table 153. System logs: NTP

Message 1	Nov 28 12:31:13 [UTM] [ntpdate] Looking Up time-f.netgear.com
Message 2	Nov 28 12:31:13 [UTM] [ntpdate] Requesting time from time-f.netgear.com
Message 3	Nov 28 12:31:14 [UTM] [ntpdate] adjust time server 69.25.106.19 offset 0.140254 sec
Message 4	Nov 28 12:31:14 [UTM] [ntpdate] Synchronized time with time-f.netgear.com
Message 5	Nov 28 12:31:16 [UTM] [ntpdate] Date and Time Before Synchronization: Tue Nov 28 12:31:13 GMT+0530 2006
Message 6	Nov 28 12:31:16 [UTM] [ntpdate] Date and Time After Synchronization: Tue Nov 28 12:31:16 GMT+0530 2006
Example	Nov 28 12:31:16 [UTM] [ntpdate] Next Synchronization after 2 Hours
Explanation	Message 1: DNS resolution for the NTP server (time-f.netgear.com).
	Message 2: Request for NTP update from the time server.
	Message 3: Adjust time by resetting system time.
	Message 4: Display date and time before synchronization, that is, when resynchronization started.
	Message 5: Display the new updated date and time.
	Message 6: Next synchronization will occur after the specified time. Example: In these logs the next synchronization will occur after 2 hours.
Recommended Action	None.

Login/Logout

This section describes logs that are generated by the administrative interfaces of the device.

Table 154. System logs: login/logout

Message	Nov 28 14:45:42 [UTM] [login] Login succeeded: user admin from 192.168.10.10
Explanation	Login of user admin from host with IP address 192.168.10.10.
Recommended Action	None.
Message	Nov 28 14:55:09 [UTM] [seclogin] Logout succeeded for user admin Nov 28 14:55:13 [UTM] [seclogin] Login succeeded: user admin from 192.168.1.214
Explanation	Secure login/logout of user admin from host with IP address 192.168.1.214.
Recommended Action	None.

Firewall Restart

This section describes logs that are generated when the firewall restarts.

Table 155. System logs: firewall restart

Message	Jan 23 16:20:44 [UTM] [wand] [FW] Firewall Restarted
Explanation	Logs that are generated when the firewall is restarted. This message is logged when the VPN firewall restarts after any changes in the configuration are applied.
Recommended Action	None.

IPSec Restart

This section describes logs that are generated when IPSec restarts.

Table 156. System logs: IPSec restart

Message	Jan 23 16:20:44 [UTM] [wand] [IPSEC] IPSEC Restarted
Explanation	Logs that are generated when the IPsec is restarted. This message is logged when IPsec restarts after any changes in the configuration are applied.
Recommended Action	None.

WAN Status

This section describes the logs that are generated by the WAN component. If there are two ISP links for Internet connectivity, the router can be configured either in auto-rollover mode or load balancing mode.

Auto-Rollover Mode

When the WAN mode is configured for auto-rollover, the primary link is active and the secondary link acts only as a backup. When the primary link goes down, the secondary link becomes active only until the primary link comes back up.

The UTM monitors the status of the primary link using the configured WAN failure detection method.

This section describes the logs that are generated when the WAN mode is set to auto-rollover.

