ProSecure Unified Threat Management (UTM) Appliance Reference Manual

PROSECURE™
SECURITY ARCHITECTURE BY NETGEAR®

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134

202-10482-02
January 2010
v1.0

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks and ProSecure and ProSafe are trademarks of NETGEAR, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving 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.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by NETGEAR could void the user's authority to operate the equipment.

EU Regulatory Compliance Statement

The ProSecure Unified Threat Management (UTM) Appliance is compliant with the following EU Council Directives: EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC. Compliance is verified by testing to the following standards: EN55022, EN55024, and EN60950-1.

For the EU Declaration of Conformity, please visit:
http://kb.netgear.com/app/answers/detail/a_id/11621/sno/0.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSecure Unified Threat Management (UTM) Appliance gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSecure Unified Threat Management (UTM) Appliance has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

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 *ftp://ds.internic.net/rfc/rfc1950.txt* (zlib format), rfc1951.txt (deflate format), and rfc1952.txt (gzip format).

Product and Publication Details

Model Number:	UTM
Publication Date:	January 2010
Product Family:	UTM
Product Name:	ProSecure Unified Threat Management (UTM) Appliance
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10482-02
Publication Version Number	1.0

Contents

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

Chapter 3
Manually Configuring Internet and WAN Settings

About This Manual

The *NETGEAR® ProSecure™ Unified Threat Management (UTM) Appliance Reference Manual* describes how to install, configure, and troubleshoot a ProSecure Unified Threat Management (UTM) Appliance. The information in this manual is intended for readers with intermediate computer and networking skills.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical conventions**. This manual uses the following typographical conventions:

Italic	Emphasis, books, CDs
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

- **Formats**. This manual uses the following formats to highlight special messages:

	**Note:** This format is used to highlight information of importance or special interest.
	**Tip:** This format is used to highlight a procedure that will save time or resources.
	**Warning:** Ignoring this type of note might result in a malfunction or damage to the equipment.
	**Danger:** This is a safety warning. Failure to take heed of this notice might result in personal injury or death.

- **Scope**. This manual is written for the UTM according to these specifications:

Product Version	ProSecure Unified Threat Management (UTM) Appliance
Manual Publication Date	January 2010

For more information about network, Internet, firewall, and VPN technologies, click the links to the NETGEAR Website in Appendix E, "Related Documents."

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

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

How to Print This Manual

To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Date	Description
202-10482-01	1.0	September 2009	Initial publication of this reference manual.
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).

Chapter 1
Introduction

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

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 or DSL modems. Dual wide area network (WAN) ports allow you to increase effective throughput 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 dual-WAN port models, dual 10/100/1000 Mbps Gigabit Ethernet WAN ports for load balancing or failover protection of your Internet connection, providing increased system reliability or increased throughput.
- Built-in four-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for extremely fast data transfer between local network resources.
- Advanced IPsec VPN and SSL VPN support.
- Depending on the model, bundled with a 1-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 anti-spam 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.

Dual-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 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 "Network Planning for Dual WAN Ports (Dual-WAN Port Models Only)" on page B-1 for the planning factors to consider when implementing the following capabilities with dual WAN port gateways:

- Single or multiple exposed hosts.
- Virtual private networks.

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 1-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 pre-installed 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.
  - Browser based, platform-independent, remote access through a number of popular browsers, such as Microsoft Internet Explorer, Mozilla Firefox, or Apple Safari.
  - Provides granular access to corporate resources based upon user type or group membership.

A Powerful, True Firewall

Unlike simple Internet sharing 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 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 e-mail 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 normally 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 De-Militarized Zone (DMZ) port to forward the traffic to one PC on your network.

Autosensing Ethernet Connections with Auto Uplink

With its internal 4-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 to the correct configuration. This feature eliminates the need 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 B-3. 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 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 your firewall from almost any type of personal computer, 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.
- **Auto detection 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 to easily configure IPsec VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure 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 to easily configure SSL connections over VPN according to the recommendations of the VPNC to ensure 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 UTMl incorporates built-in diagnostic functions such as Ping, Trace Route, DNS lookup, and remote reboot.
- **Remote management**. The UTM allows you to login 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 upgrade.
- Technical support seven days a week, 24 hours a day, according to the terms identified in the Warranty and Support information card provided with your product.

Model Comparison

Table 1-1 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 1-1. Differences Between the UTM Models

Feature	UTM5	UTM10	UTM25
IPsec VPN tunnels			
Number of supported site-to-site IPsec VPN tunnels (from which the model derives its model number)	5	10	25
Hardware			
LAN ports (Gigabit RJ-45)	4	4	4
WAN ports (Gigabit RJ-45)	1	1	2
DMZ Interfaces (configurable)	1	1	1

Table 1-1. Differences Between the UTM Models (continued)

Feature	UTM5	UTM10	UTM25
USB ports	1	1	1
Console ports (RS232)	1	1	1
Flash Memory/RAM	2 GB/512 MB	2 GB/512 MB	2 GB/1 GB
Deployment			
VLAN Support	Yes	Yes	Yes
Dual-WAN auto-rollover mode	No	No	Yes
Dual-WAN load balancing mode	No	No	Yes
Single-WAN mode	Yes	Yes	Yes

Service Registration Card with License Keys

Be sure to store the license key card that came with your UTM in a secure location. You do need these keys to activate your product during the initial setup.

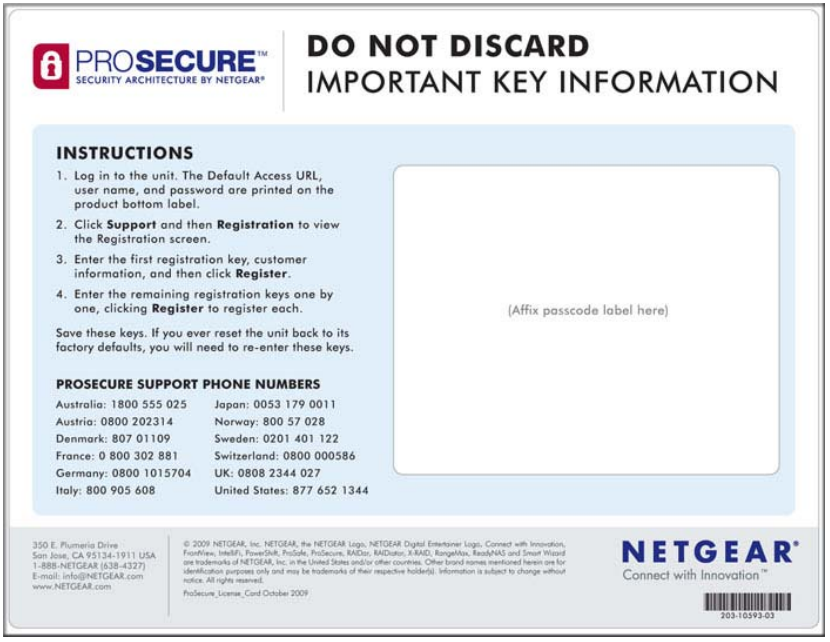


Figure 1-1

Note: When you reset the UTM to the original factory default settings after you have entered the license keys to activate the UTM (see "Registering the UTM with NETGEAR" on page 2-26), 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 re-enter 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).
- Warranty and Support Information Card.

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 label of the UTM are described below.

Front Panel

Viewed from left to right, the UTM front panel contains the following ports (see Figure 1-2 on page 1-10, which shows a dual-WAN port model, the UTM25):

- One non-functioning 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: one (single WAN-port models) or two (dual WAN port models) 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 Table 1-2.

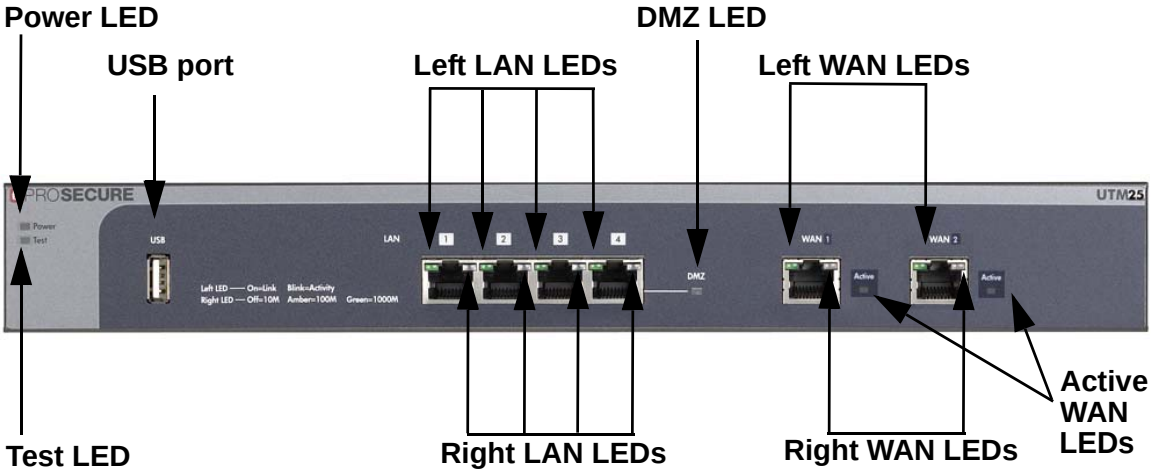


Figure 1-2

Note: Figure 1-2 shows a dual-WAN port model (the UTM25). Single-WAN port models contain the left WAN port that is shown in Figure 1-2 but no right WAN port nor any Active WAN LEDs.

The function of each LED is described in Table 1-2.

Table 1-2. LED Descriptions

Object	Activity	Description
Power	On (Green)	Power is supplied to the UTM.
	Off	Power is not supplied to the UTM.
Test	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)	Writing to flash memory (during upgrading or resetting to defaults).
	Off	The system has booted successfully.
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.
	Blink (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.
	Blink (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.

Table 1-2. LED Descriptions (continued)

Object	Activity	Description
Active LED (dual-WAN port models only)	Off	The WAN port is either not enabled or has no link to the Internet.
	On (Green)	The WAN port has a valid Internet connection.

Rear Panel

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

Figure 1-3

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

1. Cable security lock receptacle.
2. Console port. Port for connecting to an optional console terminal. The ports 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 eight seconds until the front panel Test light flashes to reset the UTM to factory default settings. All configuration settings are lost and the default password is restored.
4. AC power receptacle. Universal AC input (100-240 VAC, 50-60 Hz).

Bottom Panel With Product Label

The product label on the bottom of the UTM's enclosure displays factory default, regulatory compliance, and other information (see Figure 1-4 and Figure 1-5 on page 1-13 and Figure 1-6 on page 1-14).

Figure 1-4 shows the product label for the UTM5.

Figure 1-4

Figure 1-5 shows the product label for the UTM10.

Figure 1-5

Figure 1-6 shows the product label for the UTM25.

Figure 1-6

Choosing a Location for the UTM

The UTM is suitable for use in an office environment where it can be free-standing (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 dual-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 A, “Default Settings and Technical Specifications.”

Using 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 dual-WAN port models). Attach the mounting brackets using the hardware that is supplied with the mounting kit.

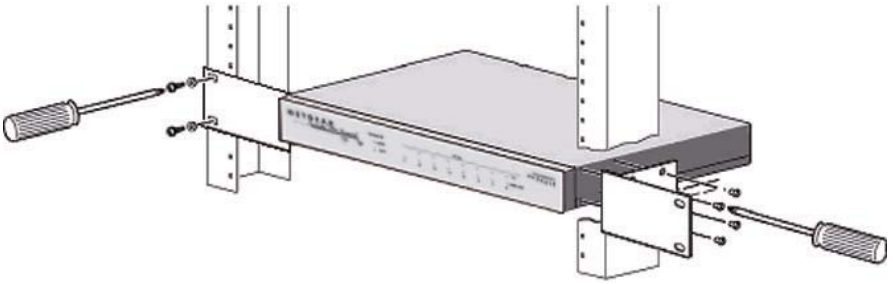


Figure 1-7

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.

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

Understanding the 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 in order 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://prosecure.netgear.com* or *http://kb.netgear.com/app/home*.
2. **Log in to the UTM**. After logging in, you are ready to set up and configure your UTM. See "Logging In to the UTM" on page 2-2.
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 dual-WAN port models only). See "Using the Setup Wizard to Perform the Initial Configuration" on page 2-7.
4. **Verify the installation**. See "Verifying Proper Installation" on page 2-26.
5. **Register the UTM**. "Registering the UTM with NETGEAR" on page 2-26.

Each of these tasks is described separately in this chapter. The configuration of the WAN mode (required for dual-WAN port models only), 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 must use a Web browser such as Microsoft Internet Explorer 6 or higher, Mozilla Firefox 3 or higher, or Apple Safari 3 or higher with JavaScript, cookies, and you must have 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 only required for the SSL VPN portal, not for the Web Management Interface.

Logging In to the UTM

To connect to the UTM, your computer needs to be configured to obtain an IP address automatically from the UTM via DHCP. For instructions on how to configure your computer for DHCP, see the document that you can access from "Preparing Your Network" in Appendix E.

To connect and log in to the UTM:

1. Start any of the qualified Web browsers, as explained in "Qualified Web Browsers" on this page.
2. Enter **https://192.168.1.1** in the address field. The NETGEAR Configuration Manager Login screen displays in the browser (see Figure 2-1 on page 2-3, which shows a dual-WAN port model, the UTM25).

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

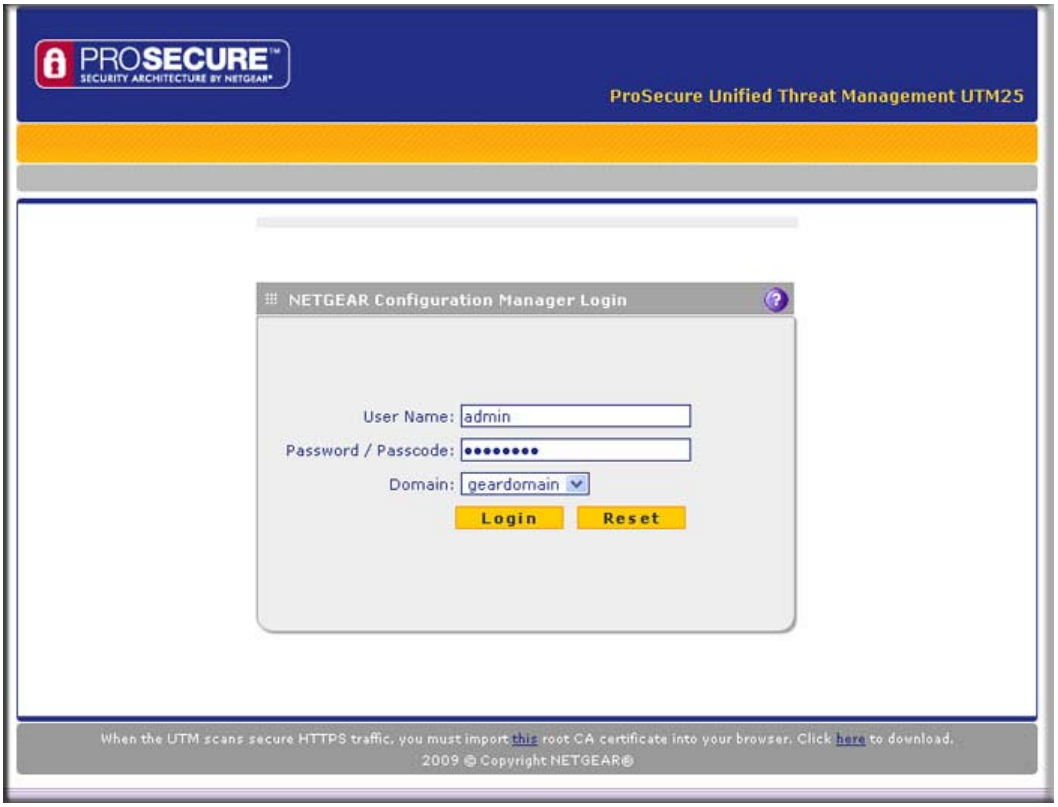


Figure 2-1

	Note: The first time that you remotely connect to the UTM with a browser via an SSL connection, you might get a warning message regarding the SSL certificate. You can follow to directions of your browser to accept the SSL certificate, or you can import the UTM's root certificate by clicking the hyperlink at the he bottom of the NETGEAR Configuration Manager Login screen.

3. In the User field, type **admin**. Use lower case letters.
4. In the Password field, type **password**. Here too, use lower case 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 appears, displaying the System Status screen. (Figure 2-2 on page 2-4 shows the top part of a dual-WAN port model screen. For information about this screen, see "Viewing System Status" on page 11-20).

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

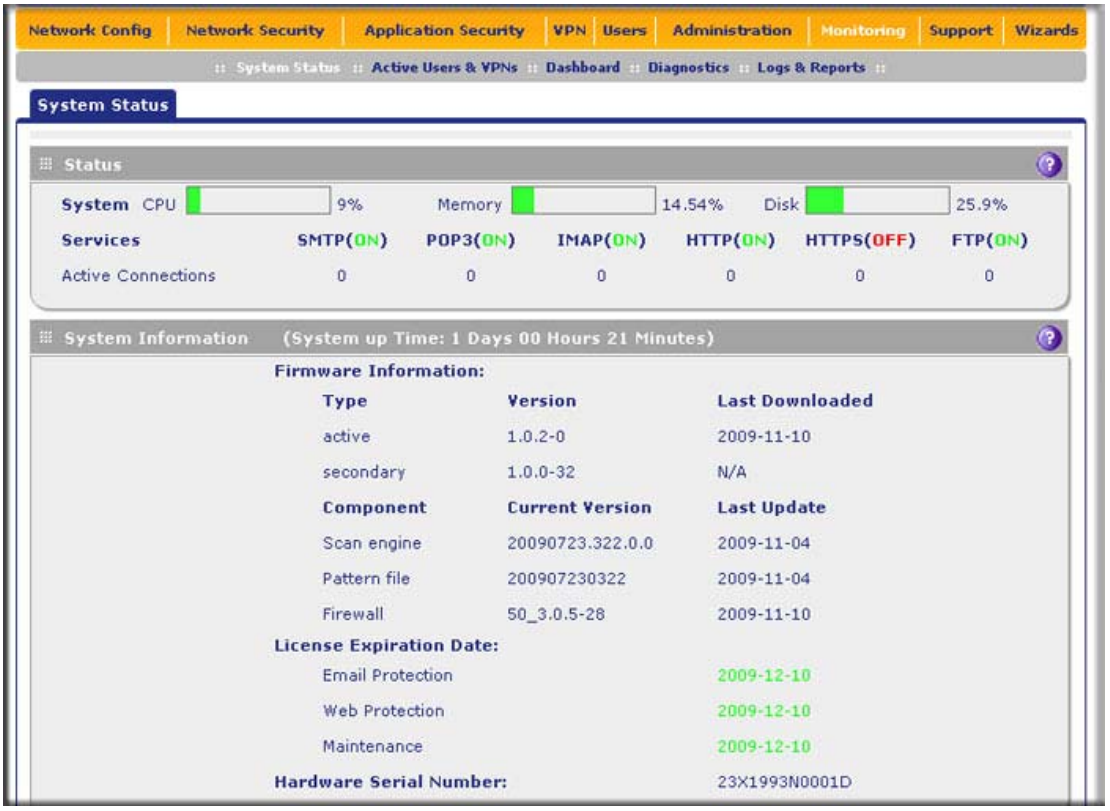


Figure 2-2

Understanding the Web Management Interface Menu Layout

Figure 2-3 shows the menu at the top of a dual-WAN port model's Web Management Interface (in this example, the UTM25). The single-WAN port model's Web Management Interface layout is identical with the exception that it shows only a single WAN ISP Setting submenu tab.

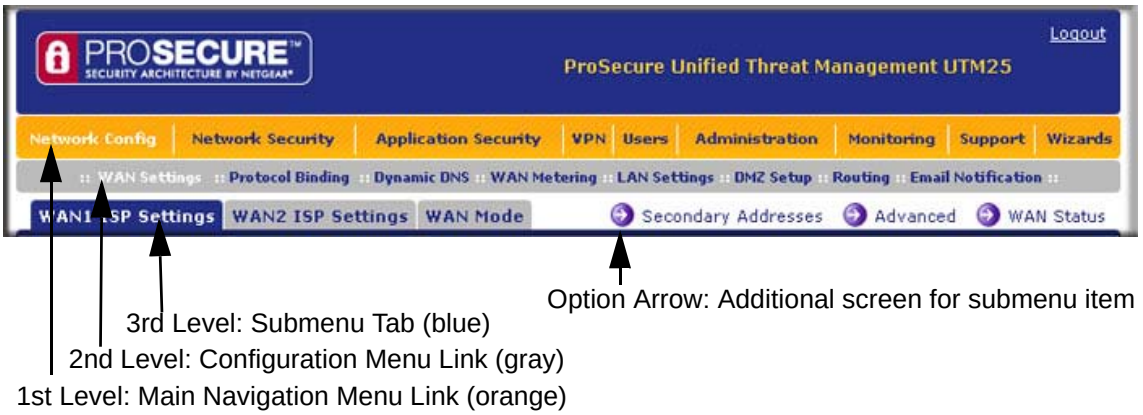


Figure 2-3

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 provide access to all the configuration functions of the UTM, and remain 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 grey background.
- **3rd Level: Submenu tabs**. Each configuration menu item has one or more submenu tabs that are listed below the grey 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, they are displayed 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. Figure 2-4 shows an example.

Figure 2-4

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

- **Apply**. Save and apply the configuration.
- **Reset**. Reset the configuration to default 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 are displayed to let you configure the table entries. The nature of the screen determines which table buttons are shown. Figure 2-5 shows an example.

Figure 2-5

Any of the following table buttons might be displayed 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 up the selected entry in the table.

- **Down**. Move down the selected entry in the table.
- **Apply**. Apply the selected entry.