Table 157. System logs: WAN status, auto rollover

Message	Nov 17 09:59:09 [UTM] [wand] [LBFO] WAN1 Test Failed 1 of 3 times_
	Nov 17 09:59:39 [UTM] [wand] [LBFO] WAN1 Test Failed 2 of 3 times_
	Nov 17 10:00:09 [UTM] [wand] [LBFO] WAN1 Test Failed 3 of 3 times_
	Nov 17 10:01:01 [UTM] [wand] [LBFO] WAN1 Test Failed 4 of 3 times_
	Nov 17 10:01:35 [UTM] [wand] [LBFO] WAN1 Test Failed 5 of 3 times_
	Nov 17 10:01:35 [UTM] [wand] [LBFO] WAN1(DOWN), WAN2(UP), ACTIVE(WAN2)_
	Nov 17 10:02:25 [UTM] [wand] [LBFO] WAN1 Test Failed 6 of 3 times_
	Nov 17 10:02:25 [UTM] [wand] [LBFO] Restarting WAN1_
	Nov 17 10:02:57 [UTM] [wand] [LBFO] WAN1 Test Failed 7 of 3 times_
	Nov 17 10:03:27 [UTM] [wand] [LBFO] WAN1 Test Failed 8 of 3 times_
	Nov 17 10:03:57 [UTM] [wand] [LBFO] WAN1 Test Failed 9 of 3 times_
	Nov 17 10:03:57 [UTM] [wand] [LBFO] Restarting WAN1_
Explanation	The logs suggest that the failover was detected after 5 attempts instead of 3 attempts. However, the reason that these messages appear is because of the WAN state transition logic that is part of the failover algorithm. You can interpret the logs in the following way:
	The primary link failure is correctly detected after the 3rd attempt. Thereafter, the algorithm attempts to restart the WAN and checks once again if WAN1 is still down. This results in the 4th failure detection message. If WAN1 is still down, the algorithm starts the secondary link. When the secondary link is up, it is marked as active. Meanwhile, the secondary link has failed again, and this results in the 5th failure detection message. Note that the 5th failure detection and the message suggesting that the secondary link is active have the same time stamp, and so they happen in the same algorithm state-machine cycle. So although it appears that the failover did not occur immediately after 3 failures, internally, the failover process is triggered after the 3rd failure, and the transition to the secondary link is completed by the 5th failure. The primary link is also restarted every 3 failures until it is functional again. In these logs, the primary link was restarted after the 6th failure, that is, 3 failures after the failover process was triggered.
Recommended Action	Check the WAN settings and WAN failure detection method configured for the primary link.

Load Balancing Mode

When the WAN mode is configured for load balancing, both the WAN ports are active simultaneously and the traffic is balanced between them. If one WAN link goes down, all the traffic is diverted to the WAN link that is active.

This section describes the logs that are generated when the WAN mode is set to load balancing.

Table 158. System logs: WAN status, load balancing

Message 1 Message 2 Message 3 Message 4	Dec 1 12:11:27 [UTM] [wand] [LBFO] Restarting WAN1_ Dec 1 12:11:31 [UTM] [wand] [LBFO] Restarting WAN2_ Dec 1 12:11:35 [UTM] [wand] [LBFO] WAN1(UP), WAN2(UP)_ Dec 1 12:24:12 [UTM] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_ Dec 1 12:29:43 [UTM] [wand] [LBFO] Restarting WAN2_ Dec 1 12:29:47 [UTM] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_
Explanation	Message 1 and Message 2 indicate that both the WANs are restarted. Message 3: This message shows that both the WANs are up and the traffic is balanced between the two WAN interfaces. Message 4: This message shows that one of the WAN links is down. At this point, all the traffic is directed through the WAN that is up.
Recommended Action	None.

PPP Logs

This section describes the WAN PPP connection logs. The PPP type can be configured through the web management interface. For more information, see *Manually Configure the Internet Connection* on page 71.

- PPPoE Idle Timeout logs

Table 159. System logs: WAN status, PPPoE idle timeout

Message 1	Nov 29 13:12:46 [UTM] [pppd] Starting connection
Message 2	Nov 29 13:12:49 [UTM] [pppd] Remote message: Success
Message 3	Nov 29 13:12:49 [UTM] [pppd] PAP authentication succeeded
Message 4	Nov 29 13:12:49 [UTM] [pppd] local IP address 50.0.0.62
Message 5	Nov 29 13:12:49 [UTM] [pppd] remote IP address 50.0.0.1
Message 6	Nov 29 13:12:49 [UTM] [pppd] primary DNS address 202.153.32.3
Message 7	Nov 29 13:12:49 [UTM] [pppd] secondary DNS address 202.153.32.3
Message 8	Nov 29 11:29:26 [UTM] [pppd] Terminating connection due to lack of activity.
Message 9	Nov 29 11:29:28 [UTM] [pppd] Connect time 8.2 minutes.
Message 10	Nov 29 11:29:28 [UTM] [pppd] Sent 1408 bytes, received 0 bytes.
Message 11	Nov 29 11:29:29 [UTM] [pppd] Connection terminated.