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

Using the Setup Wizard to Perform the Initial Configuration

The Setup Wizard facilitates the initial configuration of the UTM by taking you through ten 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 2-6

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

The following sections explain the nine 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 section below provides a specific link to a section in another chapters.

Setup Wizard Step 1 of 10: LAN Settings

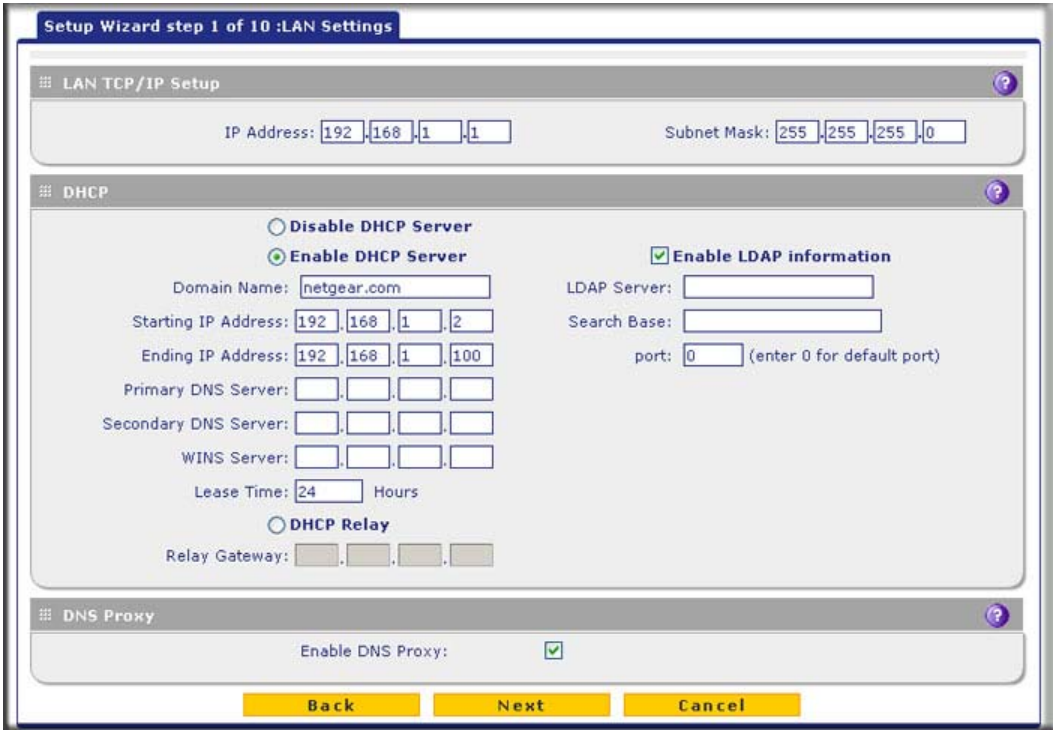


Figure 2-7

Enter the settings as explained in Table 2-1 on page 2-9, 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 "Managing Virtual LANs and DHCP Options" on page 4-1.

	Note: 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 4-4.

Table 2-1. Setup Wizard Step 1: LAN Settings

Setting	Description (or Subfield and Description)	
LAN TCP/IP Setup		
IP Address	Enter the IP address of the UTM's default VLAN (the factory default 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 will be disconnected. You must then 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 must now 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. This is the default setting.	
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 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 (the IP address in LAN TCP/IP section above).

Table 2-1. Setup Wizard Step 1: LAN Settings (continued)

Setting	Description (or Subfield and Description)	
Enable DHCP Server (continued)	Primary DNS Server	This 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 is optional. If an IP address is specified, the UTM provides this address as the secondary DNS server IP address.
	WINS Server	This 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** checkbox to enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information. Enter the settings below. **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 e-mail 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 begin. You can specify multiple search object, 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 zero.

Table 2-1. Setup Wizard Step 1: LAN Settings (continued)

Setting	Description (or Subfield and Description)
DNS Proxy	
Enable DNS Proxy	This 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 setting is enabled by default. **Note**: When you deselect the **Enable DNS Proxy** radio button, the UTM still services DNS requests that are sent to its LAN IP address unless you disable DNS Proxy in the firewall settings (see "Attack Checks" on page 5-27).

Setup Wizard Step 2 of 10: WAN Settings

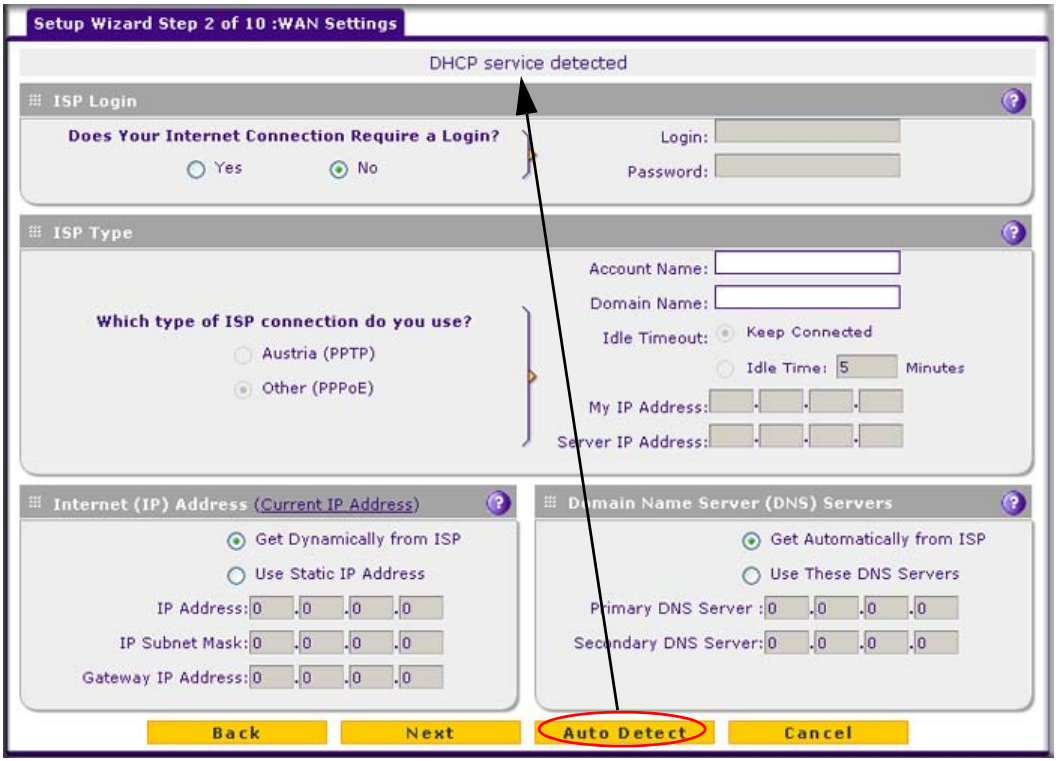


Figure 2-8

Enter the settings as explained in Table 2-2 on page 2-12, then click **Next** to go the following screen.

Note: Click the **Auto Detect** action button at the bottom of the menu. The auto-detect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support.

Note: 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, for a dual-WAN port model, select **WAN1 ISP Settings** or **WAN2 ISP Settings**, and for a single-WAN port model, select **WAN ISP Settings**. For more information about these WAN settings, see "Configuring the Internet Connections" on page 3-2.

Table 2-2. Setup Wizard Step 2: WAN Settings

Setting	Description (or Subfield and 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 below. If you select Yes, 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 must log in. Select the **Yes** radio button. Based on the connection that you select, the text box fields that require data entry are highlighted. If your ISP has not assigned any login information, then select the **No** radio box and skip this section. If you select Yes, 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 entering your full e-mail address here.
	Domain Name	Your domain name or workgroup name assigned by your ISP, or your ISP's domain name. You may leave this field blank.

Table 2-2. Setup Wizard Step 2: WAN Settings (continued)

Setting	Description (or Subfield and Description)	
Austria (PPTP) (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 Time** radio button and, in the timeout 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 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 may 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 Time** radio button and, in the timeout 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
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.	
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.
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.	

Table 2-2. Setup Wizard Step 2: WAN Settings (continued)

Setting	Description (or Subfield and Description)	
Use These DNS Servers	If your ISP has assigned DNS addresses, select the **Use these DNS Servers** radio button. Ensure 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.

Setup Wizard Step 3 of 10: System Date and Time

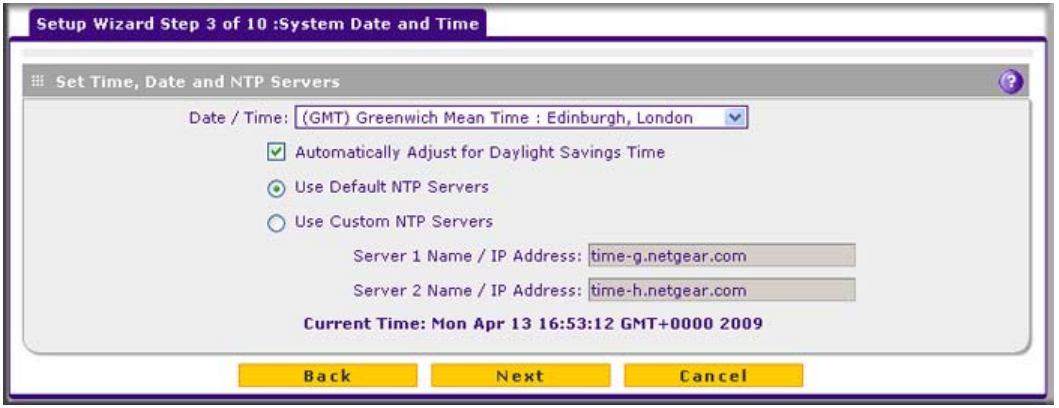


Figure 2-9

Enter the settings as explained in Table 2-3 on page 2-15, then click **Next** to go the following screen.

Note: 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 “Configuring Date and Time Service” on page 10-24.

Table 2-3. Setup Wizard Step 3: System Date and Time Settings

Setting	Description (or Subfield and Description)	
Set Time, Date and NTP Servers		
Date/Time	From the pull-down menu, select the local time zone in which the UTM operates. The proper 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** checkbox.	
NTP Server (default or custom)	From the pull-down menu, 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 must specify in the fields that become available with this menu 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://ntp.isc.org/bin/view/Servers/WebHome*.	
	Server 1 Name / IP Address	Enter the IP address or host name the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name the backup NTP server.

Setup Wizard Step 4 of 10: Services

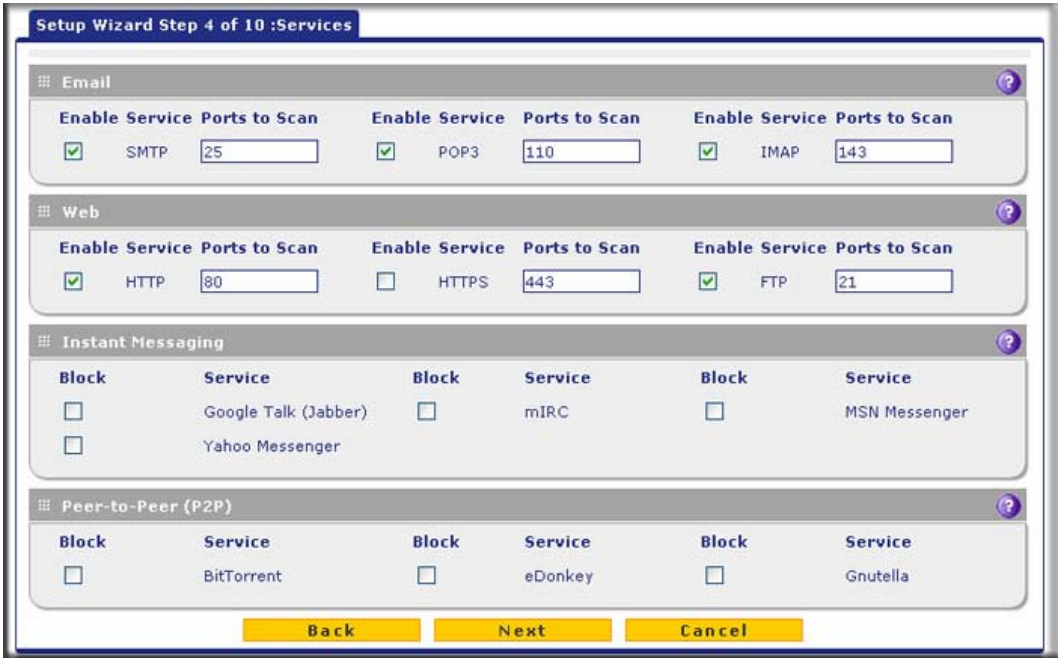


Figure 2-10

Enter the settings as explained in Table 2-4 on page 2-17, then click **Next** to go the following screen.

Note: 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 "Customizing E-mail Protocol Scan Settings" on page 6-4 and "Customizing Web Protocol Scan Settings and Services" on page 6-19.

Table 2-4. Setup Wizard Step 4: Services Settings

Setting	Description (or Subfield and Description)	
Email		
SMTP	SMTP scanning is enabled by default on standard service port 25.	To disable any of these services, deselect the corresponding checkbox. 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.	
Web		
HTTP	HTTP scanning is enabled by default on standard service port 80.	To disable HTTP scanning, deselect the corresponding checkbox. 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 checkbox. You can change the standard service port (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, deselect the corresponding checkbox. You can change the standard service port or add another port in the corresponding Ports to Scan field.
Instant Messaging		
Google Talk (Jabber)	Scanning of these instant messaging services is disabled by default. To enable any of these services, select the corresponding checkbox. **Note:** For Instant Messaging services, the following services can be blocked: logging in, sharing files, sharing video, sharing audio, and text messaging.	
Yahoo Messenger		
mIRC		
MSN 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 checkbox.	
eDonkey		
Gnutella		

Setup Wizard Step 5 of 10: Email Security

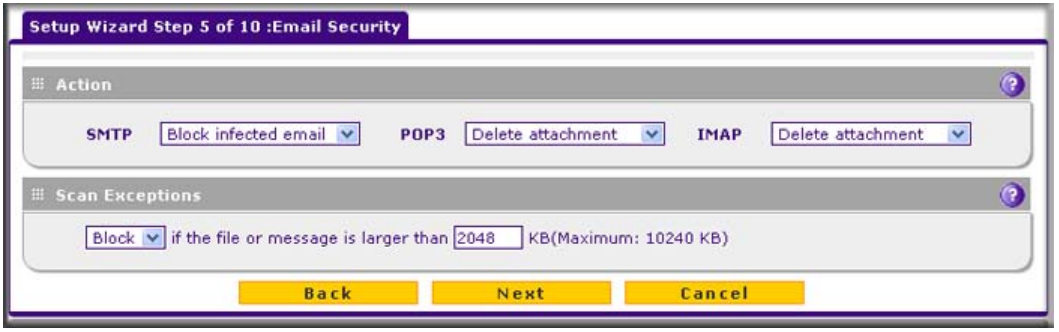


Figure 2-11

Enter the settings as explained in Table 2-5, then click **Next** to go the following screen.

Note: 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 "Customizing E-mail Anti-Virus and Notification Settings" on page 6-5.

Table 2-5. Setup Wizard Step 5: Email Security Settings

Setting	Description (or Subfield and Description)
Action	
SMTP	From the **SMTP** pull-down menu, specify one of the following actions when an infected e-mail is detected: • **Block infected email**. This is the default setting. The e-mail is blocked, and a log entry is created. • **Delete attachment**.The e-mail is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The e-mail is not blocked and the attachment is not deleted.
POP3	From the **POP3** pull-down menu, specify one of the following actions when an infected e-mail is detected: • **Delete attachment**. This is the default setting. The e-mail is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created.The e-mail is not blocked and the attachment is not deleted.

Table 2-5. Setup Wizard Step 5: Email Security Settings (continued)

Setting	Description (or Subfield and Description)
IMAP	From the **IMAP** pull-down menu, specify one of the following actions when an infected e-mail is detected: • **Delete attachment**. This is the default setting. The e-mail is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The e-mail is not blocked and the attachment is not deleted.
Scan Exceptions	
The default maximum file or message size 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 10-1). From the pull-down menu, specify one of the following actions 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.	

Setup Wizard Step 6 of 10: Web Security

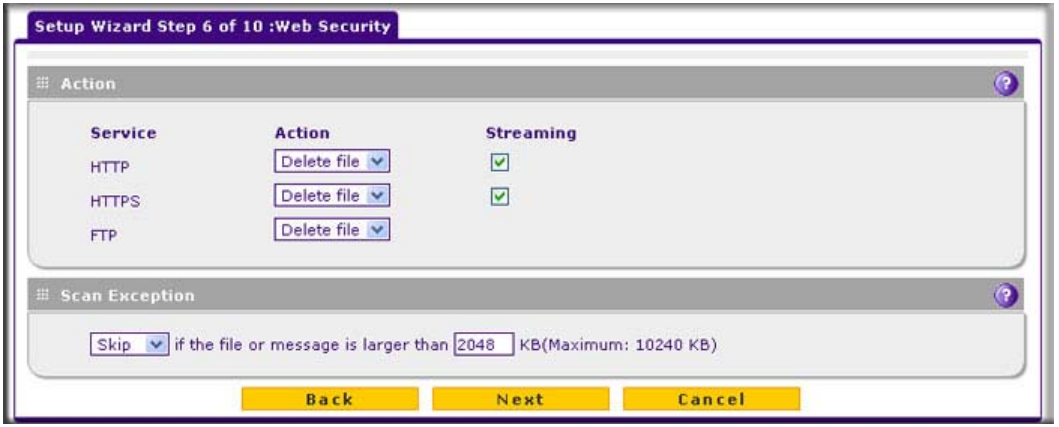


Figure 2-12

Enter the settings as explained in Table 2-6 on page 2-20, then click **Next** to go the following screen.

Note: 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 "Configuring Web Malware Scans" on page 6-21.

Table 2-6. Setup Wizard Step 6: Web Security Settings

Setting	Description (or Subfield and Description)
Action	
HTTP	From the **HTTP** pull-down menu, specify one of the following actions 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. Select the **Streaming** checkbox 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.
HTTPS	From the **HTTPS** pull-down menu, specify one of the following actions 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. Select the **Streaming** checkbox 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** pull-down menu, specify one of the following actions 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.
Scan Exceptions	
The default maximum file or object size that are 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 10-1). From the pull-down menu, specify one of the following actions 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.	

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

Figure 2-13

Enter the settings as explained in Table 2-7, then click **Next** to go the following screen.

Note: 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 "Configuring Web Content Filtering" on page 6-23.

Table 2-7. Setup Wizard Step 7: Content Filtering Settings

Setting	Description (or Subfield and Description)
Blocked Web Categories	
Select the **Enable Blocking** checkbox to enable blocking of Web categories. By default, this checkbox is deselected. Select the checkboxes 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 6-1 on page 6-2 for information about the Web categories that are blocked by default. Categories that are preceded by a green rectangular are allowed by default; categories that are preceded by a pink rectangular 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 checkboxes.	
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.	

Setup Wizard Step 8 of 10: Email Notification

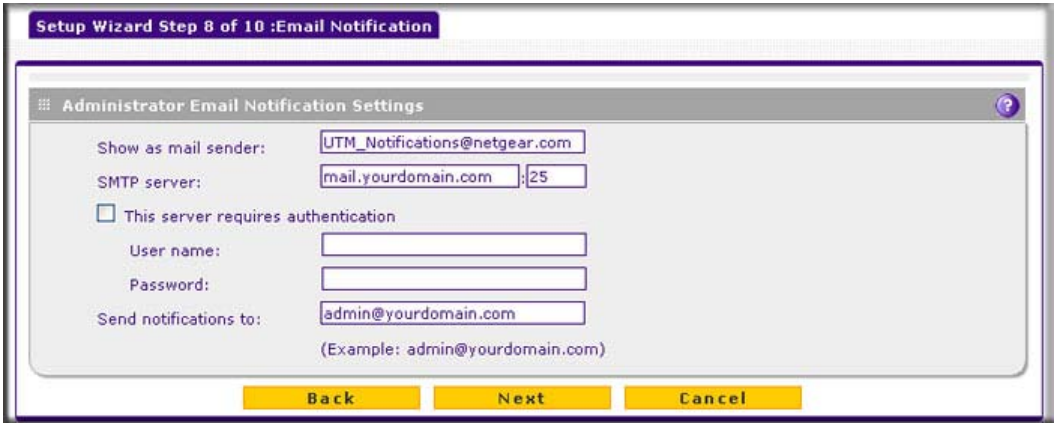


Figure 2-14

Enter the settings as explained in Table 2-8, then click **Next** to go the following screen.

Note: 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 "Configuring the E-mail Notification Server" on page 11-5.

Table 2-8. Setup Wizard Step 8: Administrator Email Notification Settings

Setting	Description (or Subfield and Description)	
Administrator Email Notification Settings		
Show as mail sender	A descriptive name of the sender for e-mail 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 e-mail SMTP server. The default port number is 25. **Note**: If you leave this field blank, the UTM cannot send e-mail notifications.	
This server requires authentication	If the SMTP server requires authentication, select the **This server requires authentication** checkbox and enter the following settings:	
	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 e-mail address of the administrator.	