Table 159. System logs: WAN status, PPPoE idle timeout (continued)

Explanation	Message 1: Establishment of the PPPoE connection starts.
	Message 2: A message from the PPPoE server indicating a correct login.
	Message 3: The authentication for PPP succeeds.
	Message 4: The local IP address that is assigned by the server.
	Message 5: The server's side IP address.
	Message 6: The primary DNS server that is configured on a WAN Settings screen.
	Message 7: The secondary DNS server that is configured on a WAN Settings screen.
	Message 8: The PPP link transitions to idle mode. This event occurs when there is no traffic from the LAN network.
	Message 9: The time in minutes that the link was up.
	Message 10: Data sent and received at the LAN side while the link was up.
	Message 11: The PPP connection terminates after the idle timeout.
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPTP Idle-Timeout logs

Table 160. System logs: WAN status, PPTP idle timeout

Message 1	Nov 29 11:19:02 [UTM] [pppd] Starting connection
Message 2	Nov 29 11:19:05 [UTM] [pppd] CHAP authentication succeeded
Message 3	Nov 29 11:19:05 [UTM] [pppd] local IP address 192.168.200.214
Message 4	Nov 29 11:19:05 [UTM] [pppd] remote IP address 192.168.200.1
Message 5	Nov 29 11:19:05 [UTM] [pppd] primary DNS address 202.153.32.2
Message 6	Nov 29 11:19:05 [UTM] [pppd] secondary DNS address 202.153.32.2
Message 7	Nov 29 11:20:45 [UTM] [pppd] No response to 10 echo-requests
	Nov 29 11:20:45 [UTM] [pppd] Serial link appears to be disconnected.
	Nov 29 11:20:45 [UTM] [pppd] Connect time 1.7 minutes.
Message 8	Nov 29 11:20:45 [UTM] [pppd] Sent 520 bytes, received 80 bytes.
Message 9	Nov 29 11:20:51 [UTM] [pppd] Connection terminated.
Explanation	Message 1: The PPP connection process starts.
	Message 2: A message from the server indicating authentication success.
	Message 3: The local IP address that is assigned by the server.
	Message 4: The server's side IP address.
	Message 5: The primary DNS address that is configured on a WAN Settings screen.
	Message 6: The secondary DNS address that is configured on a WAN Settings screen.
	Message 7: An idle link is detected.
	Message 8: Data sent and received at the LAN side while the link was up.
	Message 9: The PPP connection terminates after the idle timeout.
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPP Authentication logs

Table 161. System logs: WAN status, PPP authentication

Message 1 Message 2 Message 3 Message 4	Nov 29 11:29:26 [UTM] [pppd] Starting link Nov 29 11:29:29 [UTM] [pppd] Remote message: Login incorrect Nov 29 11:29:29 [UTM] [pppd] PAP authentication failed Nov 29 11:29:29 [UTM] [pppd] Connection terminated. WAN2(DOWN)_
Explanation	Message 1: The PPPoE connection process starts. Message 2: The PPPoE server indicates that the login is incorrect. Message 3: The PPP authentication fails because of incorrect login. Message 4: The PPP connection terminates.
Recommended Action	If authentication fails, verify the correct login name and password, and then enter the correct information.

Traffic Metering Logs

This section describes logs that are generated when the traffic meter has reached a limit.

Table 162. System logs: traffic metering

Message	Jan 23 19:03:44 [TRAFFIC_METER] TRAFFIC_METER: Monthly Limit of 10 MB has reached for WAN1._
Explanation	Logs that are generated when the traffic limit for WAN1 interface that was set at 10 MB has been reached. Depending on the setting that is configured in the When Limit is reached section on the WAN1 Traffic Meter screen (see *Enable the WAN Traffic Meter* on page 419), all the incoming and outgoing traffic might be stopped. **Note:** For WAN2 interface, see the settings on the WAN2 Traffic Meter screen.
Recommended Action	To start the traffic, restart the traffic counter in the Traffic Counter section on the WAN1 Traffic Meter screen. **Note:** For WAN2 interface, see the settings on the WAN2 Traffic Meter screen.

Unicast, Multicast, and Broadcast Logs

This section describes logs that are generated when the UTM processes unicast packets.

Table 163. System logs: unicast

Message	Nov 24 11:52:55 [UTM] [kernel] UCAST IN=SELF OUT=WAN SRC=192.168.10.1 DST=192.168.10.10 PROTO=UDP SPT=800 DPT=2049
Explanation	• This unicast packet is sent to the device from the WAN network. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

ICMP Redirect Logs

This section describes logs that are generated when the UTM processes ICMP redirect messages.

Table 164. System logs: unicast, redirect

Message	Feb 2007 22 14:36:07 [UTM] [kernel] [LOG_PACKET] SRC=192.168.1.49 DST=192.168.1.124 PROTO=ICMP TYPE=5 CODE=1
Explanation	• This packet is an ICMP redirect message sent to the device by another device. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

Multicast/Broadcast Logs

This section describes logs that are generated when the UTM processes multicast and broadcast packets.