Setup Wizard Step 9 of 10: Signatures & Engine

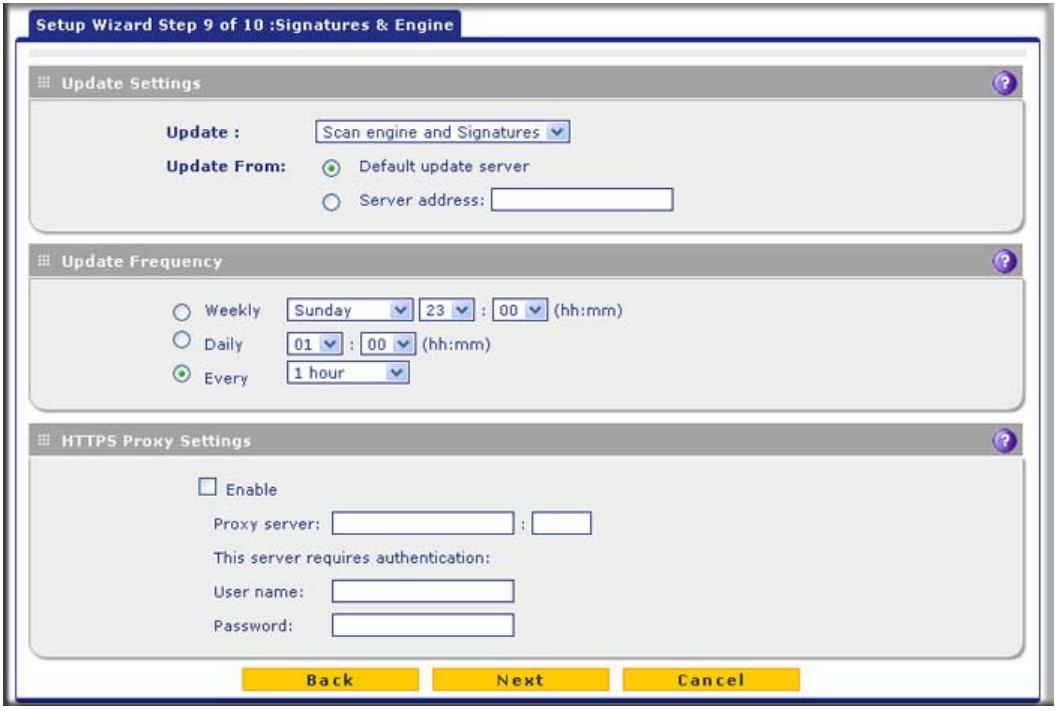


Figure 2-15

Enter the settings as explained in Table 2-9 on page 2-25, then click **Next** to go the following screen.

Note: 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 and Engine**. For more information about these settings, see "Updating the Scan Signatures and Scan Engine Firmware" on page 10-21.

Table 2-9. Setup Wizard Step 9: Signatures & Engine Settings

Setting	Description (or Subfield and Description)	
Update Settings		
Update	From the pull-down menu, 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 Update Frequency settings below.	
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.	
Update Frequency		
Specify the frequency with which the UTM checks for file updates: • **Weekly**. From the pull-down menus, select the weekday, hour, and minutes that the updates occur. • **Daily**. From the pull-down menus, select the hour, and minutes that the updates occur. • **Every**. From the pull-down menu, 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 via a proxy server, select the **Enable** checkbox 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.

Setup Wizard Step 10 of 10: Saving the Configuration

Figure 2-16

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

Verifying Proper 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.

Testing Connectivity

Verify that network traffic can pass through the UTM:

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

Testing 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 DoS program 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 properly scans HTTP traffic:

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 “Customizing Web Protocol Scan Settings and Services” on page 6-19 and “Configuring Web Malware Scans” on page 6-21.
2. Check the downloaded eicar.com test file, and note the attached malware information file.

Registering the UTM with NETGEAR

To receive threat management component updates and technical support, you must register your UTM with NETGEAR. The support registration key is provided with the product package (see “Service Registration Card with License Keys” on page 1-8).

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 3 types of licenses to perform the initial testing and configuration. To use the trial period, do not click Register in step 4 of the procedure below 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.

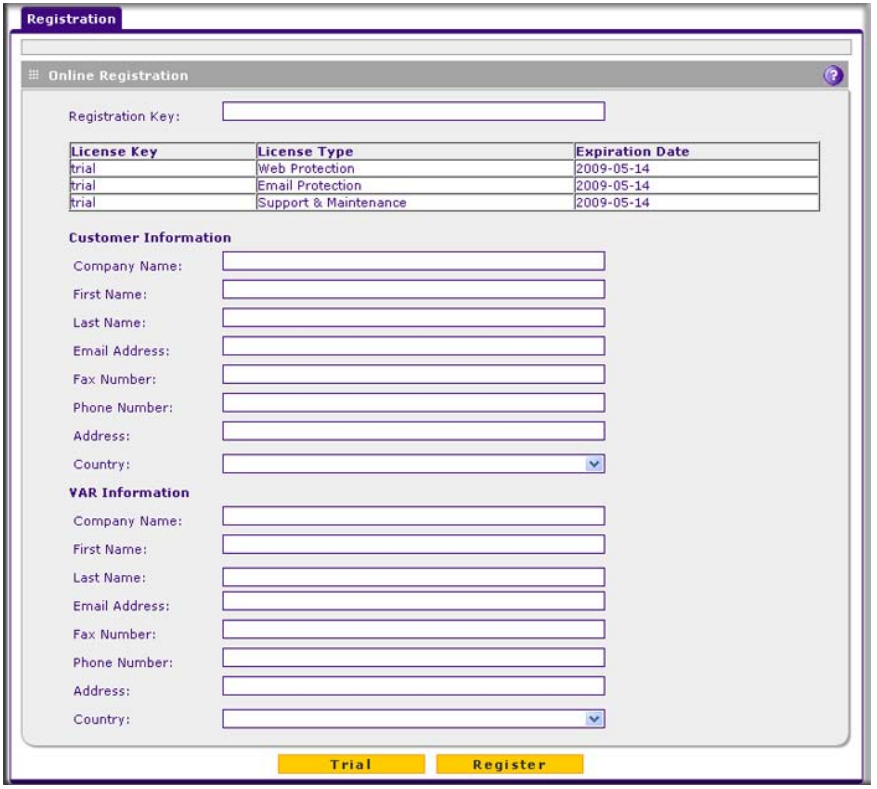


Figure 2-17

2. Enter the license key in the Registration Key field.
3. Fill out the customer and VAR fields.
4. Click **Register**.

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:** When you reset the UTM to the original factory default settings after you have entered the license keys to activate the UTM (see "Registering the UTM with NETGEAR" on page 2-26), 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 re-enter the license keys and re-activate the UTM.

What to Do Next

You have completed setting up and deploying 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 2-8.

The UTM is ready for use. However, some important tasks that you might want to address before you deploy the UTM in your network are listed below:

- "Configuring the WAN Mode (Required for Dual-WAN Port Models Only)" on page 3-9.
- "Configuring VPN Authentication Domains, Groups, and Users" on page 9-1.
- "Managing Digital Certificates" on page 9-17.
- "Using the IPsec VPN Wizard for Client and Gateway Configurations" on page 7-3.
- "Using the SSL VPN Wizard for Client Configurations" on page 8-2.

Chapter 3
Manually Configuring Internet and WAN Settings

	**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 Dual WAN and Dynamic DNS, and to configure secondary WAN addresses and advanced WAN options.

This chapter contains the following sections:

Understanding the Internet and WAN Configuration Tasks

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

1. **Configure the Internet connections to your ISP(s)**. During this phase, you connect to your ISPs. You can also program the WAN traffic meters at this time if desired. See "Configuring the Internet Connections" on page 3-2.
2. **Configure the WAN mode (required for operation of the dual-WAN port models)**. For all models, select either NAT or classical routing. For the dual-WAN port models only, select either dedicated (single WAN) mode, auto-rollover mode, or load balancing mode. For load balancing, you can also select any necessary protocol bindings. See "Configuring the WAN Mode (Required for Dual-WAN Port Models Only)" on page 3-9.
3. **Configure secondary WAN addresses on the WAN ports (optional)**. Configure aliases for each WAN port. See "Configuring Secondary WAN Addresses" on page 3-17.

4. **Configure dynamic DNS on the WAN ports (optional)**. Configure your fully qualified domain names during this phase (if required). See "Configuring Dynamic DNS" on page 3-19.
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 "Configuring Advanced WAN Options" on page 3-22.

Each of these tasks is detailed separately in this chapter.

Note: For information about how to configure the WAN meters, see "Enabling the WAN Traffic Meter" on page 11-1.

Configuring the Internet Connections

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 section only if you want to make changes to your Internet connections.

To set up your UTM for secure Internet connections, you configure WAN ports 1 and 2. The Web Configuration Manager offers two connection configuration options:

- Automatic detection and configuration of the network connection.
- Manual configuration of the network connection.

Each option is detailed in the sections following.

Automatically Detecting and Connecting

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

1. Select **Network Config** > **WAN Settings** from the menu. On dual-WAN port models, the WAN Settings tabs appear, with the WAN1 ISP Settings screen in view (see Figure 3-1 on page 3-3). On the single-WAN port models, the WAN ISP screen displays.

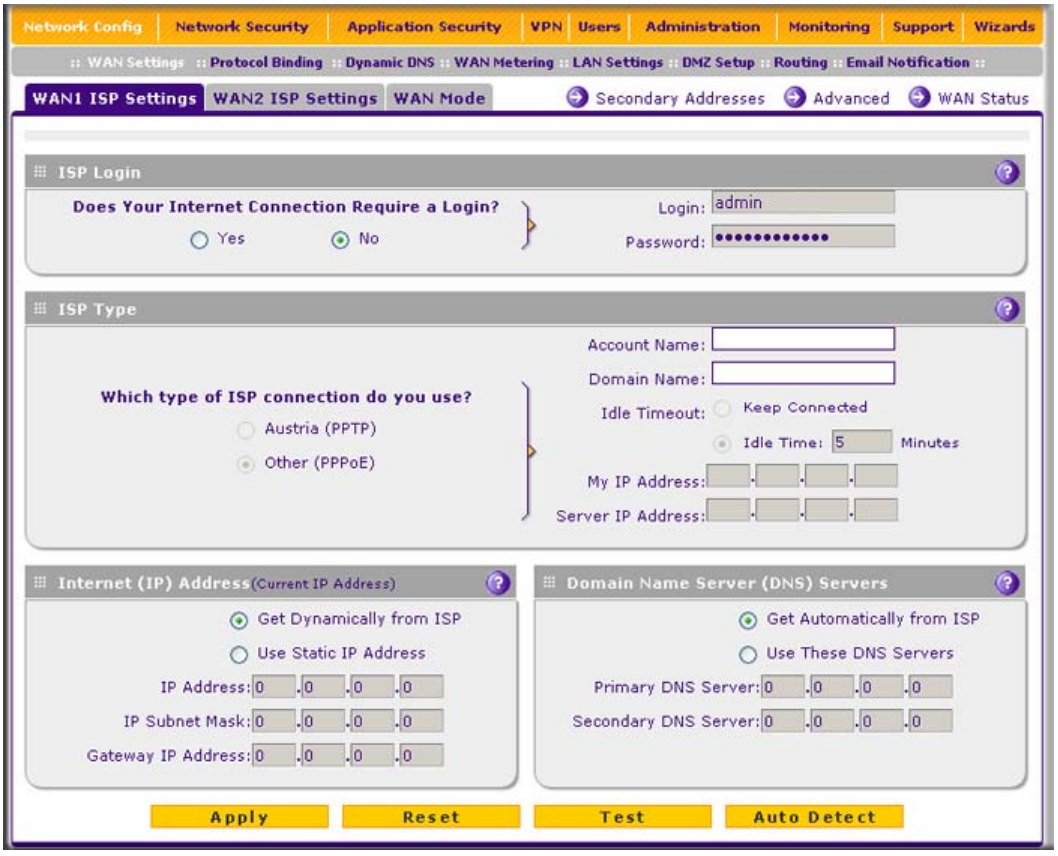


Figure 3-1

2. Click the **Auto Detect** action button at the bottom of the menu. The auto-detect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support. (Figure 3-2 shows a dual-WAN port model's screen. A single-WAN port model's screen shows only a single WAN ISP Settings submenu tab.)

Figure 3-2

The auto-detect process will return one of the following results:

- If the auto-detect process is successful, a status bar at the top of the menu displays the results (see the red text in Figure 3-2 on page 3-3).
- If the auto-detect process senses a connection method that requires input from you, it prompts you for the information. All methods with their required settings are detailed in Table 3-1.

Table 3-1. Internet connection methods

Connection Method	Data Required
DHCP (Dynamic IP)	No data is required.
PPPoE	Login (Username, Password); Account Name, Domain Name
PPTP	Login (Username, Password), Account Name, Local IP address, and PPTP Server IP address;
Fixed (Static) IP	Static IP address, Subnet, and Gateway IP; and related data supplied by your ISP.

- If the auto-detect process does not find a connection, you are prompted to either check the physical connection between your UTM and the cable or DSL line or to check your UTM's MAC address. For more information, see "Configuring the WAN Mode (Required for Dual-WAN Port Models Only)" on page 3-9 and "Troubleshooting the ISP Connection" on page 12-5.

3. To verify the connection, click the **WAN Status** option arrow at the top right of the screen. A popup window appears, displaying the connection status of the WAN port

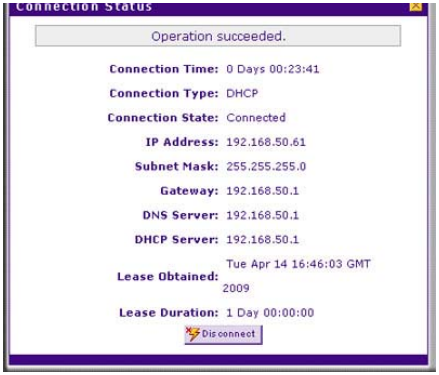


Figure 3-3

The WAN Status window should show a valid IP address and gateway. If the configuration was not successful, skip ahead to "Manually Configuring the Internet Connection" on this page , or see "Troubleshooting the ISP Connection" on page 12-5.

	**Note:** If the configuration process was successful, you are connected to the Internet through WAN port 1. If you intend to use the dual WAN capabilities of the UTM25, continue with the configuration process for WAN port 2.

	**Note:** For more information about the WAN Connection Status screen, see "Viewing the WAN Ports Status" on page 11-27.

4. Click the WAN2 ISP Settings tab (dual-WAN port models only).
5. Repeat the previous steps to automatically detect and configure the WAN2 Internet connection (dual-WAN port models only).
6. Open the WAN Status window and verify a successful connection

If your WAN ISP configuration was successful, you can skip ahead to "Configuring the WAN Mode (Required for Dual-WAN Port Models Only)" on page 3-9.

If one or both automatic WAN ISP configurations failed, you can attempt a manual configuration as described in the following section, or see "Troubleshooting the ISP Connection" on page 12-5.

Setting 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. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then you must enter that address. Setting the UTM's MAC address is controlled through the Advanced options on the single WAN-port model's WAN ISP Settings screen or the dual WAN-port model's WAN1 ISP Settings and WAN2 ISP Settings screen (see"Configuring Advanced WAN Options" on page 3-22).

Manually Configuring the Internet Connection

Unless your ISP automatically assigns your configuration via DHCP, you need to obtain configuration parameters from your ISP in order to manually establish an Internet connection. The necessary parameters for various connection types are listed in Table 3-1 on page 3-4.

To manually configure the WAN1 ISP (dual-WAN port models) or WAN ISP (single-WAN port models) settings:

1. On a dual-WAN port model, select **Network Configuration** > **WAN Settings** > **WAN1 ISP Settings**. The WAN Settings tabs appear, with the WAN1 ISP Settings screen in view (see Figure 3-1 on page 3-3, which shows a dual-WAN port model's screen). On a single-WAN port model, select **Network Configuration > WAN Settings > WAN ISP Settings**. The WAN ISP Settings screen displays. Figure 3-4 shows the ISP Login section of the screen.

Figure 3-4

2. In the ISP Login section of the screen, select one of the following options:
   - If your ISP requires an initial login to establish an Internet connection, click **Yes** (this is the default).
   - If a login is not required, click **No** and ignore the Login and Password fields.
3. If you clicked **Yes**, enter the login name in the Login field and the password in the Password field. This information is provided by your ISP.
4. In the ISP Type section on the screen, select the type of ISP connection that you use from the three listed options. By default, "Other (PPPoE)" is selected, as shown in Figure 3-5.

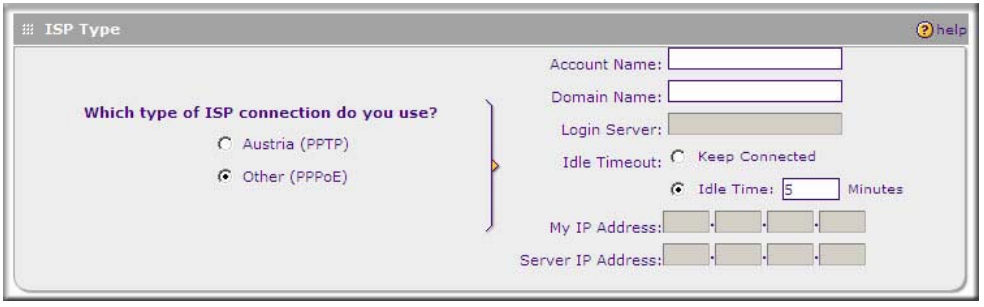


Figure 3-5

5. If your connection is PPTP or PPPoE, your ISP requires an initial login. Enter the settings as explained in Table 3-2.

Table 3-2. PPTP and PPPoE Settings

Setting	Description (or Subfield and 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 valid account name for the PPTP connection (usually your e-mail “ID” assigned by your ISP). Some ISPs require entering your full e-mail address here.
	Domain Name	Your domain name or workgroup name assigned by your ISP, or your ISP’s domain name. You may 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 Time** radio button and, in the timeout 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 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 may 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 Time** radio button and, in the timeout 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.

6. Configure the Internet (IP) Address settings as explained in Table 3-3. Click the **Current IP Address** link to see the currently assigned IP address.

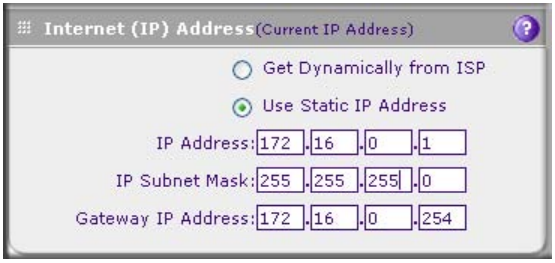


Figure 3-6

Table 3-3. Internet (IP) Address Settings

Setting	Description (or Subfield and 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.	
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.

7. Configure the Domain Name Server (DNS) servers settings as explained in Table 3-4 on page 3-9.

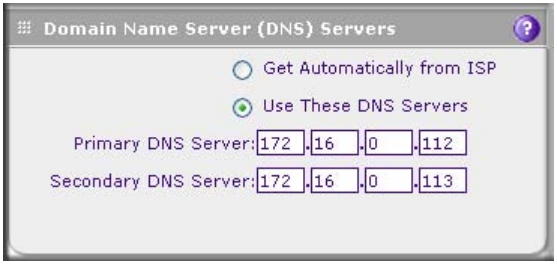


Figure 3-7

Table 3-4. DNS Server Settings

Setting	Description (or Subfield and Description)	
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, select the **Use these DNS Servers** radio button. Ensure 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.

8. Click **Test** to evaluate your entries. The UTM attempts to make a connection according to the settings that you entered.
9. Click **Apply** to save any changes to the WAN1 ISP settings of a dual-WAN port model or WAN ISP settings of a single-WAN port model. (Or, click **Reset** to discard any changes and revert to the previous settings.)
10. For the dual-WAN port models only, if you intend to use a dual WAN mode, click the **WAN2 ISP Settings** tab and configure the WAN2 ISP settings using the same steps as WAN1.

When you are finished, click the **Logout** link at the upper right corner of the Web Management Interface or proceed to additional setup and management tasks.

Configuring the WAN Mode (Required for Dual-WAN Port Models Only)

On dual-WAN port models only, the dual-WAN ports of 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), or one port can be disabled.

- **Auto-Rollover Mode**. The selected WAN interface is defined as the primary link and the other interface is defined as the rollover link. 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 port that must act as the primary link for this mode. Ensure that the backup WAN port has also been configured and that you configure the WAN Failure Detection Method on the WAN Mode screen to support auto-rollover.

- **Load Balancing Mode**. The UTM distributes the outbound traffic equally among the WAN interfaces that are functional.

	**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.

- **Single WAN Port Mode**. The selected WAN interface is made primary and the other is disabled.

For whichever WAN mode you choose, you must also choose either NAT or classical routing, as explained in the following sections.

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.

- The UTM uses NAT to select the correct PC (on your LAN) to receive any incoming data.
- If you only have a single public Internet IP address, you must 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.

To configure NAT:

1. Select **Network Config** > **WAN Settings** from the menu, then click the **WAN Mode** tab. The WAN Mode screen displays (see Figure 3-8 on page 3-12).
2. In the NAT (Network Address Translation) section of the screen select the **NAT** radio button.
3. Click **Apply** to save your settings.

Classical Routing (All Models)

In classical routing mode, the UTM performs routing, but without NAT. To gain Internet access, each PC on your LAN must 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 learn the status of the WAN ports, you can view the System Status screen page (see "Viewing System Status" on page 11-20) or look at the LEDs on the front panel (see "Front Panel" on page 1-10).

To configure classical routing:

1. Select **Network Config** > **WAN Settings** from the menu, then click the **WAN Mode** tab. The WAN Mode screen displays (see Figure 3-8 on page 3-12).
2. In the NAT (Network Address Translation) section of the screen select the **Classical Routing** radio button.
3. Click **Apply** to save your settings.

Configuring Auto-Rollover Mode (Dual-WAN Port Models Only)

For the dual-WAN port models only, 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 will act 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 check the connection of the primary link at regular intervals to detect router status. Link failure is detected in one of the following ways:

- By sending DNS queries to a DNS server, or
- By sending a ping request to an IP address, or
- 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 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.

To configure the dual-WAN ports for auto-rollover mode:

1. Select **Network Config** > **WAN Settings** from the menu, then click the **WAN Mode** tab. The WAN Mode screen displays.

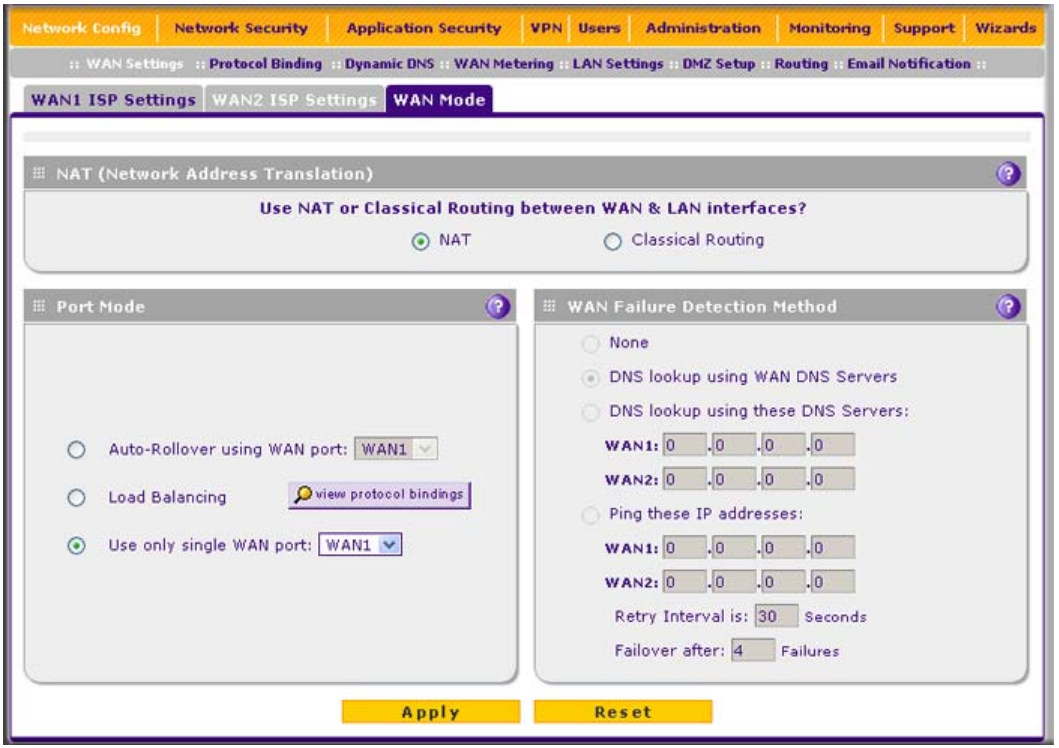


Figure 3-8

2. Enter the settings as explained in Table 3-5.

Table 3-5. Auto-Rollover Mode Settings (Dual-WAN Port Models Only)

Setting	Description (or Subfield and Description)
Port Mode	
Auto-Rollover using WAN port	Select the **Auto-Rollover using** WAN port radio button. Then, from the pull-down menu, select the WAN port that must function as the as the primary link for this mode. **Note**: Ensure that the backup WAN port is configured before enabling Auto-Rollover mode.

Table 3-5. Auto-Rollover Mode Settings (Dual-WAN Port Models Only) (continued)

Setting	Description (or Subfield and Description)	
WAN Failure Detection Method Select *one* of the following detection failure methods:		
DNS lookup using WAN DNS Servers	DNS queries are sent to the DNS server configured on the WAN ISP pages (see "Configuring the Internet Connections" on page 3-2).	
DNS lookup using this DNS Server	DNS queries are sent to this server through the WAN interface 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. Enter the following DNS settings:	
	WAN1	The IP address of the DNS server for port WAN1.
	WAN2	The IP address of the DNS server for port WAN2.
	Retry Interval is	The retry interval in seconds. The DNS query is sent periodically after every test period. The default test period is 30 seconds.
	Failover after	The number of failover attempts. The primary WAN link is considered down after the configured number of queries have failed to elicit a reply. The backup link is brought up after this has occurred. The failover default is 4 failures.
Ping these IP addresses	A public IP address that does not reject the ping request and does not consider ping traffic to be abusive. Queries are sent to this server 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. Enter the following DNS settings:	
	WAN1	The IP address of the DNS server for port WAN1.
	WAN2	The IP address of the DNS server for port WAN2.
	Retry Interval is	The retry interval in seconds. The 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 link is considered down after the configured number of queries have failed to elicit a reply. The backup link is brought up after this has occurred. The failover default is 4 failures.

Note: The default time to roll over after the primary WAN interface fails is 2 minutes; a 30-second minimum test period for a minimum of 4 tests.

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

When a rollover occurs, you can configure the UTM to generate a notification e-mail to a specified address (see "Configuring and Activating System, E-mail, and Syslog Logs" on page 11-6). When the UTM detects that the failed primary WAN interface has been restored, an automatic rollover to the primary WAN interface occurs.

Configuring Load Balancing and Optional Protocol Binding (Dual-WAN Port Models Only)

For the dual-WAN port models only, to use multiple ISP links simultaneously, configure load balancing. In load balancing mode, either 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.

To configure the dual-WAN ports for load balancing mode with optional protocol binding:

1. Select **Network Config** > **WAN Settings** from the menu, then click the **WAN Mode** tab. The WAN Mode screen displays (see Figure 3-8 on page 3-12).
2. Select the **Load Balancing** radio button.
3. Optional: Next to the Load Balancing radio button, click the **view protocol bindings** button. The WAN1 Protocol Bindings screen displays (see Figure 3-9 on page 3-15). (The Web Management Interface path to this screen is **Network Config** > **Protocol Bindings**.)

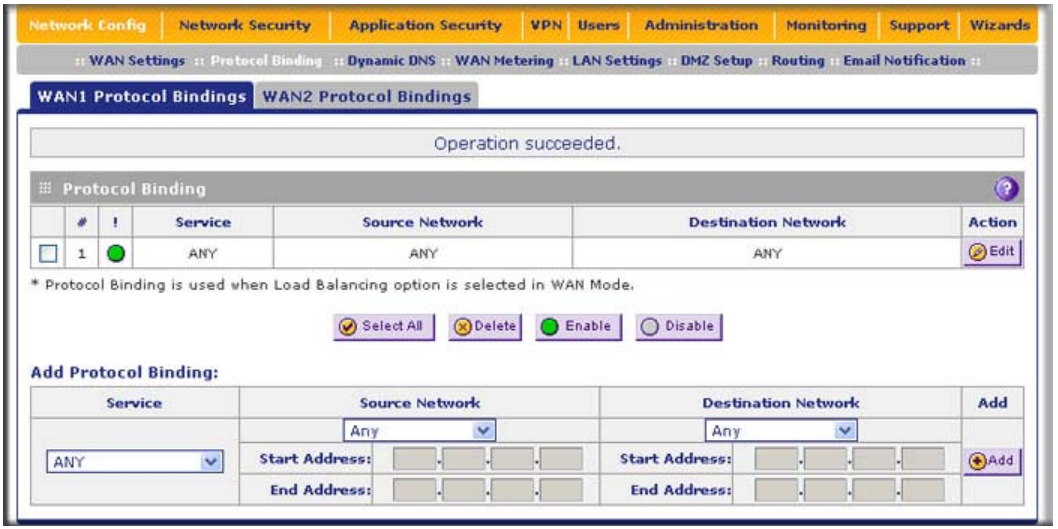


Figure 3-9

a. Figure 3-9 shows one example in the Protocol Binding table. Configure the protocol binding settings as explained in Table 3-6.

Table 3-6. Protocol Binding Settings (Dual-WAN Port Models Only)

Setting	Description (or Subfield and Description)	
Add Protocol Binding		
Service	From the pull-down menu, select a service or application to be covered by this rule. If the service or application does not appear in the list, you must define it using the Services menu (see "Services-Based Rules" on page 5-3).	
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 pull-down menu:	
	Any	All devices on your LAN.
	Single address	In the Start Address field, enter the IP address to which the rule is applied.
	Address range	In the Start Address field and End Address field, enter the IP addresses for the range to which the rule is applied.

Table 3-6. Protocol Binding Settings (Dual-WAN Port Models Only) (continued)

Setting	Description (or Subfield and Description)	
Source Network (continued)	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 may also assign a customized name to a group (see "Changing Group Names in the Network Database" on page 4-16).
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 pull-down menu:	
	Any	All Internet IP address.
	Single address	In the Start Address field, enter the IP address that is covered by the rule.
	Address range	In the Start Address field and End Address field, enter the IP addresses for the range that is covered by the rule.

b. Click the **Add** table button in the rightmost column to add the protocol binding rule to the Protocol Binding table. The rule is automatically enabled, which is indicated by the "!" status icon that displays a green circle.

c. Repeat step a and step b for each protocol binding rule that you want to add to the Protocol Binding table.

d. If not all table entries are enabled, select the table entries that you want to enable, or click the **Select All** table button. Then, click the **Enable** table button.

e. Open the WAN2 Protocol Bindings screen and repeat step a through step d to set protocol bindings for the WAN2 port.

f. Return to the WAN Mode screen by selecting **Network Config** > **WAN Settings** from the menu and clicking the **WAN Mode** tab.

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

Configuring Secondary WAN Addresses

A single WAN Ethernet port can 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 FTP server, even though both servers use the same physical IP address. You can add several secondary IP addresses to the WAN port of a single-WAN port model or to WAN1 port and WAN2 port of a dual-WAN port model.

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

- In the WAN Destination IP Address pull-down menus of the following inbound firewall rule screens:
  - Add LAN WAN Inbound Service screen
  - Add DMZ WAN Inbound Service screen
- In the NAT IP pull-down menus 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 “Using Rules to Block or Allow Specific Kinds of Traffic” on page 5-3).

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 properly configured IP addresses on a dual-WAN port model:
Primary WAN1 IP address: 10.0.0.1 with subnet 255.0.0.0
Secondary WAN1 IP: 30.0.0.1 with subnet 255.0.0.0
Primary WAN2 IP address: 20.0.0.1 with subnet 255.0.0.0
Secondary WAN2 IP: 40.0.0.1 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: 192.168.20.1 with subnet 255.255.255.0

To add a secondary WAN address to a WAN port:

1. Select **Network Config** > **WAN Settings** from the menu. On a dual-WAN port model, the WAN Settings submenu tabs appear with the WAN1 ISP Settings screen in view. On a single WAN model, the WAN Settings submenu tabs appear with the WAN ISP Settings screen in view.
2. Click the **Secondary Addresses** option arrow. On a dual-WAN port model, the WAN1 Secondary Addresses screen displays (see Figure 3-10, which shows some examples in the List of Secondary WAN addresses table). On a a single-WAN port model, the WAN Secondary Addresses screen displays.

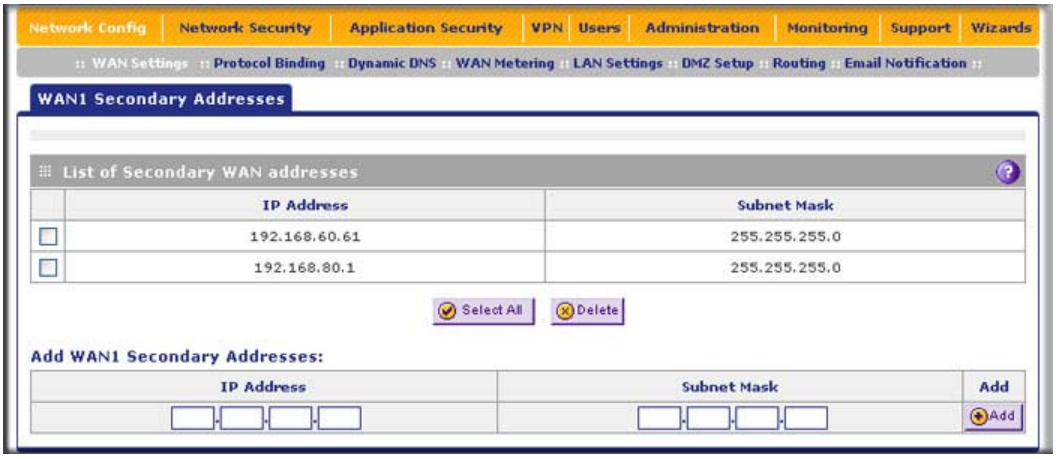


Figure 3-10

The List of Secondary WAN addresses table displays the secondary LAN IP addresses added to the UTM.

3. In the Add WAN1 Secondary Addresses section (dual-WAN port models) or Add WAN Secondary Addresses section of the screen (single-WAN port models), enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to WAN1 port (dual-WAN port models) or to the single WAN port (single-WAN port models).
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.
4. 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 3 and step 4 for each secondary IP address that you want to add to the List of Secondary WAN addresses table.

Configuring 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 must set up an account with a DDNS provider such as DynDNS.org, TZO.com, or Oray.net. (Links to DynDNS, TZO and Oray are provided for your convenience as submenu tabs of the Dynamic DNS configuration menu.) The UTM firmware includes software that notifies dynamic DNS 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 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 a fully qualified domain name (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 a fully qualified domain name (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 dynamic DNS service does not work because private addresses are not routed on the Internet.

To configure Dynamic DNS:

1. Select **Network Config** > **Dynamic DNS** from the menu.
2. Click the **Dynamic DNS** tab. The Dynamic DNS screen displays (see Figure 3-11 on page 3-20).

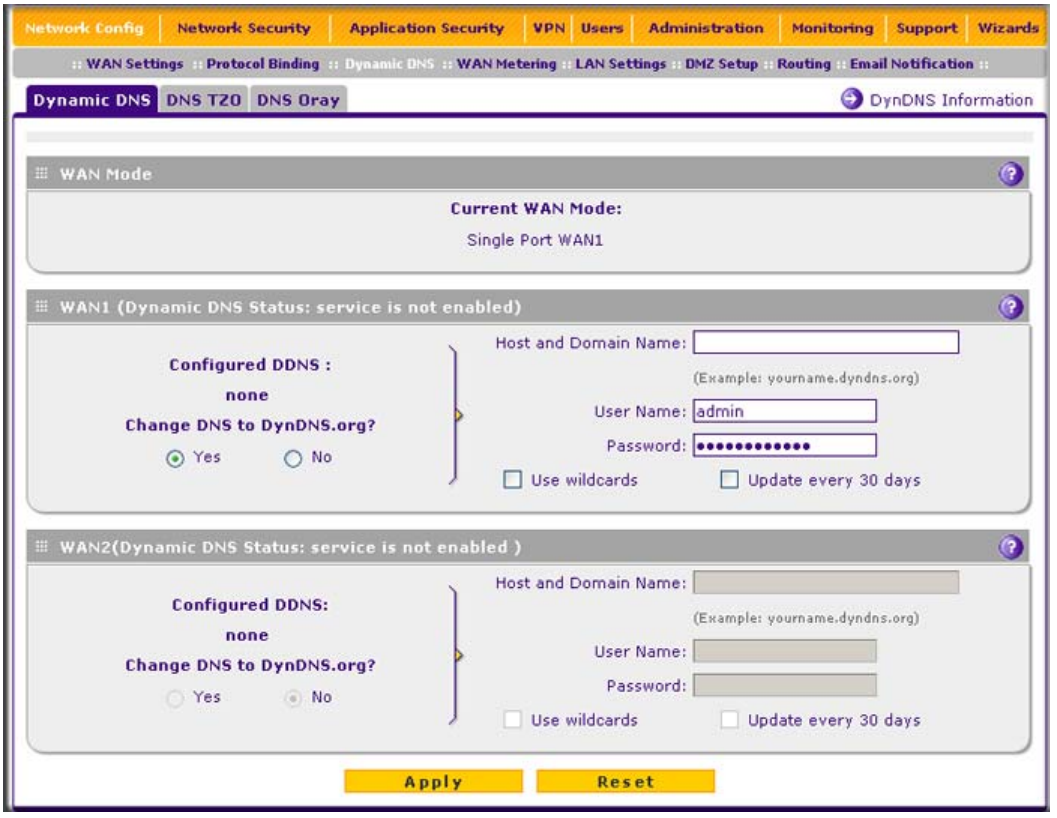


Figure 3-11

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

3. Select the submenu tab for your DDNS service provider:

- Dynamic DNS submenu tab (which is shown in Figure 3-11) for DynDNS.org or DYNDNS.com.
- DNS TZO submenu tab for TZO.com.
- DNS Oray submenu tab for Oray.net.

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

Figure 3-12:

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

6. For each WAN port of a dual-WAN port model or for the single WAN port of a single-WAN port model, configure the DDNS service settings as explained in Table 3-7, which shows the settings for a dual-WAN port model. (The screen for a single-WAN port model shows settings for a single WAN port only.)

Table 3-7. DNS Service Settings

Setting	Description (or Subfield and Description)	
WAN1 (Dynamic DNS Status: ...)		
Change DNS to (DynDNS, TZO, or Oray)	Select the **Yes** radio button to enable the DDNS service. The service that displays on screen depends on the submenu tab for 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.
	User Name	The user name for DDNS server authentication.
	Password	The password that is used for DDNS server authentication.
	Use wildcards	If your DDNS provider allows the use of wild cards in resolving your URL, you may select the **Use wildcards** checkbox 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 it appears, you can select the **Update every 30 days** checkbox to enable a periodic update.
WAN2 (Dynamic DNS Status: ...)		
See the information for WAN 1 above about how to enter the settings. You can select different DDNS services for WAN 1 and WAN 2.		

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

Configuring Advanced WAN Options

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

To configure advanced WAN options:

1. Select **Network Config** > **WAN Settings** from the menu. On a dual-WAN port model, the WAN Settings tabs appear, with the WAN1 ISP Settings screen screen in view. On a single-WAN port model, the WAN ISP Settings screen displays.
2. Click the **Advanced** option arrow. On a dual-WAN port model, the WAN1 Advanced Options screen displays (see Figure 3-13). On a single WAN port model, the WAN Advanced Options screen displays.

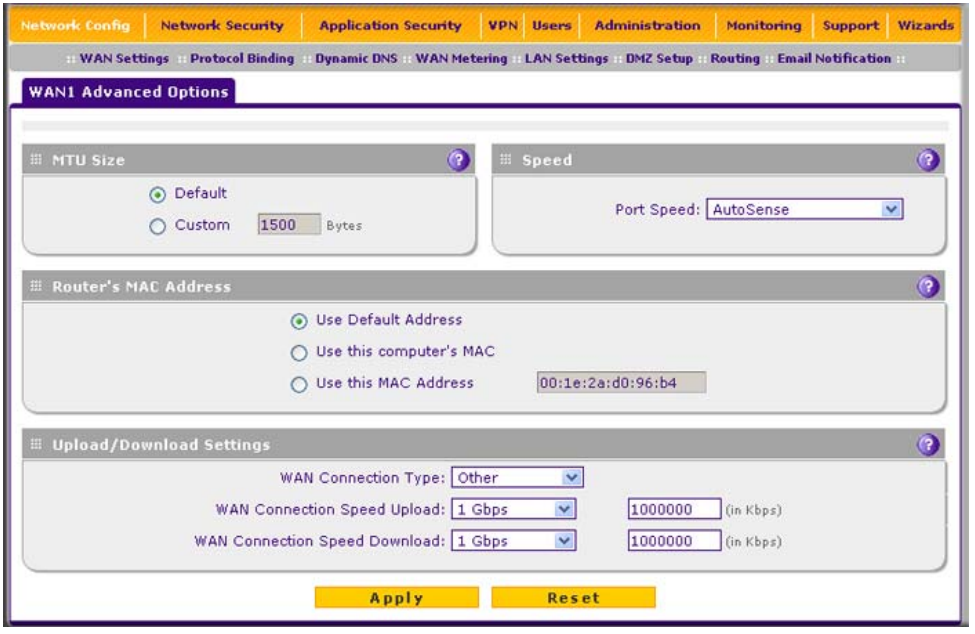


Figure 3-13

3. Enter the default information settings as explained in Table 3-8.

Table 3-8. Advanced WAN Settings

Setting	Description (or Subfield and 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.
Port 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 pull-down menu. Use the half-duplex settings only of the full-duplex settings do not function properly. Select one of the following speeds from the pull-down menu: • **AutoSense**. Speed autosensing. This is the default setting, which can sense 1000BaseT 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.	
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	Select the **Use this computer's MAC** 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 you ISP requires MAC authentication.

Table 3-8. Advanced WAN Settings (continued)

Setting	Description (or Subfield and Description)
Use this MAC Address	Select the **Use this MAC Address** radio button to 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.
Upload/Download Settings These settings rate-limit the traffic that is being forwarded by the UTM.	
WAN Connection Type	From the pull-down menu, 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 pull-down menu, 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 to the right.
WAN Connection Speed Download	From the pull-down menu, 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 to the right.

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

Note: Depending on the changes that you make, when you click **Apply**, the UTM might restart, or services such as HTTP and SMTP might restart.

Note: For dual-WAN port models only, to configure advanced WAN options for WAN2 port, select **Network Config** > **WAN Settings** from the menu. The WAN Settings tabs appear, with the WAN1 ISP Settings screen in view. Now, click the **WAN2 ISP Settings** tab and then the **Advanced** option arrow. The WAN2 Advanced Options screen displays.

Additional WAN-Related Configuration Tasks

- If you want the ability to manage the UTM remotely, enable remote management (see "Configuring Remote Management Access" on page 10-12). If you enable remote management, NETGEAR strongly recommend that you change your password (see "Changing Passwords and Administrator Settings" on page 10-9).
- You can set up the traffic meter for each WAN, if desired. See "Enabling the WAN Traffic Meter" on page 11-1.

Chapter 4
LAN Configuration

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."

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

Managing 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. End nodes 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 must 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.

Managing the UTM's 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 default PVID 1. However, you can assign another PVID to a LAN port by selecting a VLAN profile from the pull-down menu on the LAN Setup screen.

After you have created a VLAN profile and assigned one or more ports to the profile, you must first 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 must be assigned 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 VLAN, 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 member 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 "Using the Setup Wizard to Provision the UTM in Your Network" on page 2-1." For information about how to add and edit a VLAN profile, including its DHCP options, see "Configuring a VLAN Profile" on page 4-6.

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

1. Select **Network Config** > **LAN Settings** from the menu. The LAN submenu tabs appear, with the LAN Setup screen in view. (Figure 4-1 shows two VLAN profiles as an example.)