Table 165. System logs: multicast/broadcast

Message	Jan 1 07:24:13 [UTM] [kernel] MCAST-BCAST IN=WAN OUT=SELF SRC=192.168.1.73 DST=192.168.1.255 PROTO=UDP SPT=138 DPT=138
Explanation	• The multicast or broadcast packet is sent to the device from the WAN network. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

Invalid Packet Logging

This section describes logs that are generated when the UTM processes invalid packets.

Table 166. System logs: invalid packets

Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID] [NO_CONNTRACK_ENTRY] [DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	No connection tracking entry exists.
Recommended Action	None.
Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][RST_PACKET][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Invalid RST packet.
Recommended Action	None.

Table 166. System logs: invalid packets (continued)

Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][ICMP_TYPE][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=ICMP TYPE=19 CODE=0
Explanation	Invalid ICMP type.
Recommended Action	None.
Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][TCP_FLAG_COMBINATION][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Invalid TCP flag combination.
Recommended Action	None.
Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][BAD_CHECKSUM]DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Bad checksum.
Recommended Action	None.
Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][BAD_HW_CHECKSUM][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=ICMP TYPE=3 CODE=0
Explanation	Bad hardware checksum for ICMP packets.
Recommended Action	None.
Message	[INVALID][MALFORMED_PACKET][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Malformed packet.
Recommended Action	None.
Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][SHORT_PACKET][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Short packet.
Recommended Action	None.
Message	[INVALID][INVALID_STATE][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Packet with invalid state.
Recommended Action	None.

Table 166. System logs: invalid packets (continued)

Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][REOPEN_CLOSE_CONN][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Attempt to reopen or close a session.
Recommended Action	None.
Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][OUT_OF_WINDOW][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Packet not in TCP window.
Recommended Action	None.
Message	2007 Oct 1 00:44:17 [UTM] [kernel] [INVALID][ERR_HELPER_ROUTINE][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Error returned from helper routine.
Recommended Action	None.

Content-Filtering and Security Logs

This section describes the log messages that are generated by the content-filtering and security mechanisms.

Web Filtering and Content-Filtering Logs

This section describes logs that are generated when the UTM filters web content.

Table 167. Content-filtering and security logs: web filtering and content filtering

Message	2009-08-01 00:00:01 HTTP ldap_domain ldap_user 192.168.1.3 192.168.35.165 http://192.168.35.165/testcases/files/virus/normal/%b4%f3%d3%da2048.rar SizeLimit Block
Explanation	Logs that are generated when web content is blocked because the allowed size limit is exceeded. The message shows the date and time, protocol, domain, user, client IP address, server IP address, URL, reason for the action, and the action that is taken.
Recommended Action	None.

Table 167. Content-filtering and security logs: web filtering and content filtering (continued)

Message	2009-08-01 00:00:01 HTTP ldap_domain ldap_user 192.168.1.3 192.168.35.165 http://192.168.35.165/testcases/files/virus/normal/%b4%f3%d3%da2048.rar URL Block
Explanation	Logs that are generated when web content is blocked because an access violation of a blocked web category occurs. The message shows the date and time, protocol, domain, user, client IP address, server IP address, URL, reason for the action, and the action that is taken.
Recommended Action	None.
Message	2009-08-01 00:00:01 HTTP ldap_domain ldap_user 192.168.1.3 192.168.35.165 http://192.168.35.165/testcases/files/virus/normal/%b4%f3%d3%da2048.rar FileType Block
Explanation	Logs that are generated when web content is blocked because an access violation of a blocked web file extension occurs. The message shows the date and time, protocol, domain, user, client IP address, server IP address, URL, reason for the action, and the action that is taken.
Recommended Action	None.
Message	2009-08-01 00:00:01 HTTP ldap_domain ldap_user 192.168.1.3 192.168.35.165 http://192.168.35.165/testcases/files/virus/normal/%b4%f3%d3%da2048.rar Proxy Block
Explanation	Logs that are generated when web content is blocked because of a proxy violation. The message shows the date and time, protocol, domain, user, client IP address, server IP address, URL, reason for the action, and the action that is taken.
Recommended Action	None.
Message	2009-08-01 00:00:01 HTTP ldap_domain ldap_user 192.168.1.3 192.168.35.165 http://192.168.35.165/testcases/files/virus/normal/%b4%f3%d3%da2048.rar Keyword Block
Explanation	Logs that are generated when web content is blocked because of a keyword violation. The message shows the date and time, protocol, domain, user, client IP address, server IP address, URL, reason for the action, and the action that is taken.
Recommended Action	None.

Spam Logs

This section describes logs that are generated when the UTM filters spam email messages.