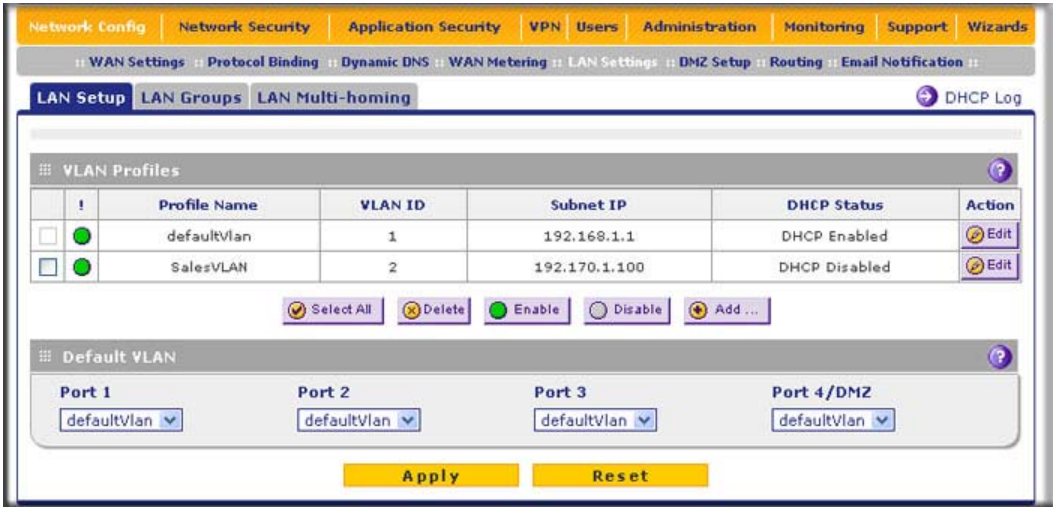


Figure 4-1

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

- **Checkbox**. 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.
  - Grey 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 that provides access to the Edit VLAN Profile screen.

2. Assign a VLAN profile to a LAN port (Port 1, Port 2, Port 3, or Port 4/DMZ) by selecting a VLAN profile from the pull-down menu. Both enabled and disabled VLAN profiles are displayed in the pull-down menus.
3. Click **Apply** to save your settings.

VLAN DHCP Options

For each VLAN, you must specify the Dynamic Host Configuration Protocol (DHCP) options. The configuration of the DHCP options for the UTM's default VLAN, or VLAN 1, are explained in Chapter 2, "Using the Setup Wizard to Provision the UTM in Your Network. 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 must 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. See the link to "Preparing Your Network" in Appendix E for an explanation of DHCP and information about how to assign IP addresses for your network.

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 menu)
- 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 only obtain IP addresses 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 must 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 dual-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.

Configuring a VLAN Profile

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

To add or edit a VLAN profile:

1. Select **Network Config** > **LAN Settings** from the menu. The LAN submenu tabs appear, with the LAN Setup screen in view (see Figure 4-2, which shows two VLAN profiles as an example).

> **Note:** For information about how to manage VLANs, see "Managing the UTM's Port-Based VLANs" on page 4-2. The information below describes how to configure a VLAN profile.

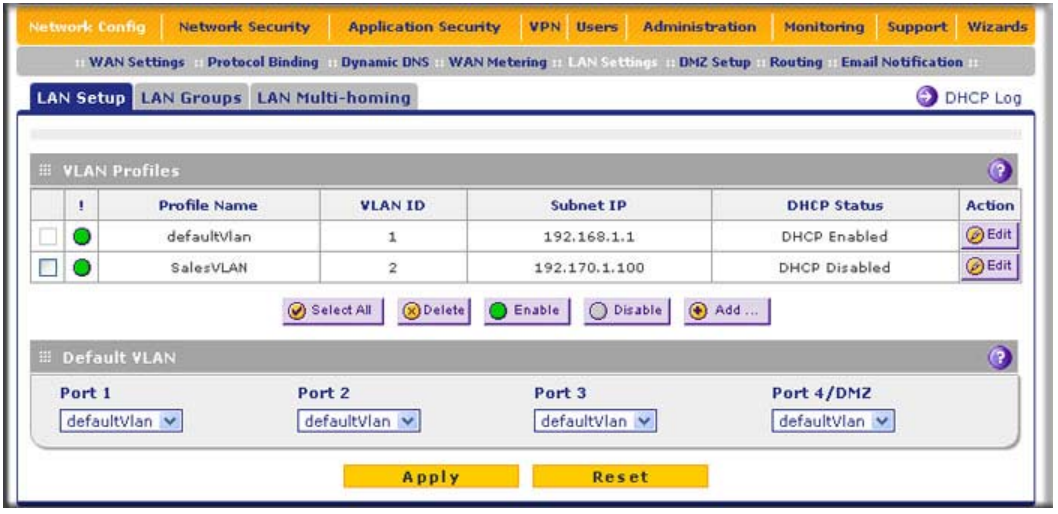


Figure 4-2

2. Either select an entry from the VLAN Profiles table by clicking 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 (see Figure 4-3).

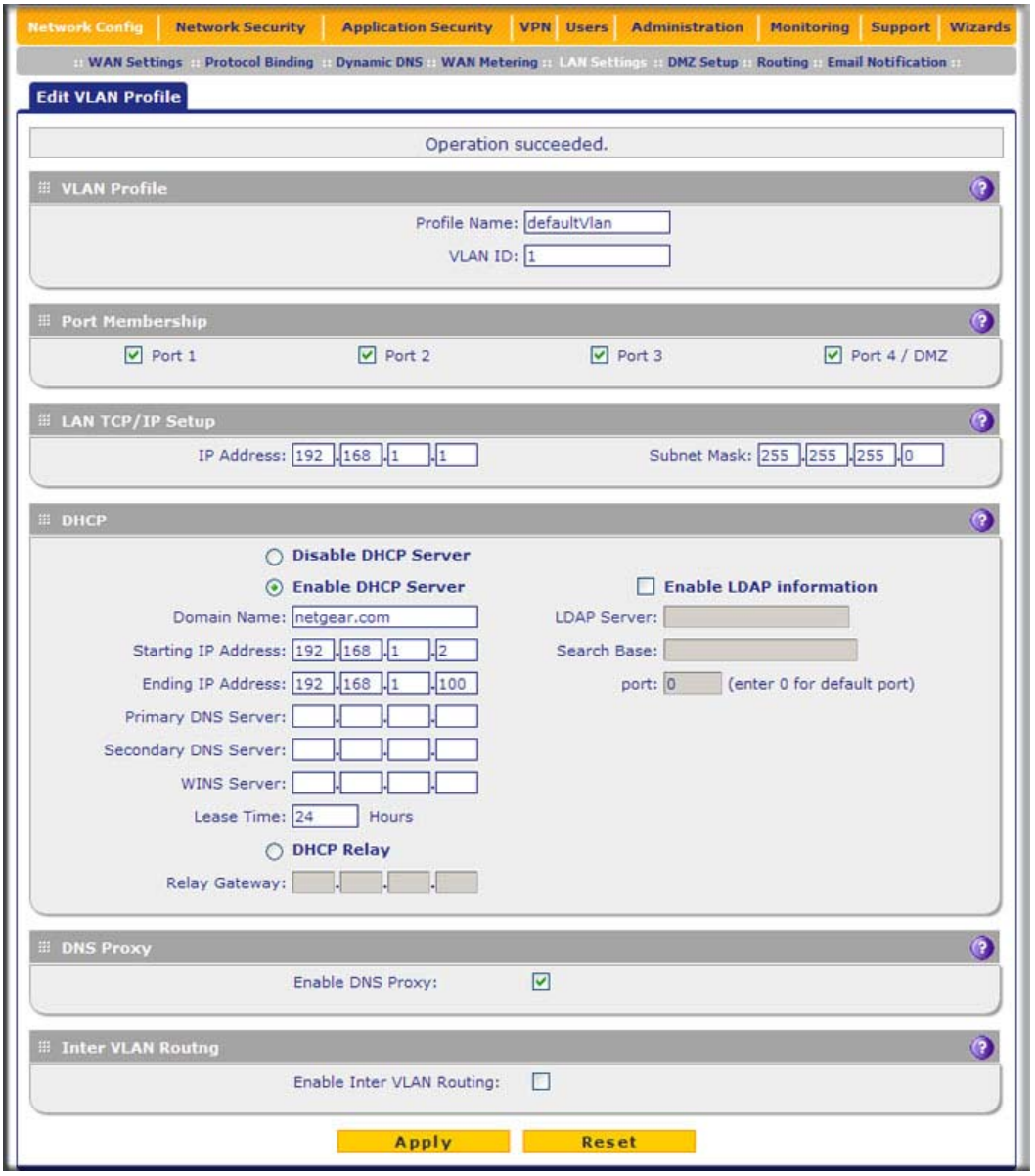


Figure 4-3

3. Enter the settings as explained in Table 4-1.

Table 4-1. VLAN Profile Settings

Setting	Description (or Subfield and 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 VLAN 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		
Port 1 Port 2 Port 3 Port 4 / DMZ	Select one, several, or all port checkboxes to make the port(s) member of this VLAN. **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 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 will be disconnected. You must then 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 must now 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. This is the default setting.	
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 is optional. Enter the domain name of the UTM.

Table 4-1. VLAN Profile Settings (continued)

Setting	Description (or Subfield and Description)	
Enable DHCP Server (continued)	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 (the IP address in LAN TCP/IP section above).
	Primary DNS Server	This 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 is optional. If an IP address is specified, the UTM provides this address as the secondary DNS server IP address.
	WINS Server	This 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** checkbox to enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information. Enter the settings below. **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 e-mail security.	
	LDAP Server	The IP address or name of the LDAP server.

Table 4-1. VLAN Profile Settings (continued)

Setting	Description (or Subfield and Description)	
Enable LDAP information (continued)	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begin. You can specify multiple search object, 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 zero.
DNS Proxy		
Enable DNS Proxy	This 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 setting is disabled by default. **Note**: When you deselect the **Enable DNS Proxy** radio button, the UTM still services DNS requests that are sent to its LAN IP address unless you disable DNS Proxy in the firewall settings (see "Attack Checks" on page 5-27).	
Inter VLAN Routing		
Enable Inter VLAN Routing	This is optional. Select the **Enable Inter VLAN Routing** radio button to ensure that traffic is routed only to VLANs for which inter VLAN routing is enabled. This setting is disabled by default. When the **Enable Inter VLAN Routing** radio button is deselected, traffic from this VLAN is not routed to other VLANs, and traffic from other VLANs is not routed to this VLAN.	

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

Note: Once 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. To change these default traffic rules, see Chapter 5, "Firewall Protection."

Configuring Multi-Home 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 must be unique and must not 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 properly configured IP addresses on a dual-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** from the menu. The LAN Settings submenu tabs appear, with the LAN Setup screen in view.
2. Click the **LAN Multi-homing** submenu tab. The LAN Multi-homing screen displays.

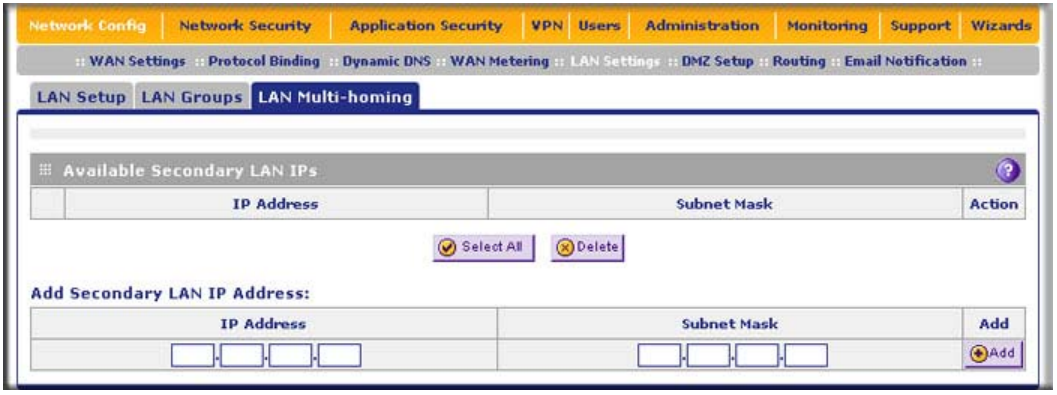


Figure 4-4

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

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

   Repeat step 3 and step 4 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 must be manually configured with the IP addresses, gateway IP address and DNS server IP addresses.

Managing Groups and Hosts (LAN Groups)

The Known PCs and Devices table on the LAN Groups screen (see Figure 4-5 on page 4-14) 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.

Some advantages of the Network Database are:

- Generally, you do not need to enter either IP address or MAC addresses. 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 PCs. 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 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 "Managing the Network Database" on this page) and apply restrictions (outbound rules and inbound rules) to each group (see "Using Rules to Block or Allow Specific Kinds of Traffic" on page 5-3).
  - 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 "Setting Web Access Exceptions and Scanning Exclusions" on page 6-41).
  - If necessary, you can also create firewall rules to apply to a single PC (see "Enabling Source MAC Filtering" on page 5-42). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.

Managing the Network Database

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

To view the Network Database:

1. Select **Network Config** > **LAN Settings** from the menu. The LAN Settings submenu tabs appear, with the LAN Setup screen in view.
2. Click the **LAN Groups** submenu tab. The LAN Groups screen displays (see Figure 4-5 on page 4-14, which shows some examples in the Known PCs and Devices table).

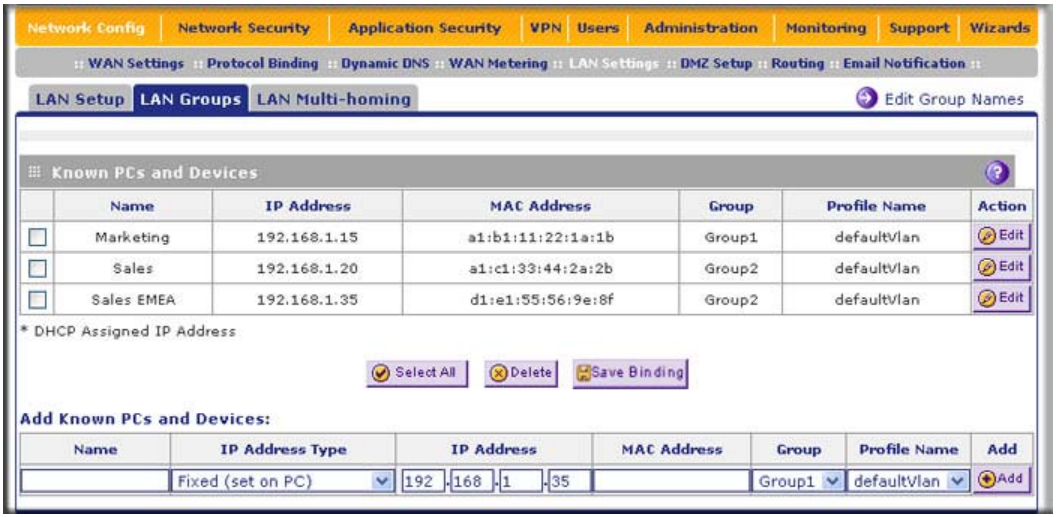


Figure 4-5

The Known PCs and Devices table lists the entries in the Network Database. For each PC or device, the following fields are displayed:

- **Checkbox**. 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 pull-down menu in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen.
- **Action**. The Edit table button that provides access to the Edit Groups and Hosts screen.

Adding 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 Figure 4-5 on page 4-14), enter the settings as explained in Table 4-2.

Table 4-2. Add Known PCs and Devices Settings

Setting	Description (or Subfield and Description)
Name	Enter the name of the PC or device.
IP Address Type	From the pull-down menu, select how the PC or device receives it 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 "Setting Up Address Reservation" on page 4-17). **Note**: When assigning a reserved IP address to a client, the IP address selected must be outside the range of addresses allocated to the DHCP server pool.
IP Address	Enter the IP address that this PC or device is assigned in the IP Address field. 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 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 pull-down menu, select the group to which the PC or device is assigned. (Group 1 is the default group.)
Profile Name	From the pull-down menu, select the VLAN profile to which the PC or device is assigned. (The 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 checkbox for the table entry and click **Save Binding** to bind the IP address to the MAC address for DHCP assignment.

Editing 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 Figure 4-5 on page 4-14), click the **Edit** table button of a table entry. The Edit Groups and Hosts screen displays (see Figure 4-6, which contains some examples).

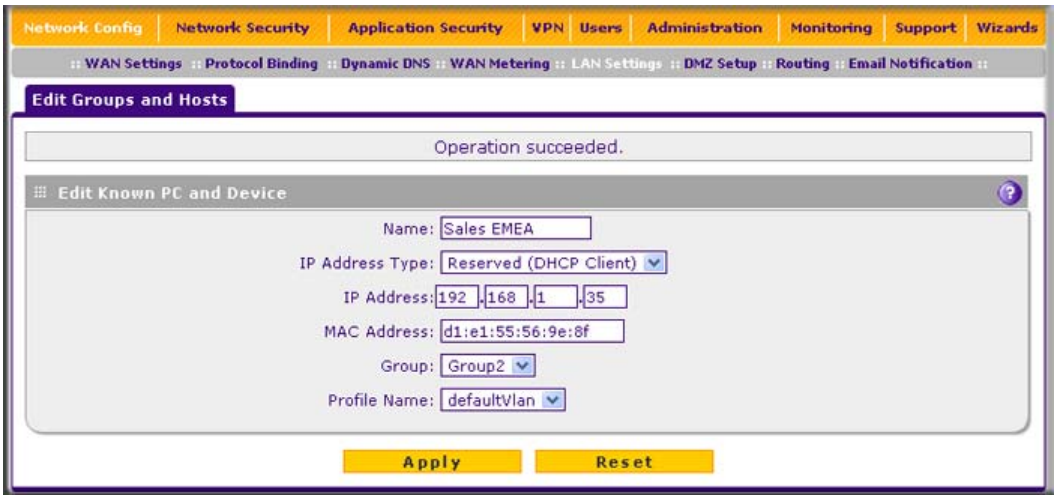


Figure 4-6

2. In the Edit Known PC and Device section, specify the fields and make selections from the pull-down menus as explained in step 1 of the previous section (“Adding PCs or Devices to the Network Database” on page 4-15).
3. Click **Apply** to save your settings in the Known PCs and Devices table.

Changing 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 Settings** from the menu. The LAN Settings submenu tabs appear, with the LAN Setup screen in view.
2. Click the **LAN Groups** submenu tab. The LAN Groups screen displays (see Figure 4-5 on page 4-14, which shows some examples in the Known PCs and Devices table).

3. Click the **Edit Group Names** option arrow at the right of the LAN submenu tabs. The Network Database Group Names screen displays. (Figure 4-7 shows some examples.)

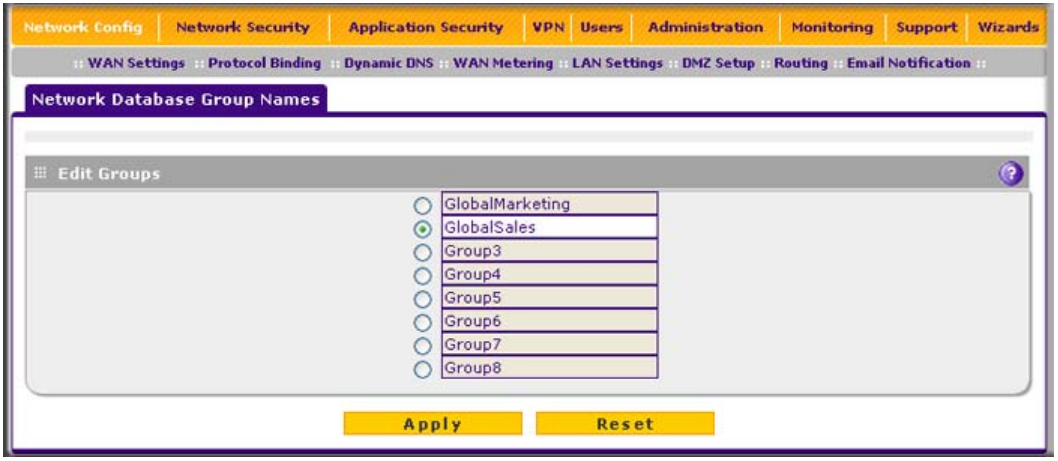


Figure 4-7

4. Select the radio button next to any group name to enable editing.
5. Type a new name in the field. The maximum number of characters is 15; spaces and double quotes (") are not allowed.
6. Repeat step 4 and step 5 for any other group names.
7. Click **Apply** to save your settings.

Setting 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 must be outside of the DHCP server pool.

To reserve an IP address, select **Reserved (DHCP Client)** from the IP Address Type pull-down menu on the LAN Groups screen as described in "Adding PCs or Devices to the Network Database" on page 4-15 or on the Edit Groups and Hosts screen as described in "Editing PCs or Devices in the Network Database" on page 4-16.

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.

Configuring and Enabling the DMZ Port

The De-Militarized 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 e-mail server) and provide public access to them. The fourth LAN port on the UTM (the rightmost LAN port) can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN. 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 properly with them, but there are other applications that might not function well. In some cases, local PCs can run the application properly if those PCs are used on the DMZ port.

Note: A separate firewall security profile is provided for the DMZ port that is hardware-independent of the standard firewall security 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, see "Front Panel" on page 1-10) 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** from the menu. The DMZ Setup screen displays.

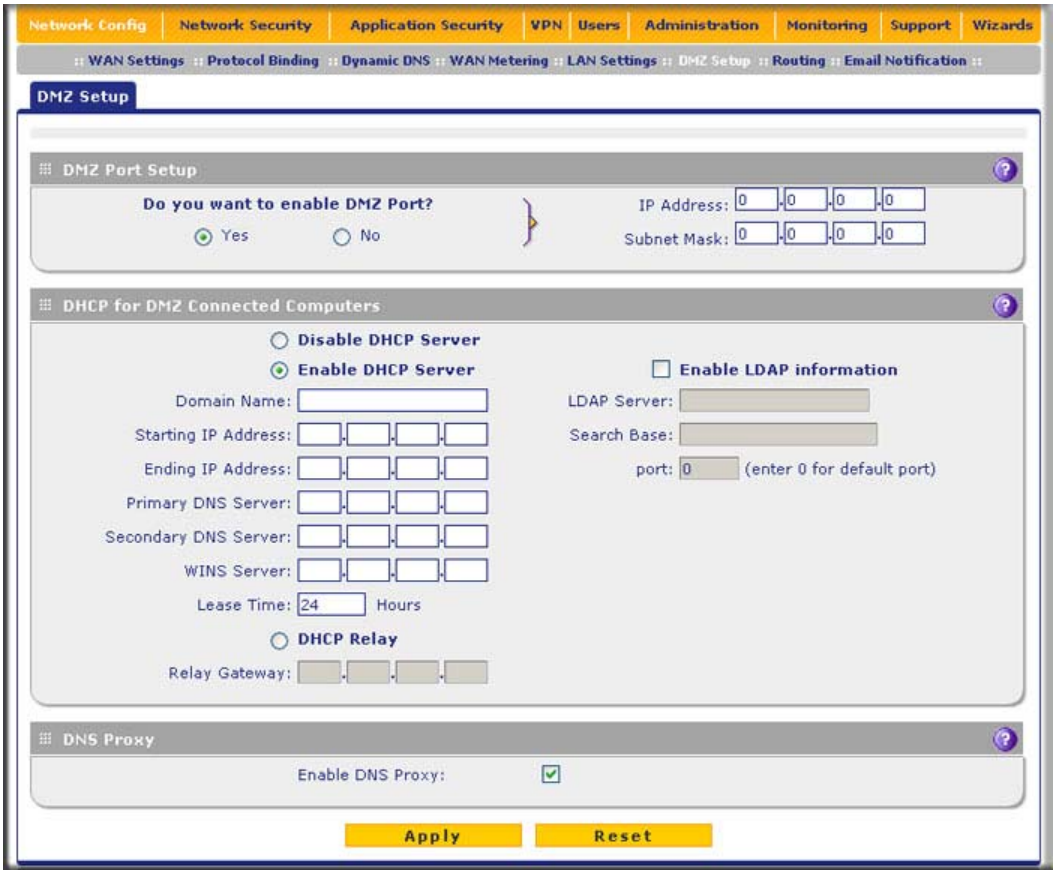


Figure 4-8

2. Enter the settings as explained in Table 4-3 on page 4-20.

Table 4-3. DMZ Setup Settings

Setting	Description (or Subfield and 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. Enter the IP address and Subnet Mask fields (see below). • **No**. Allows 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.
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. This is the default setting.	
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 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 (the IP address in LAN TCP/IP section above).

Table 4-3. DMZ Setup Settings (continued)

Setting	Description (or Subfield and Description)	
Enable DHCP Server (continued)	Primary DNS Server	This 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 is optional. If an IP address is specified, the UTM provides this address as the secondary DNS server IP address.
	WINS Server	This is optional. Enter a WINS server IP address to specify the Windows NetBios Server IP if one is present in your network.
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses is 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** checkbox to enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information. Enter the following settings:	
	LDAP Server	The IP address or name of the LDAP sever.
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begin. You can specify multiple search object, 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 in 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 zero.

Table 4-3. DMZ Setup Settings (continued)

Setting	Description (or Subfield and Description)
DNS Proxy	
Enable DNS Proxy	This 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 setting is enabled by default. **Note**: The UTM still services DNS requests sent to its LAN IP address unless you disable DNS Proxy in the firewall settings (see "Attack Checks" on page 5-27).

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

Note: The DMZ LED next to LAN port 4 (see "Front Panel" on page 1-10) lights green to indicate that the DMZ port is enabled.

To define the DMZ WAN Rules and LAN DMZ Rules, see "Setting DMZ WAN Rules" on page 5-15 and "Setting LAN DMZ Rules" on page 5-19, respectively.

Managing Routing

Static Routes provide additional routing information to your UTM. Under normal circumstances, the 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 automatically sets up routes between VLANs and secondary IP addresses that you have configured on the LAN Multi-homing screen (see "Configuring Multi-Home LAN IPs on the Default VLAN" on page 4-11). Therefore, you do not need to manually add a static route between a VLAN and a secondary IP address.

Configuring Static Routes

To add a static route to the Static Route table:

1. Select **Network Config** > **Routing** from the menu. The Routing screen displays.

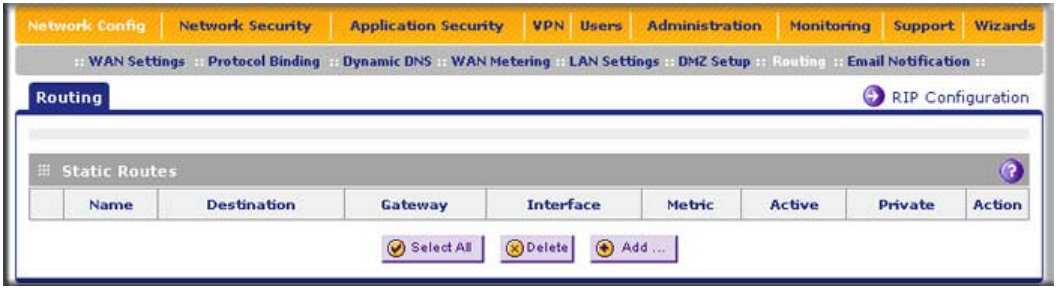


Figure 4-9

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

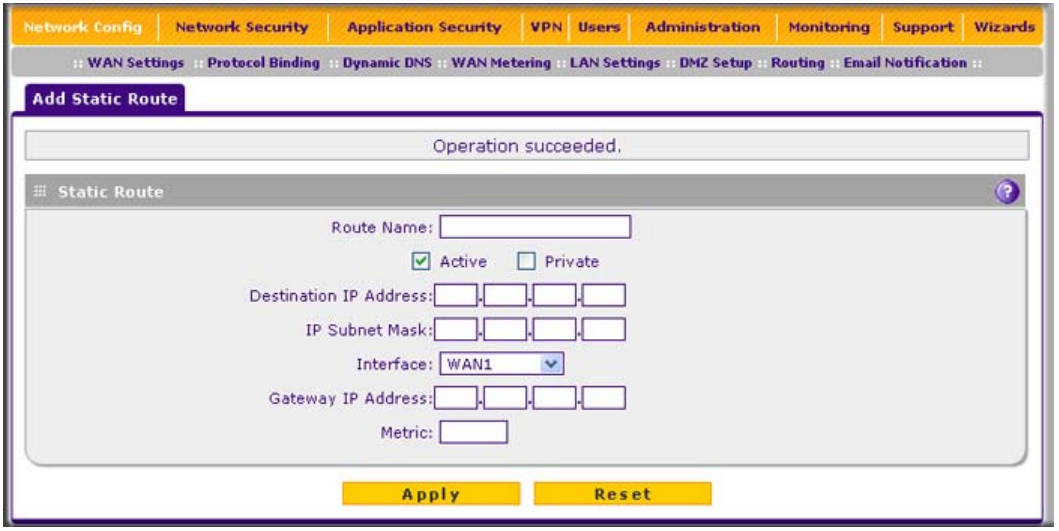


Figure 4-10

3. Enter the settings as explained in Table 4-4.

Table 4-4. Static Route Settings

Setting	Description (or Subfield and 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** checkbox. **Note**: A route can be added to the table and made inactive, if not needed. This allows routes to be used 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** checkbox. Doing so prevents the static route from being advertised in RIP.
Destination IP Address	The destination IP address to the host or network to which the route leads.
IP Subnet Mask	The IP subnet mask to the host or network to which the route leads. If the destination is a single host, enter 255.255.255.255.
Interface	From the pull-down menu, select the interface that is the physical network interface (WAN1, WAN2, LAN, or DMZ for the dual-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 Route table.

To edit a static route that is in the Static Route table:

1. Select its entry from the table and click the **Edit** table button in the Action column. The Edit Static Route screen displays. This screen is identical to the Add Static Route screen that is described above with the exception that you cannot change the name of the static route.
2. Enter the settings as explained in Table 4-4.
3. Click **Apply** to save your settings.

Configuring Routing Information Protocol (RIP)

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 Configuration** > **Routing** from the menu.
2. Click the **RIP Configuration** option arrow at the right of the Routing submenu tab. The **RIP Configuration** screen displays.

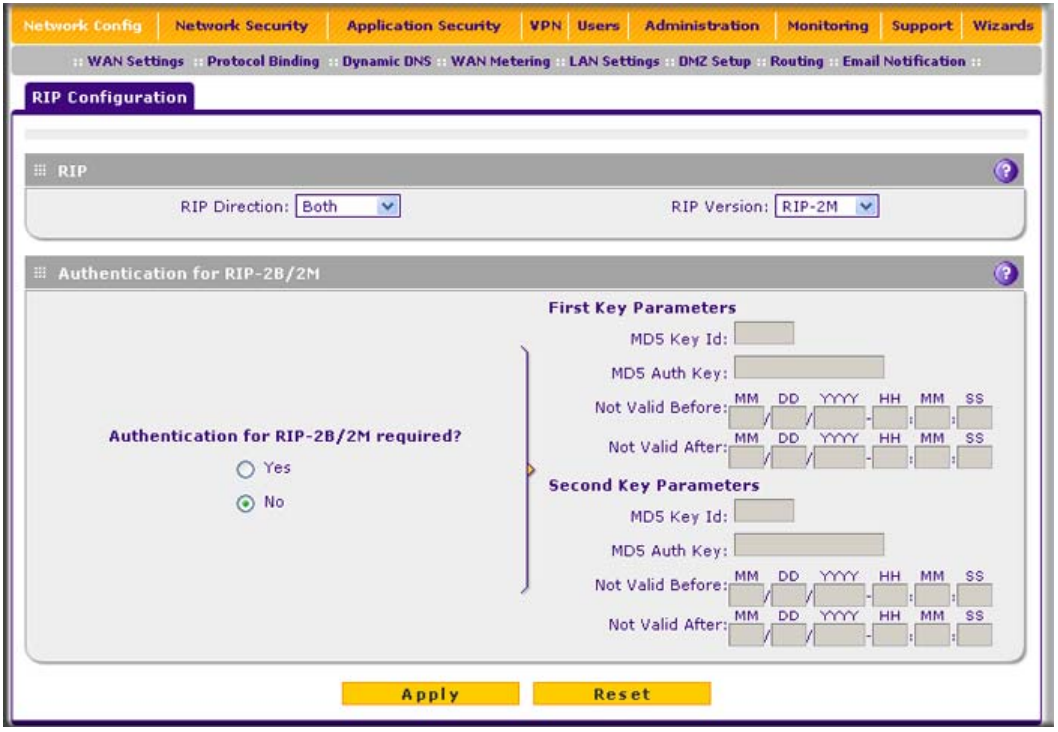


Figure 4-11

3. Enter the settings as explained in Table 4-5 on page 4-26.

Table 4-5. RIP Configuration Settings

Setting	Description (or Subfield and Description)	
RIP		
RIP Direction	From the RIP Direction pull-down menu, select the direction in which the UTM sends and receives RIP packets: • **None**. The neither advertises its route table nor does it accept any RIP packets from other routers. This effectively disables RIP. • **In Only**. The accepts RIP information from other routers but does not advertises its routing table. • **Out Only**. The advertises its routing table but does not accept RIP information from other routers. • **Both**. The advertises its routing table and also processes RIP information received from other routers.	
RIP Version	From the RIP Version pull-down menu, 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 fields below.	
	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 4-5. RIP Configuration Settings (continued)

Setting	Description (or Subfield and 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 is 192.168.1.100.
- The UTM connects to a remote network where you must 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 must 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 must be defined as follows:

- The destination IP address and IP subnet mask must specify that the static route applies to all 134.177.x.x IP addresses.
- The gateway IP address must 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.

Chapter 5
Firewall Protection

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

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. To set up LAN Groups, see "Managing Groups and Hosts (LAN Groups)" on page 4-12.

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 Internet sharing 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 “Configuring VPN Authentication Domains, Groups, and Users” on page 9-1 and “Configuring Remote Management Access” on page 10-12).
2. Although rules (see “Using Rules to Block or Allow Specific Kinds of Traffic” on page 5-3) is the basic way of managing the traffic through your system, you can further refine your control using the following features and capabilities of the UTM:
   - Groups and hosts (see “Managing Groups and Hosts (LAN Groups)” on page 4-12)
   - Services (see “Services-Based Rules” on page 5-3)
   - Schedules (see “Setting a Schedule to Block or Allow Specific Traffic” on page 5-41)
   - Allow or block sites and applications (see “Setting Web Access Exception Rules” on page 6-41)
   - Source MAC filtering (see “Enabling Source MAC Filtering” on page 5-42)
   - Port triggering (see “Configuring Port Triggering” on page 5-46)
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 10-1.
5. You can monitor blocked content and malware threats in real-time. For more information, see “Monitoring Real-Time Traffic, Security, and Statistics” on page 11-14.
6. The firewall logs can be configured to log and then e-mail denial of access, general attack information, and other information to a specified e-mail address. For information about how to configure logging and notifications, see “Configuring Logging, Alerts, and Event Notifications” on page 11-5.

Using 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 5-1. 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

Services-Based Rules

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

- **Outbound Rules (service blocking)**. Outbound traffic is normally allowed unless the firewall is configured to disallow it.
- **Inbound Rules (port forwarding)**. Inbound traffic is normally 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 default list. These added services can then have rules defined for them to either allow or block that traffic (see "Adding Customized Services" on page 5-32).

- **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 “Creating Quality of Service (QoS) Profiles” on page 5-35).

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 “Enabling Source MAC Filtering” on page 5-42 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. Only enable those ports that are necessary for your network.

Table 5-2 on page 5-5 describes the fields that define the rules for outbound traffic and that are common to most Outbound Service screens (see Figure 5-3 on page 5-14, Figure 5-6 on page 5-17, and Figure 5-9 on page 5-20).

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

- “Setting LAN WAN Rules” on page 5-12
- “Setting DMZ WAN Rules” on page 5-15
- “Setting LAN DMZ Rules” on page 5-19.

Table 5-2. Outbound Rules Overview

Setting	Description (or Subfield and Description)
Service	The service or application to be covered by this rule. If the service or application does not appear in the list, you must define it using the Services menu (see “Adding Customized Services” on page 5-32).
Action (Filter)	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. ALLOW rules are only useful 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 pull-down menu 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 “Setting a Schedule to Block or Allow Specific Traffic” on page 5-41).
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 to apply the rule to a single device on your LAN. • Address range. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices. • Groups. Select the Group to which the rule applies. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See “Managing Groups and Hosts (LAN Groups)” on page 4-12.
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 Start and Finish fields.
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 to apply the rule to a single PC on the DMZ network. • Address range. Enter the required addresses in the Start and Finish fields to apply the rule to a range of DMZ computers.

Table 5-2. Outbound Rules Overview (continued)

Setting	Description (or Subfield and Description)
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 "Creating Quality of Service (QoS) Profiles" on page 5-35. **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 non-blocking inbound or outbound firewall rule.
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. Bandwidth limiting occurs in the following ways: • For outbound traffic: on the available WAN interface in the single WAN port 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.
Log	The settings 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 debugging your rules. • Never. Never log traffic considered by this rule, whether it matches or not.
NAT IP	The settings that specify 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. The options are: • WAN Interface Address: All the outgoing packets on the WAN are to the address of the assigned WAN interface. • Single Address: All the outgoing packets on the WAN are assigned the specified IP address, for example, a secondary WAN address that you have configured. **Note**: This 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 address any of your local computers. 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 PCs 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 "Configuring Dynamic DNS" on page 3-19).
- 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 menu to keep the PC's IP address constant (see "Setting Up Address Reservation" on page 4-17).
- Local PCs must 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 "Configuring Port Triggering" on page 5-46 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). For example, multiple concurrent connections of the same application from one host or IP addresses (such as multiple DNS queries from one PC) triggers the UTM's DoS protection. For more information about protecting the UTM from incoming threats, see "Using the Intrusion Prevention System" on page 5-49.

Table 5-3 on page 5-8 describes the fields that define the rules for inbound traffic and that are common to most Inbound Service screens (see Figure 5-4 on page 5-15, Figure 5-7 on page 5-18 and Figure 5-10 on page 5-21).

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

- "Setting LAN WAN Rules" on page 5-12
- "Setting DMZ WAN Rules" on page 5-15
- "Setting LAN DMZ Rules" on page 5-19

Table 5-3. Inbound Rules Overview

Setting	Description (or Subfield and Description)
Service	The service or application to be covered by this rule. If the service or application does not appear in the list, you must define it using the Services menu (see "Adding Customized Services" on page 5-32).
Action (Filter)	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.
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This pull-down menu 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 "Setting a Schedule to Block or Allow Specific Traffic" on page 5-41).
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.)
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	You can enable this setting and specify a port number if you want to assign the LAN server or DMZ server to a specific port.
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 dual-WAN port models, it can either be the address of the WAN1 or WAN2 interface or another public IP address (when you have a secondary WAN address configured). On the single-WAN port models, it can either be the address of the single WAN interface or another public IP address (when you have a secondary WAN address configured).

Table 5-3. Inbound Rules Overview (continued)

Setting	Description (or Subfield and Description)
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 to apply the rule to a single device on your LAN. • Address range. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices. • Groups. Select the Group to which the rule applies. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See “Managing Groups and Hosts (LAN Groups)” on page 4-12. **Note**: This field is not applicable to inbound LAN WAN rules.
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 Start and Finish fields.
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 to apply the rule to a single PC on the DMZ network. • Address range. Enter the required addresses in the Start and Finish fields to apply the rule to a range of DMZ computers. **Note**: This field is not applicable to inbound DMZ WAN rules.
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 “Creating Quality of Service (QoS) Profiles” on page 5-35. **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 non-blocking inbound or outbound firewall rule.

Table 5-3. Inbound Rules Overview (continued)

Setting	Description (or Subfield and Description)
Log	The settings 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 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. Bandwidth limiting occurs in the following ways: • For outbound traffic: on the available WAN interface in the single WAN port 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 services at your location. If you are unsure, see the Acceptable Use Policy of your ISP.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules screen as the last item in the list, as shown in the LAN WAN Rules screen example in Figure 5-1.

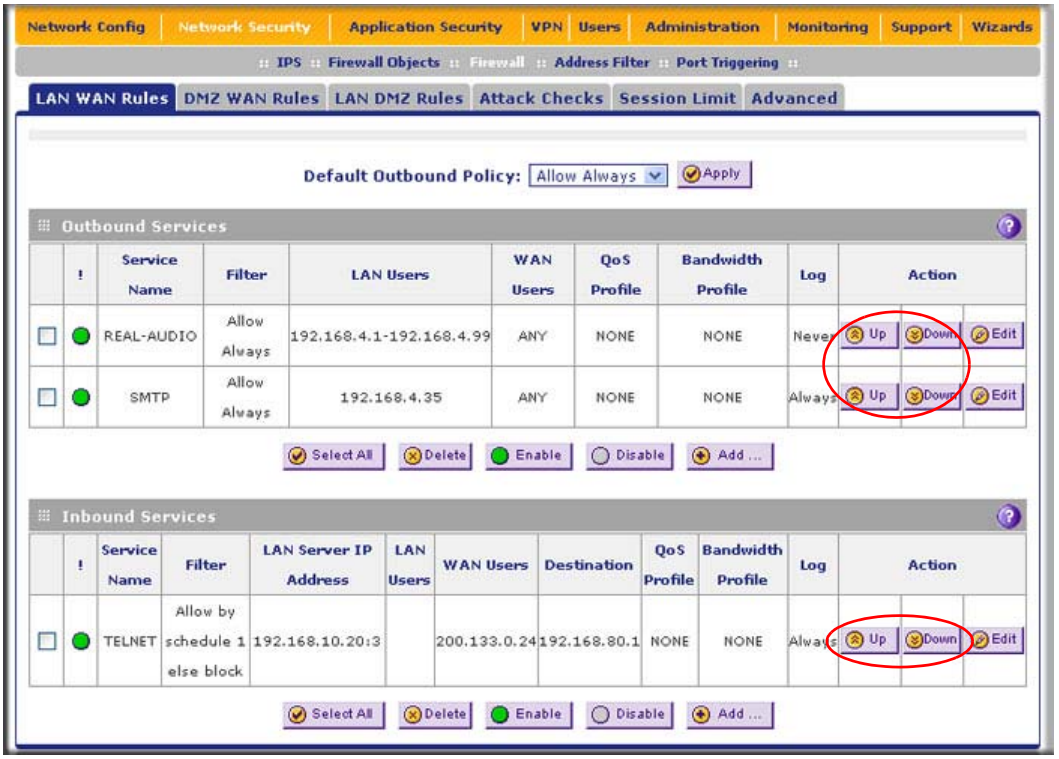


Figure 5-1

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 allows you to relocate a defined rule to a new position in the table.

Setting 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** from the menu. The Firewall submenu tabs appear, with the LAN WAN Rules screen in view.
2. Next to Default Outbound Policy, select **Block Always** from the pull-down menu.
3. Next to the pull-down menu, click the **Apply** table button.