Table 168. Content-filtering and security logs: spam

Message	2009-02-28 23:59:59 SMTP radius_domain radius_user1 192.168.1.2 192.168.35.165 xlzimap@test.com xlzpop3@test.com Blocked by list.dsbl.org 0 RBL Block
Explanation	Logs that are generated when spam messages are blocked by the RBL. The message shows the date and time, protocol, domain, user, client IP address, server IP address, sender, recipient, subject line, size, mechanism that detected the spam, and the action that is taken.
Recommended Action	None.
Message	2009-02-28 23:59:59 SMTP radius_domain radius_user1 192.168.1.2 192.168.35.165 xlzimap@test.com xlzpop3@test.com Blocked by customized blacklist 0 Heuristic Block
Explanation	Logs that are generated when spam messages are blocked by the blacklist. The message shows the date and time, protocol, domain, user, client IP address, server IP address, sender, recipient, subject line, size, mechanism that detected the spam, and the action that is taken.
Recommended Action	None.
Message	2009-02-28 23:59:59 SMTP radius_domain radius_user1 192.168.1.2 192.168.35.165 xlzimap@test.com xlzpop3@test.com Blocked by customized blacklist 58882 Distributed Spam Analysis Block
Explanation	Logs that are generated when spam messages are blocked by distributed spam analysis. The message shows the date and time, protocol, protocol, domain, client IP address, server IP address, sender, recipient, subject line, size, mechanism that detected the spam, and the action that is taken.
Recommended Action	None.

Traffic Logs

This section describes logs that are generated when the UTM processes web and email traffic.

Table 169. Content-filtering and security logs: traffic

Message	2009-02-28 23:59:59 HTTP 99 radius_domain radius_user1 192.168.1.2 192.168.33.8 xlzimap@test.com xlzpop3@test.com [MALWARE INFECTED] Fw: cleanvirus
Explanation	Web and email traffic logs for HTTP, SMTP, POP3, IMAP, HTTPS, and FTP traffic. In this sample message, a malware threat was cleaned from the traffic. The message shows the date and time, protocol, size of the web file or email, domain, user, client IP address, server IP address, sender, recipient, and web URL or email subject line.
Recommended Action	None.

Virus Logs

This section describes logs that are generated when the UTM detects viruses.

Table 170. Content-filtering and security logs: virus

Message	2008-02-29 23:59:00 POP3 OF97/Jerk Delete cleanvirus.zip radius_domain radius_user1 192.168.1.2 192.168.35.166 xlzimap@test.com xlzimap@test.com [MALWARE INFECTED] Fw: cleanvirus
Explanation	Virus logs for all services. The message shows the date and time, protocol, virus name, the action that is taken, file name, domain, user, client IP address, server IP address, sender, recipient, and web URL or email subject line.
Recommended Action	None.

Email Filter Logs

This section describes logs that are generated when the UTM filters email content.

Table 171. Content-filtering and security logs: email filter

Message	2009-04-31 23:59:59 SMTP radius_domain radius_user1 192.168.1.2 192.168.35.165 xlzimap@test.com xlzpop3@test.com test Keyword test BlockMail
Explanation	Logs that are generated when emails are blocked because of a keyword violation in the subject line. The message shows the date and time, protocol, domain, user, client IP address, server IP address, sender, recipient, email subject line, reason for the action, details, and the action that is taken.
Recommended Action	None.

IPS Logs

This section describes logs that are generated when traffic matches IPS rules.

Table 172. Content-filtering and security logs: IPS

Message	2008-12-31 23:59:37 drop TCP 192.168.1.2 3496 192.168.35.165 8081 WEB-CGI Trend Micro OfficeScan CGI password decryption buffer overflow attempt
Explanation	Logs that are generated when traffic matches IPS rules. The message shows the date and time, the action that is taken, protocol, client IP address, client port number, server IP address, server port number, IPS category, and reason for the action.
Recommended Action	None.

Port Scan Logs

This section describes logs that are generated when ports are scanned.

Table 173. Content-filtering and security logs: port scan

Message	2008-12-31 23:59:12 192.168.1.10 192.168.35.160 5 10 1 18:188 UDP Portscan
Explanation	Logs that are generated when port scans are detected. The message shows the date and time, client IP address, server IP address, connection number, IP number, port number, port range, and details.
Recommended Action	None.

Application Logs

This section describes logs that are generated when the UTM filters application traffic.

Table 174. Content-filtering and security logs: applications

Message	2008-12-31 23:59:31 0 block 1 8800115 2 TCP 192.168.1.2 543 65.54.239.210 1863 MSN login attempt
Explanation	Logs that are generated when an IM/P2P traffic violation occurs. The message shows the date and time, the action that is taken, protocol, client IP address, client port number, server IP address, server port number, IM/P2P category, and reason for the action.
Recommended Action	None.

Routing Logs

This section explains the logging messages for each network segment such as LAN-to-WAN for debugging purposes. These logs might generate a significant volume of messages.

LAN-to-WAN Logs

This section describes logs that are generated when the UTM processes LAN-to-WAN traffic.

Table 175. Routing logs: LAN to WAN

Message	Nov 29 09:19:43 [UTM] [kernel] LAN2WAN[ACCEPT] IN=LAN OUT=WAN SRC= 192.168.10.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from the LAN to the WAN has been allowed by the firewall. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

LAN-to-DMZ Logs

This section describes logs that are generated when the UTM processes LAN-to-DMZ traffic.

Table 176. Routing logs: LAN to DMZ

Message	Nov 29 09:44:06 [UTM] [kernel] LAN2DMZ[ACCEPT] IN=LAN OUT=DMZ SRC= 192.168.10.10 DST=192.168.20.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from the LAN to the DMZ has been allowed by the firewall. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

DMZ-to-WAN Logs

This section describes logs that are generated when the UTM processes DMZ-to-WAN traffic.

Table 177. Routing logs: DMZ to WAN

Message	Nov 29 09:19:43 [UTM] [kernel] DMZ2WAN[DROP] IN=DMZ OUT=WAN SRC= 192.168.20.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from the DMZ to the WAN has been dropped by the firewall. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

WAN-to-LAN Logs

This section describes logs that are generated when the UTM processes WAN-to-LAN traffic.

Table 178. Routing logs: WAN to LAN

Message	Nov 29 10:05:15 [UTM] [kernel] WAN2LAN[ACCEPT] IN=WAN OUT=LAN SRC= 192.168.1.214 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from the LAN to the WAN has been allowed by the firewall. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

DMZ-to-LAN Logs

This section describes logs that are generated when the UTM processes DMZ-to-LAN traffic.

Table 179. Routing logs: DMZ to WAN

Message	Nov 29 09:44:06 [UTM] [kernel] DMZ2LAN[DROP] IN=DMZ OUT=LAN SRC= 192.168.20.10 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from the DMZ to the LAN has been dropped by the firewall. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

WAN-to-DMZ Logs

This section describes logs that are generated when the UTM processes WAN-to-DMZ traffic.

Table 180. Routing logs: WAN to DMZ

Message	Nov 29 09:19:43 [UTM] [kernel] WAN2DMZ[ACCEPT] IN=WAN OUT=DMZ SRC= 192.168.1.214 DST=192.168.20.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from the WAN to the DMZ has been allowed by the firewall. • For other settings, see *Table 149* on page 582.
Recommended Action	None.

Default Settings and Technical Specifications

<div align="right">

G

</div>

This appendix provides the default settings and the physical and technical specifications of the UTM in the following sections:

- *Default Settings*
- *Physical and Technical Specifications*

Default Settings

You can use the factory default reset button located on the rear panel to reset all settings to their factory defaults. This is called a hard reset (for more information, see *Revert to Factory Default Settings* on page 405):

- To perform a hard reset, press and hold the factory default reset button for approximately 8 seconds (until the Test LED blinks rapidly). The UTM returns to the factory configuration settings that are shown in the following table.

- Pressing the factory default reset button for a shorter period of time simply causes the UTM to reboot.

The following table shows the default configuration settings for the UTM:

Table 181. UTM default configuration settings

Feature		Default behavior
Router login		
	User login URL	https://192.168.1.1
	Administrator user name (case-sensitive)	admin
	Administrator login password (case-sensitive)	password
	Guest user name (case-sensitive)	guest
	Guest login password (case-sensitive)	password

Table 181. UTM default configuration settings (continued)

Feature		Default behavior
Internet connection		
	WAN MAC address	Use default address
	WAN MTU size	1500
	Port speed	AutoSense
Local network (LAN)		
	LAN IP address	192.168.1.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	Disabled
	DHCP server	Enabled
	DHCP starting IP address	192.168.1.2
	DHCP starting IP address	192.168.1.100
Management		
	Time zone	GMT
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
	Remote management	HTTPS enabled CLI disabled
Firewall		
	Inbound (communications coming in from the Internet)	All communication denied
	Outbound (communications from the LAN to the Internet)	All communication allowed
	Source MAC filtering	Disabled
	Stealth mode	Enabled
	Respond to ping on Internet ports	Disabled