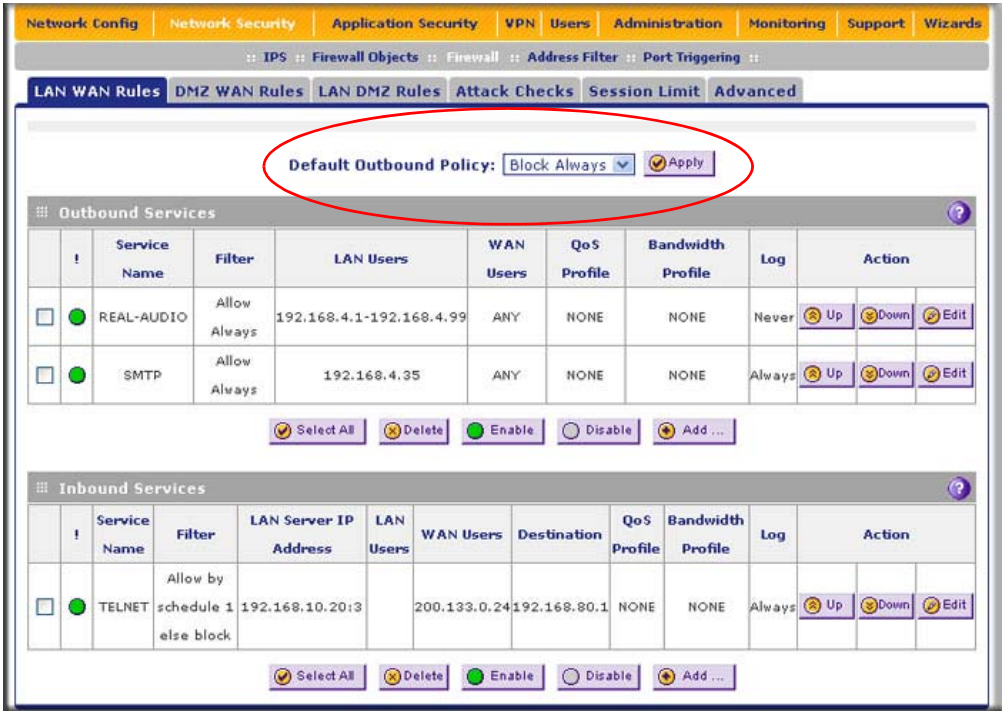


Figure 5-2

To make changes to an existing outbound or inbound service rule, in the Action column to the right of to the rule, click on 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 WAN Outbound Service screen (identical to Figure 5-3 on page 5-14) or Edit LAN WAN Inbound Service screen (identical to Figure 5-4 on page 5-15) 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 checkbox to the left of the 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:
   - **Enable**. Enables the rule or rules. The "!" status icon changes from a grey circle to a green circle, indicating that the rule is 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 grey circle, indicating that the rule is or rules are disabled.
   - **Delete**. Deletes the rule or rules.

LAN WAN Outbound Services 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 may block or allow traffic between an internal IP LAN address and any external WAN IP address according to the schedule created in the Schedule menu.

You can also tailor these rules to your specific needs (see "Administrator Tips" on page 5-2).

	**Note:** This feature is for advanced administrators only! 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.

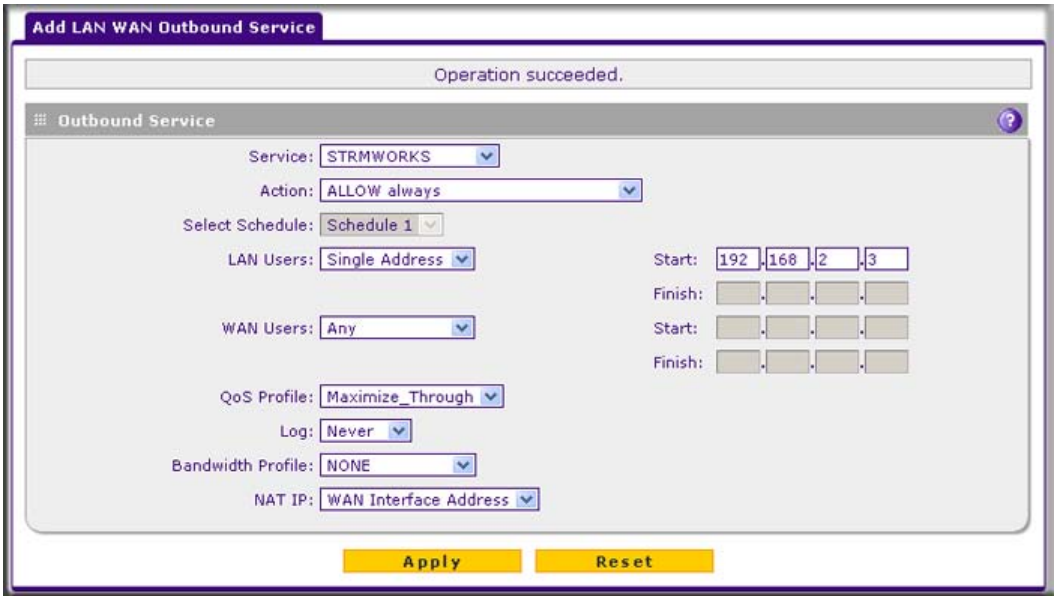


Figure 5-3

2. Enter the settings as explained in Table 5-2 on page 5-5.
3. Click **Apply** to save your changes. The new rule is now added to the Outbound Services table.

LAN WAN Inbound Services 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. Only enable 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.

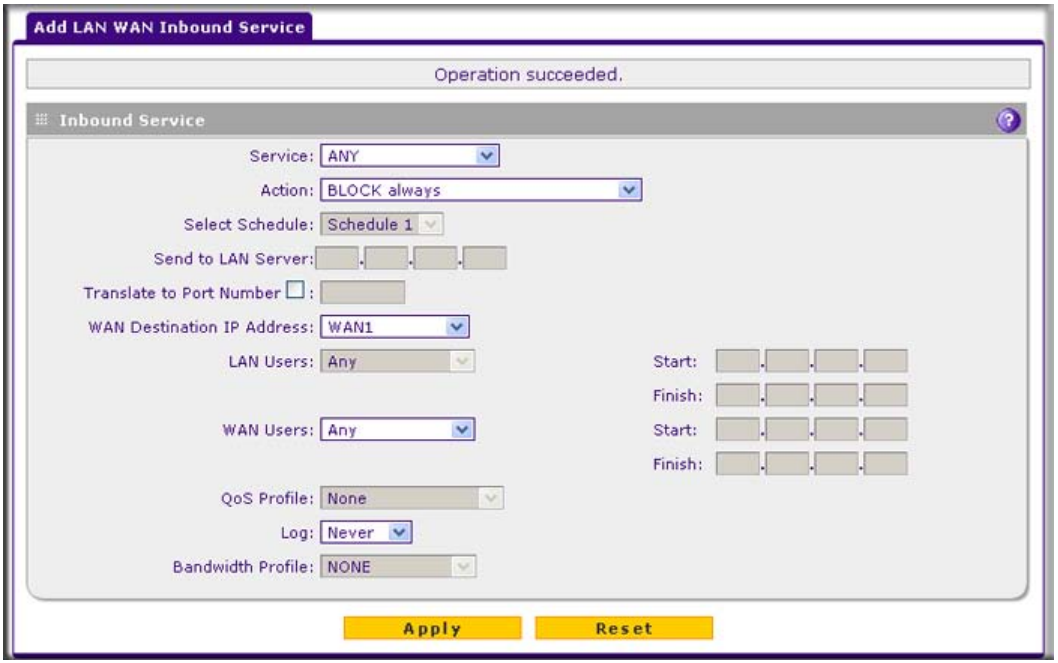


Figure 5-4

2. Enter the settings as explained in Table 5-3 on page 5-8.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Setting 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 allow all traffic from and to the Internet to pass through. You can then apply firewall rules to block specific types of traffic from either going out from the DMZ to the Internet (outbound) or coming in from the Internet to the DMZ (inbound).

There is no pull-down menu 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 blocking all outbound traffic and then enabling only specific services to pass through the UTM. You do so by adding outbound services rules (see “DMZ WAN Outbound Services Rules” on page 5-17).

To access the DMZ WAN Rules screen:

1. Select **Network Security** > **Firewall** from the menu. The Firewall submenu tabs appear.
2. Click the **DMZ WAN Rules** submenu tab. The DMZ WAN Rules screen displays. (Figure 5-5 shows a rule in the Outbound Services table as an example).

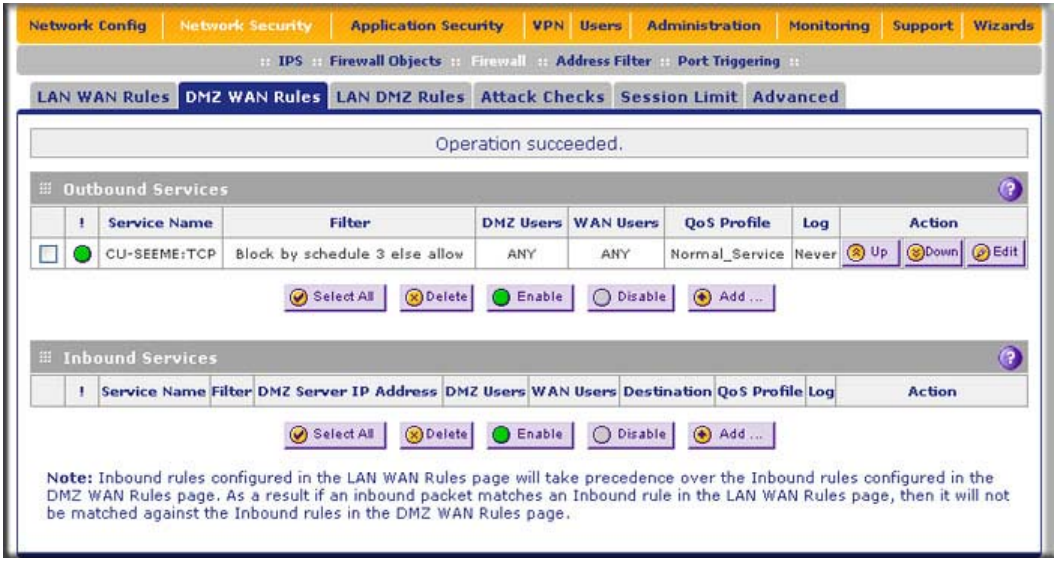


Figure 5-5

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

In the Action column to the right of to the rule, click on 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 DMZ WAN Outbound Service screen (identical to Figure 5-6 on page 5-17) or Edit DMZ WAN Inbound Service screen (identical to Figure 5-7 on page 5-18) 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 checkbox to the left of the 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 grey circle, indicating that the rule is or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Delete**. Deletes the rule or rules.

DMZ WAN Outbound Services Rules

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

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.

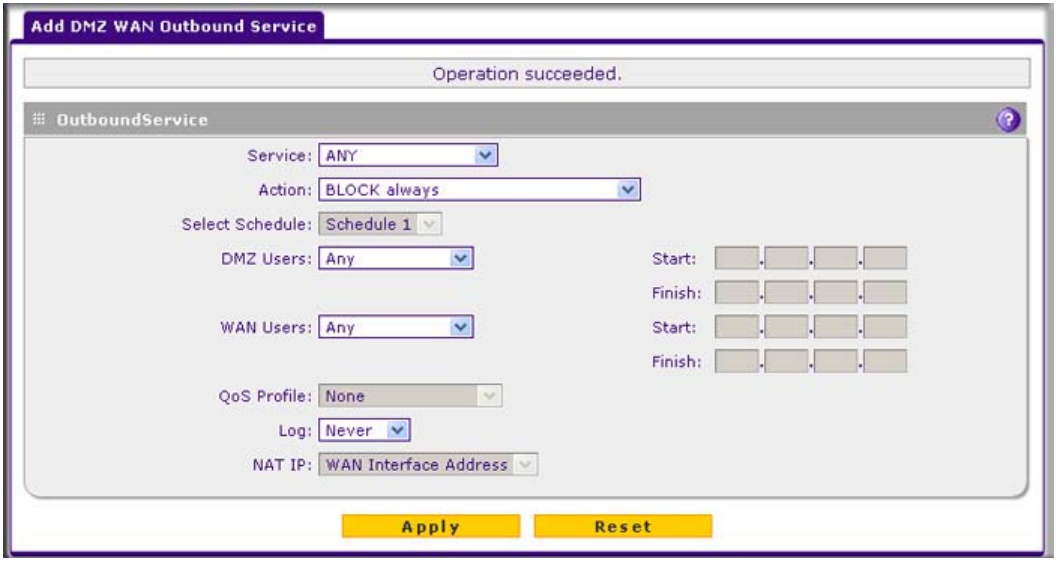


Figure 5-6

2. Enter the settings as explained in Table 5-2 on page 5-5.
3. Click **Apply.** The new rule is now added to the Outbound Services table. The rule is automatically enabled.

DMZ WAN Inbound Services 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 allowed.

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.

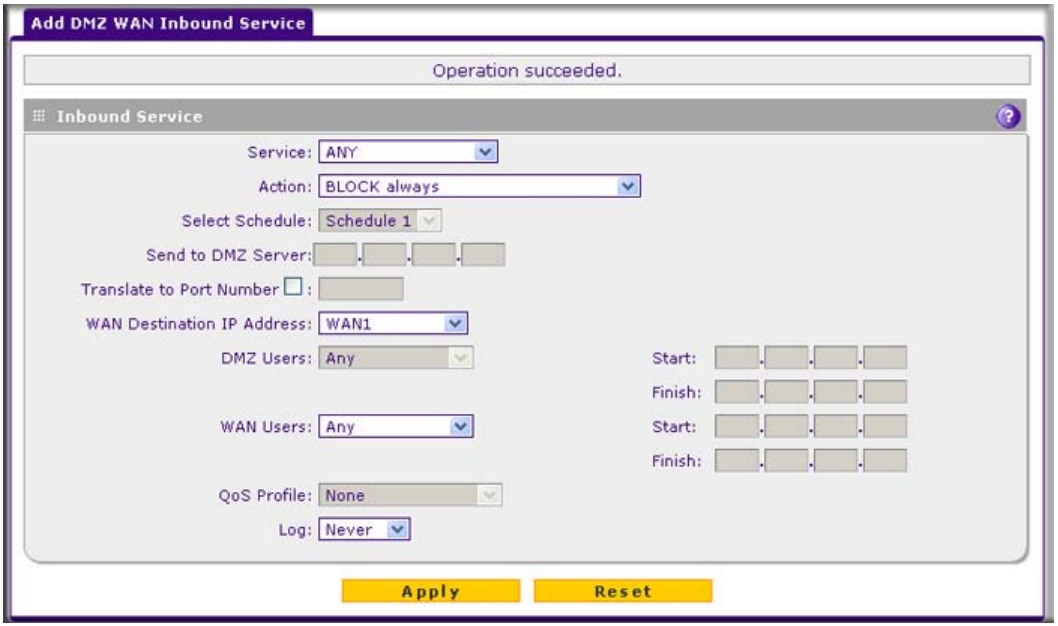


Figure 5-7

2. Enter the settings as explained in Table 5-3 on page 5-8.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Setting 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 allow all traffic between the local LAN and DMZ network. You can then apply firewall rules to block specific types of traffic from either going out from the LAN to the DMZ (outbound) or coming in from the DMZ to the LAN (inbound).

There is no pull-down menu 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 blocking all outbound traffic and then enabling only specific services to pass through the UTM. You do so by adding outbound services rules (see "LAN DMZ Outbound Services Rules" on page 5-20).

To access the LAN DMZ Rules screen:

1. Select **Network Security** > **Firewall** from the menu. The Firewall submenu tabs appear.
2. Click the **LAN DMZ Rules** submenu tab. The LAN DMZ Rules screen displays.

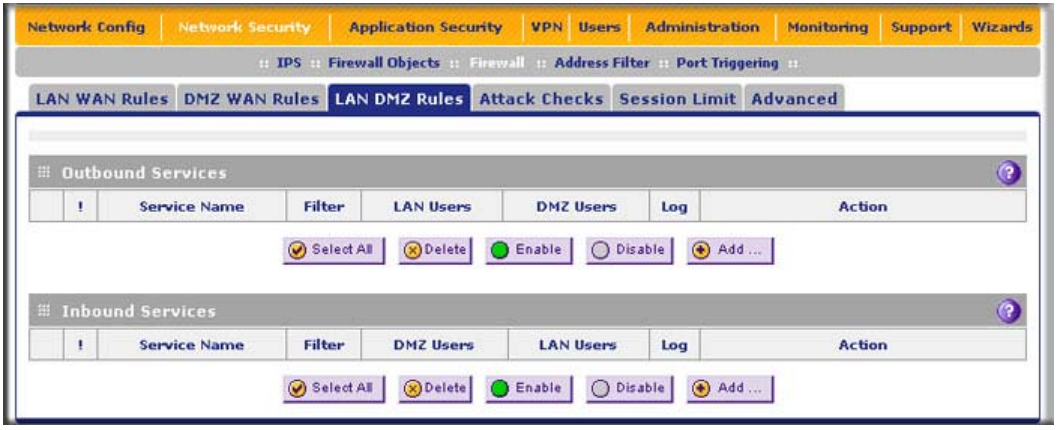


Figure 5-8

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

In the Action column to the right of to the rule, click on 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 5-9 on page 5-20) or Edit LAN DMZ Inbound Service screen (identical to Figure 5-10 on page 5-21) 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 checkbox to the left of the 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 grey circle, indicating that the rule is or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Delete**. Deletes the rule or rules.

LAN DMZ Outbound Services Rules

You may 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 may block or allow traffic between the DMZ and any internal LAN IP address according to the schedule created in the Schedule menu.

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.

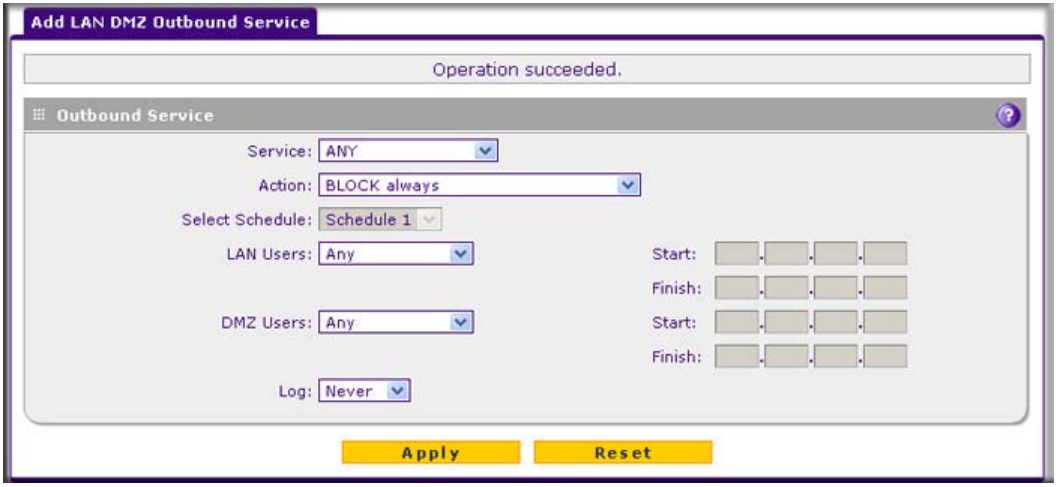


Figure 5-9

2. Enter the settings as explained in Table 5-2 on page 5-5.
3. Click **Apply.** The new rule is now added to the Outbound Services table. The rule is automatically enabled.

LAN DMZ Inbound Services 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 allowed.

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 5-10

2. Enter the settings as explained in Table 5-3 on page 5-8.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Inbound Rules Examples

LAN WAN Inbound Rule: Hosting 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.

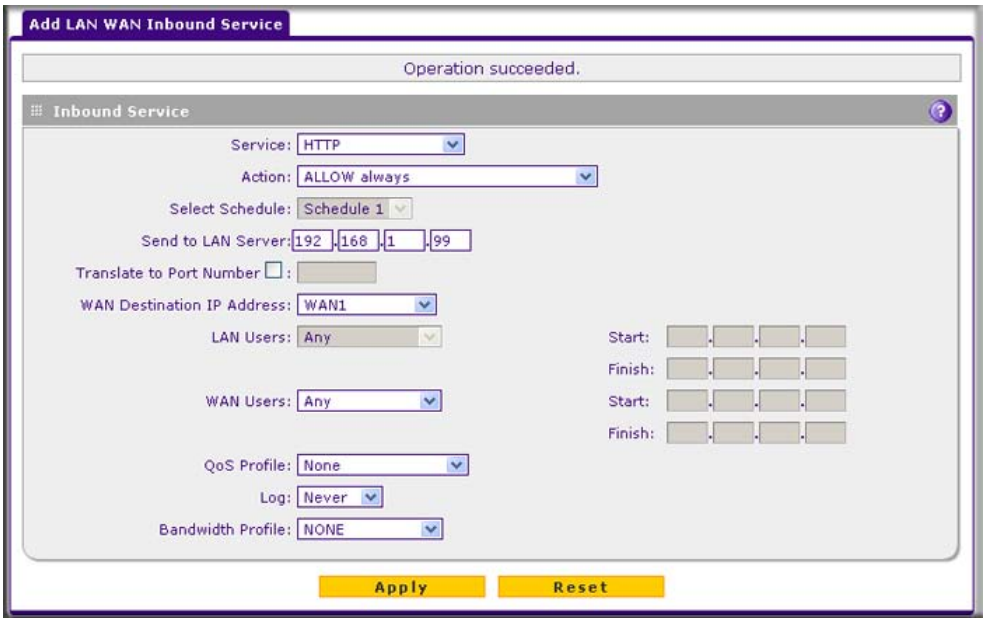


Figure 5-11

LAN WAN Inbound Rule: Allowing 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 Figure 5-11 on page 5-22). In the example, CU-SeeMe connections are allowed only from a specified range of external IP addresses.