Physical and Technical Specifications

The following table shows the physical and technical specifications for the UTM:

Table 182. UTM physical and technical specifications

Feature			Specification
Network protocol and standards compatibility			
	Data and Routing Protocols		TCP/IP, RIP-1, RIP-2, DHCP, PPPoA (UTM9S only), PPPoE, PPTP
Power adapter			
	UTM5, UTM10, and UTM25		100–240V, AC/50–60 Hz, Universal Input, 1.2 Amp Max
	UTM9S, UTM50, and UTM150		100–240V, AC/50–60 Hz, Universal Input, 1.0 Amp Max
Dimensions and weight			
	Dimensions (W x H x D)	UTM5, UTM10, and UTM25	33 x 4.3 x 20.9 cm
			13 x 1.7 x 8.2 inches
		UTM50 and UTM150	44 x 4.3 x 25.3 cm
			17.3 x 1.7 x 9.96 inches
		UTM9S	44 x 4.3 x 28.5 cm
			17.3 x 1.7 x 11.25 inches
	Weight	UTM5, UTM10, and UTM25	2.1 kg
			4.6 lb
		UTM50 and UTM150	2.9 kg
			6.4 lb
		UTM9S	2.56 kg
			5.65 lb
Environmental specifications			
	Operating temperatures		0º to 45ºC
			32º to 113ºF
	Storage temperatures		–20º to 70ºC
			–4º to 158ºF
	Operating humidity		90% maximum relative humidity, noncondensing
	Storage humidity		95% maximum relative humidity, noncondensing

Table 182. UTM physical and technical specifications (continued)

Feature			Specification
Major regulatory compliance			
	Meets requirements of		FCC Class A
			CE
			WEEE
			RoHS
Interface specifications			
	LAN	UTM5, UTM9S, UTM10, UTM25, and UTM150	4 LAN autosensing 10/100/1000BASE-T, RJ-45, one of which is a configurable DMZ interface
		UTM50	6 LAN autosensing 10/100/1000BASE-T, RJ-45, one of which is a configurable DMZ interface
	WAN	Single WAN port models	1 WAN autosensing 10/100/1000BASE-T, RJ-45
		Multiple WAN port models	2 or 4 WAN autosensing 10/100/1000BASE-T, RJ-45
	1 administrative console port		RS-232
	1 USB		nonfunctioning, included for future management enhancements

The following table shows the IPSec VPN specifications for the UTM:

Table 183. UTM IPSec VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	The number of supported site-to-site IPSec VPN tunnels depends on the model (see *Table 1* on page 19).
IPSec encryption algorithm	DES, 3DES, AES-128, AES-192, AES-256
IPSec authentication algorithm	SHA-1, MD5
IPSec key exchange	IKE, manual key, pre-shared key, PKI, X.500
IPSec authentication types	Local user database, RADIUS PAP, RADIUS CHAP
IPSec certificates supported	CA certificate, self-signed certificate

The following table shows the SSL VPN specifications for the UTM:

Table 184. UTM SSL VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	The number of supported dedicated SSL VPN tunnels depends on the model (see NETGEAR's documentation at *http://prosecure.netgear.com*).
SSL versions	SSLv3, TLS1.0
SSL encryption algorithm	DES, 3DES, ARC4, AES-128, AES-192, AES-256
SSL message integrity	MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1
SSL authentication types	Local user database, RADIUS-PAP, RADIUS-CHAP, RADIUS-MSCHAP, RADIUS-MSCHAPv2, WiKID-PAP, WiKID-CHAP, MIAS-PAP, MIAS-CHAP, NT domain
SSL certificates supported	CA certificate, self-signed certificate

The following table shows the wireless specifications for the UTM9S wireless module:

Table 185. Wireless specifications UTM9S wireless module

Feature	Description
802.11b/bg/ng wireless specifications	
802.11bg data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps, and autorate capable
802.11ng data rates (including Greenfield)	Channels with data rates for a 20-MHz channel spacing (width): 0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps, 5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps, 10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 130 Mbps, 15 / 144.44 Mbps, and autorate capable
	Channels with data rates for a 40-MHz channel spacing (width): 0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, and autorate capable
802.11b/bg/ng operating frequencies	• 2.412–2.462 GHz (US) • 2.457–2.462 GHz (Spain) • 2.410–2.484 GHz (Japan 11b) • 2.410–2.472 GHz (Japan 11ng) • 2.457–2.472 GHz (France) • 2.412–2.472 GHz (Europe ETSI) • 2.412–2.472 GHz (China)
802.11 b/bg/ng encryption	• 64-bit, 128-bit, and 256-bit WEP • AES • TKIP

Table 185. Wireless specifications UTM9S wireless module (continued)

Feature	Description
802.11a/na wireless specifications	
802.11a data rates	6, 9, 12, 18, 24, 36, 48, 54 Mbps, and autorate capable
802.11na data rates (includes Greenfield)	Channels with data rates for a 20-MHz channel spacing (width): 0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps, 5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps, 10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 130 Mbps, 15 / 144.44 Mbps, and autorate capable
	Channels with data rates for a 40-MHz channel spacing (width): 0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, and autorate capable
802.11a/na Operating Frequencies	• 5.180–5.240 GHz (US, lower frequencies) • 5.260–5.320 GHz (US, middle frequencies) • 5.180–5240 GHz (CE [EU], lower frequencies) • 5.260–5.320 GHz (CE [EU], middle frequencies) • 5.500–5.680 GHz (CE [EU], upper frequencies)
802.11 a/na encryption	• 64-bit, 128-bit, and 256-bit WEP • AES • TKIP

Note: For default email and web scan settings, see *Table 38* on page 176.

Notification of Compliance (Wired)

H

NETGEAR Wired Products

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSecure Unified Threat Management (UTM) Appliance complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

*   Reorient or relocate the receiving antenna.
*   Increase the separation between the equipment and the receiver.
*   Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
*   Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, ProSecure Unified Threat Management (UTM) Appliance, does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

European Union

The ProSecure Unified Threat Management (UTM) Appliance complies with essential requirements of EU EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC as supported by applying the following test methods and standards:

*   EN55022: 2006 / A1: 2007
*   EN55024: 1998 / A1: 2001 / A2 : 2003
*   EN60950-1: 2005 2nd Edition
*   EN 61000-3-2:2006
*   EN 61000-3-3:1995 w/A1: 2001+A2: 2005

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to *ftp://downloads.netgear.com/files/GPLnotice.pdf*.

For GNU General Public License (GPL) related information, please visit *http://support.netgear.com/app/answers/detail/a_id/2649*.

Additional Copyrights

AES	Copyright (c) 2001, Dr. Brian Gladman, brg@gladman.uk.net, Worcester, UK. All rights reserved. TERMS Redistribution and use in source and binary forms, with or without modification, are permitted 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. 3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission. This software is provided "as is" with no express or implied warranties of correctness or fitness for purpose.
Open SSL	Copyright (c) 1998–2000 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: 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 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, 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).

MD5	Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.
	License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.
	RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.
	These notices must be retained in any copies of any part of this documentation and/or software.
PPP	Copyright (c) 1989 Carnegie Mellon University. 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 Carnegie Mellon University. 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 MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Zlib	zlib.h. Interface of the zlib general purpose compression library version 1.1.4, March 11th, 2002. Copyright (C) 1995–2002 Jean-loup Gailly and Mark Adler.
	This software is provided "as is," without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:
	1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
	2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
	3. This notice may not be removed or altered from any source distribution.
	Jean-loup Gailly: jloup@gzip.org; Mark Adler: madler@alumni.caltech.edu.
	The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files rfc1950.txt (zlib format), rfc1951.txt (deflate format), and rfc1952.txt (gzip format). For more information, see *http://www.ietf.org/rfc/*.

Notification of Compliance (Wireless)

NETGEAR Wireless Routers, Gateways, APs

I

Regulatory Compliance Information

Note: This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

$C \in \textcircled{!}$

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328 (2.4 GHz), EN301 489-17 EN60950-1

For complete DoC, visit the NETGEAR EU Declarations of Conformity website at:
http://support.netgear.com/app/answers/detail/a_id/11621/

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSecure Unified Threat Management (UTM) Appliance complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

• This device may not cause harmful interference, and
• This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

• Reorient or relocate the receiving antenna.
• Increase the separation between the equipment and the receiver.
• Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
• Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

• Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
• This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (ProSecure Unified Threat Management (UTM) Appliance) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to
ftp://downloads.netgear.com/files/GPLnotice.pdf.

For GNU General Public License (GPL) related information, please visit
http://support.netgear.com/app/answers/detail/a_id/2649.

Interference Reduction Table

The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters

Household Appliance	Recommended Minimum Distance (in feet and meters)
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Index