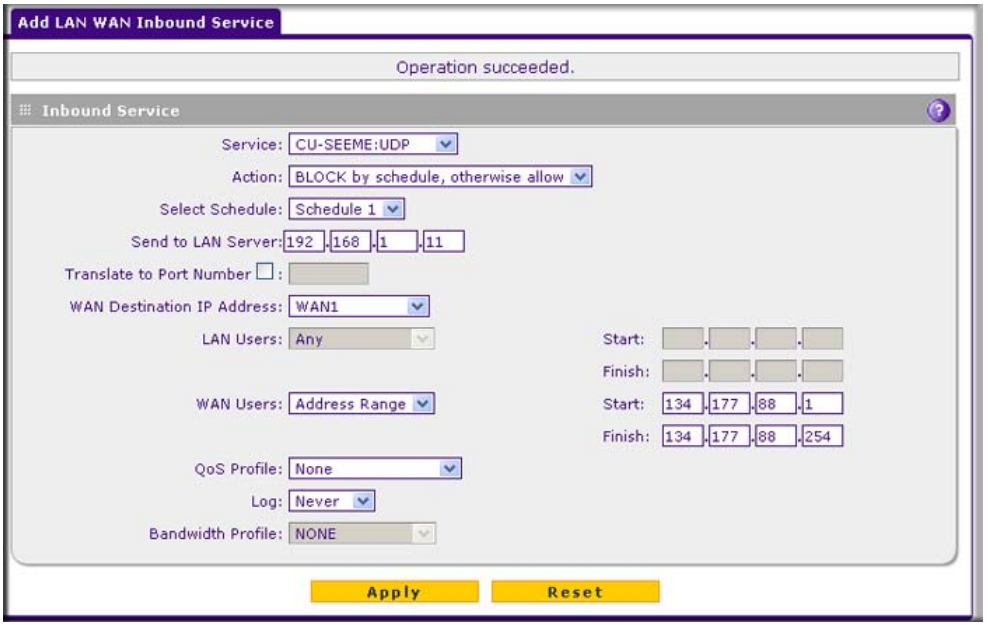


Figure 5-12

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

In this example, we will configure multi-NAT to support multiple public IP addresses on one WAN interface. By creating an inbound rule, we will configure 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:
  - WAN1 IP address (dual-WAN port models) or WAN IP address (single-WAN port models): 10.1.0.118
  - LAN IP address subnet: 192.168.1.1; subnet 255.255.255.0
  - DMZ IP address subnet: 192.168.10.1; 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** from the menu. The Firewall submenu tabs appear.
2. If your server is to be on your LAN, select the **LAN WAN Rules** submenu tab. (This is the screen we will use in this example).
   If your server is to be on your DMZ, select **DMZ WAN Rules** submenu tab.
3. Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays.

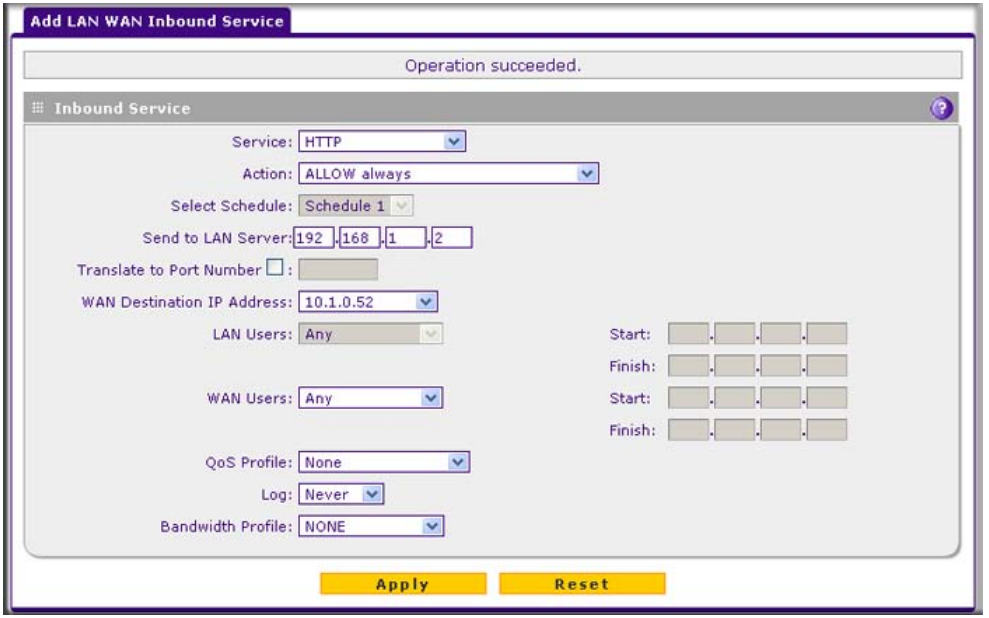


Figure 5-13

4. From the Service pull-down menu, select **HTTP** for a Web server.
5. From the Action pull-down menu, 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 dual-WAN port models only: from the WAN Destination IP Address pull-down menu, select the Web server (the simulated 10.1.0.52 address in this example) that you first must have defined on the WAN1 Secondary Addresses or WAN2 Secondary Addresses screen (see "Configuring Secondary WAN Addresses" on page 3-17).
   For the single-WAN port models, the WAN Destination IP Address is a fixed field.
8. Click **Apply** to save your settings. Your 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*>**, where **<*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: Specifying 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 Figure 5-14 on page 5-26..

	**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.

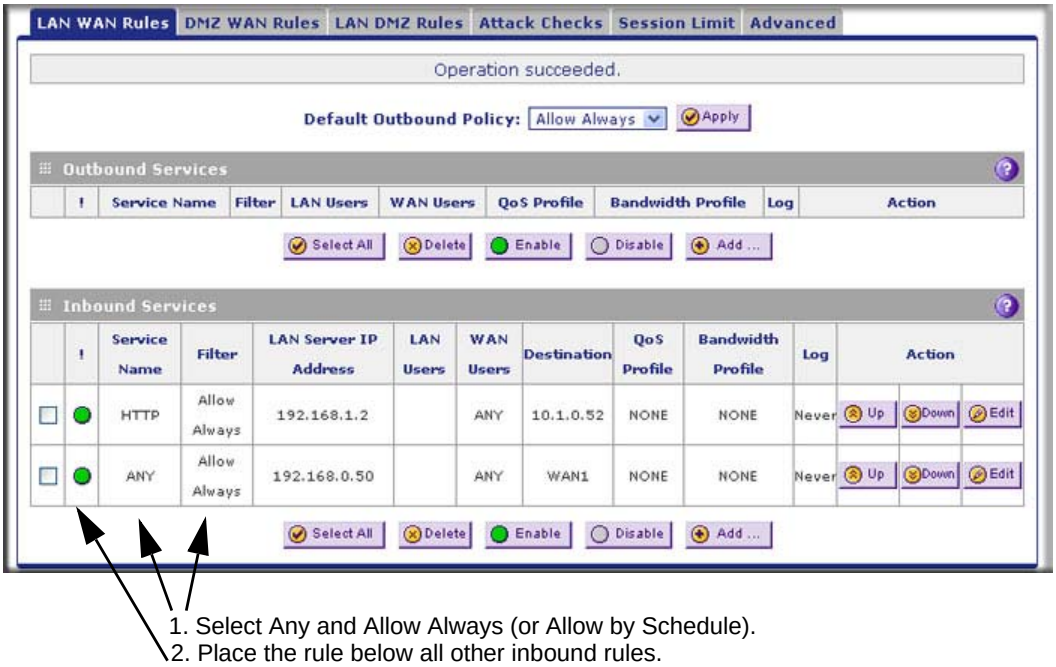


Figure 5-14

Outbound Rules Example

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

LAN WAN Outbound Rule: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. See an example in Figure 5-15 on page 5-27.

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

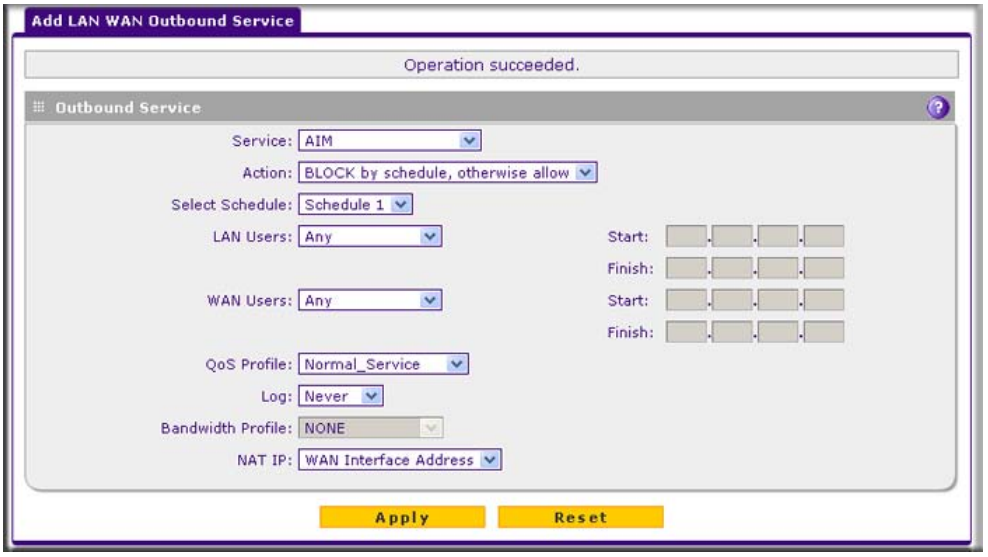


Figure 5-15

Configuring Other Firewall Features

You can configure attack checks, set session limits, and manage the Application Level Gateway (ALG) for SIP sessions.

Attack Checks

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. The various types of attack checks are listed on the Attack Checks screen and defined in Table 5-4 on page 5-28.

To enable the appropriate attack checks for your network environment:

1. Select **Network Security** > **Firewall** from the menu. The Firewall submenu tabs appear.

2. Click the **Attack Checks** submenu tab. The Attack Checks screen displays.

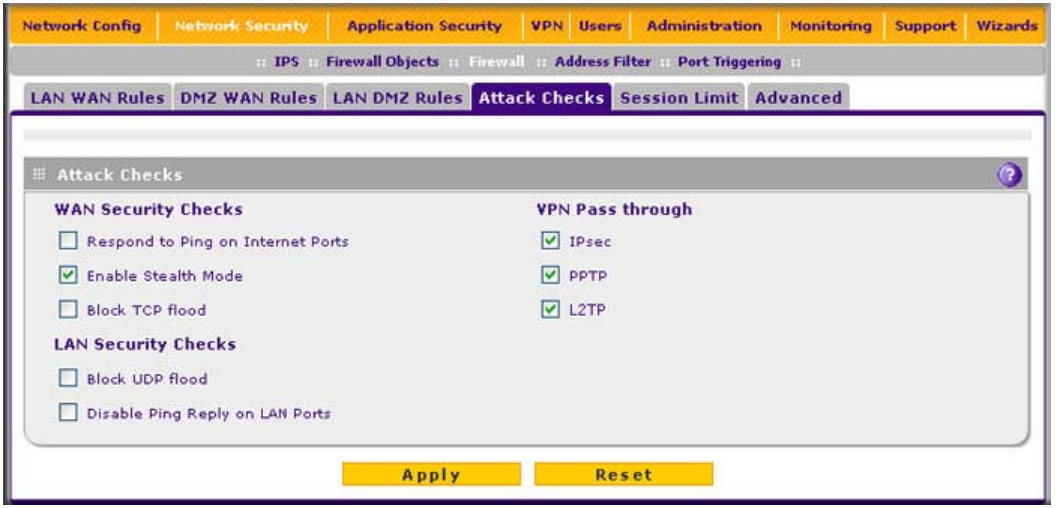


Figure 5-16

3. Enter the settings as explained in Table 5-4.

Table 5-4. Attack Checks Settings

Setting	Description (or Subfield and Description)
WAN Security Checks	
Respond To Ping On Internet Ports	Select the **Respond To Ping On Internet Ports** checkbox to enable the UTM to respond to a ping from the Internet. A ping can be used as a diagnostic tool. Keep this checkbox deselected 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** checkbox (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** checkbox 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 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** checkbox is deselected.

Table 5-4. Attack Checks Settings (continued)

Setting	Description (or Subfield and Description)
LAN Security Checks.	
Block UDP flood	Select the **Block UDP flood** checkbox to prevent the UTM from accepting more than 20 simultaneous, active UDP connections from a single device on the LAN. By default, the **Block UDP flood** checkbox is deselected. 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. Check for the application listening at that port. 2. See that no application is listening at that port. 3. Reply 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 him, thus making the attacker's network location anonymous.
Disable Ping Reply on LAN Ports	Select the **Disable Ping Reply on LAN Ports** checkbox to prevent the UTM from responding to a ping on a LAN port. A ping can be used as a diagnostic tool. Keep this checkbox deselected unless you have a specific reason to prevent the UTM from responding to a ping on a LAN port.
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 per 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 checkboxes: • **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 checkboxes are selected.

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

Setting Session Limits

Session limits allows you to specify the total number of sessions that are allowed, per user, over an IP connection across the UTM. The Session Limit feature is disabled by default.

To enable and configure the Session Limit feature:

1. Select **Network Security** > **Firewall** from the menu. The Firewall submenu tabs appear.
2. Click the **Session Limit** submenu tab. The Session Limit screen displays.

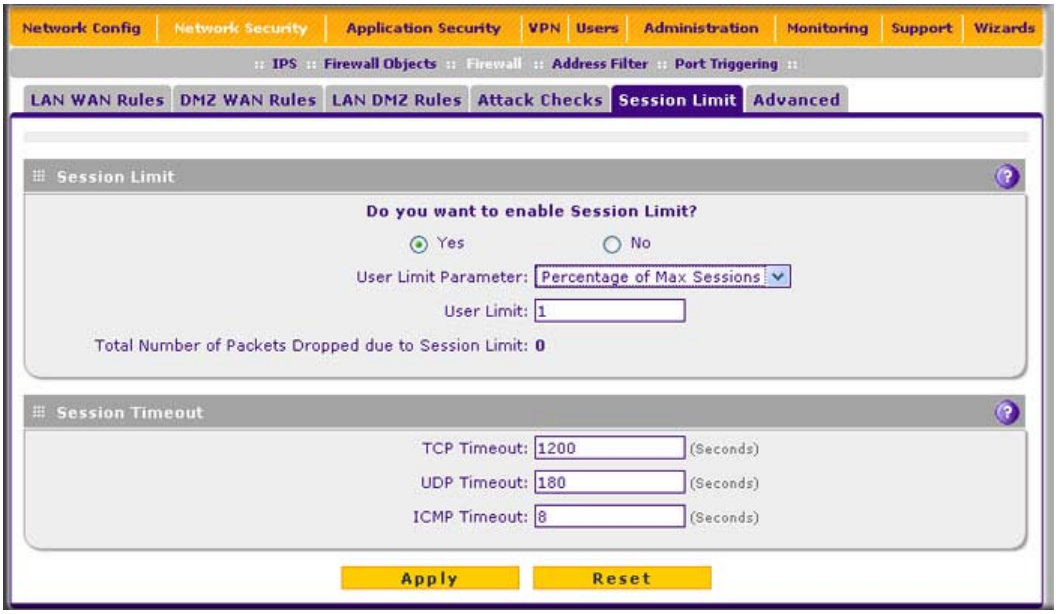


Figure 5-17

3. Click the **Yes** radio button under Do you want to enable Session Limit?
4. Enter the settings as explained in Table 5-5 on page 5-31.

Table 5-5. Session Limit Settings

Setting	Description (or Subfield and Description)
Session Limit	
User Limit Parameter	From the **User Limit Parameter** pull-down menu, select one of the following options: • **Percentage of Max Sessions**. A percentage of the total session connection capacity of the UTM. • **Number of Sessions**. An absolute number of maximum sessions.
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 non-configurable counter that displays the total number of dropped packets when the session limit is reached.
Session Timeout	
TCP Timeout	For each protocol, specify a timeout in seconds. A session expires if no data for the session is received for the duration of the timeout period. The default timeout periods are 1200 seconds for TCP sessions, 180 seconds for UDP sessions, and 8 seconds for ICMP sessions.
UDP Timeout	
ICMP Timeout	

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

Managing 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** from the menu. The Firewall submenu tabs appear.
2. Click the **Advanced** submenu tab. The Advanced screen displays (see Figure 5-18 on page 5-32).

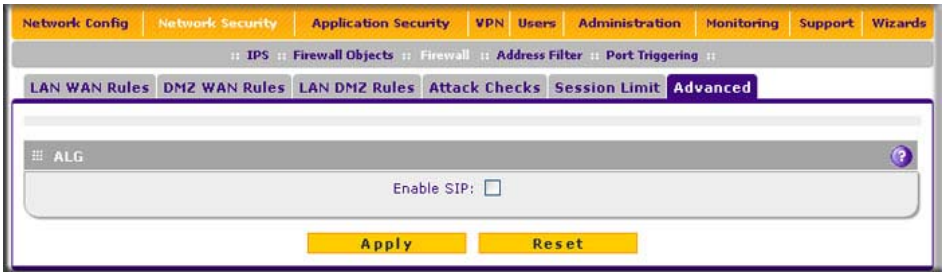


Figure 5-18

3. Select the **Enable SIP** checkbox.
4. Click **Apply** to save your settings.

Creating Services, QoS Profiles, and Bandwidth Profiles

When you create inbound and outbound firewall rules, you use firewall objects such as services, 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. For information about adding services, see “Adding Customized Services” on page 5-32.
- **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 “Creating Quality of Service (QoS) Profiles” on page 5-35.
- **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 “Creating Bandwidth Profiles” on page 5-38.

Note: A schedule narrows down the period during which a firewall rule is applied. For information about specifying schedules, see “Setting a Schedule to Block or Allow Specific Traffic” on page 5-41.

Adding 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 menu shows a list of services that you have defined, as shown in Figure 5-19.

To define a new service, first you must determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups of 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** > **Firewall Objects** from the menu. The Firewall Objects submenu tabs appear, with the Services screen in view. The screen displays the Custom Services table with the user-defined services. (Figure 5-19 shows some examples.)

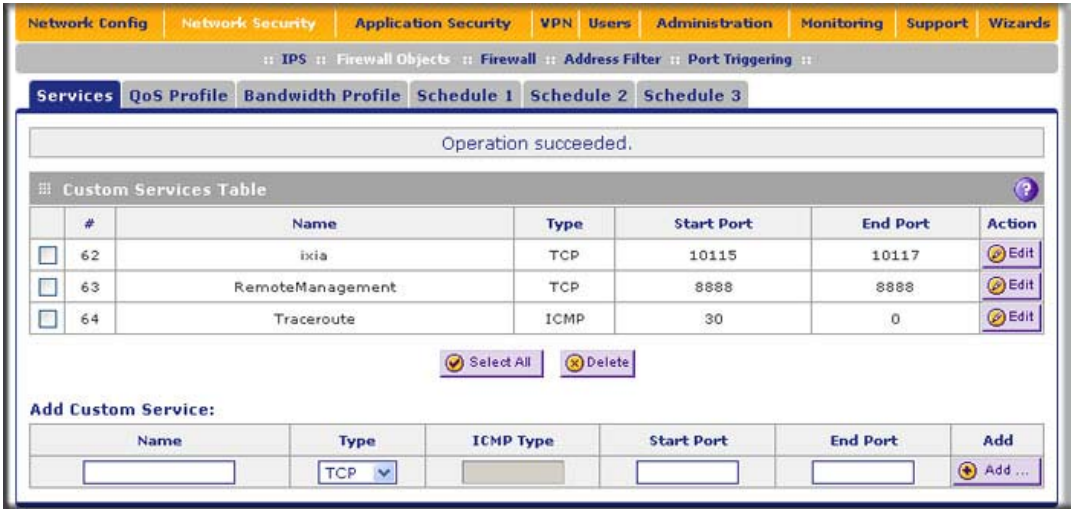


Figure 5-19

2. In the Add Customer Service section of the screen, enter the settings as explained in Table 5-6.

Table 5-6. Services Settings

Setting	Description (or Subfield and Description)
Name	A descriptive name of the service for identification and management purposes.
Type	From the **Type** pull-down menu, 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*. This field is enabled only when you select **ICMP** from the **Type** pull-down menu.
Start Port	The first TCP or UDP port of a range that the service uses. This field is enabled only when you select **TCP** or **UDP** from the **Type** pull-down menu.
Finish Port	The first 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 Finish Port fields. This field is enabled only when you select **TCP** or **UDP** from the **Type** pull-down menu.

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.

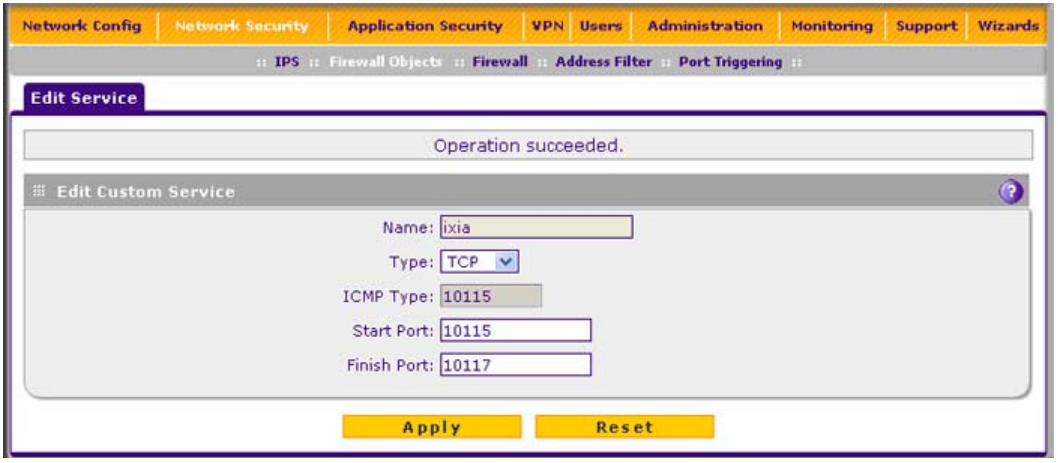


Figure 5-20

2. Modify the settings that you wish to change (see Table 5-6 on page 5-34).
3. Click **Apply** to save your changes. The modified service is displayed in the Custom Services table.

Creating Quality of Service (QoS) 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 non-blocking inbound or outbound firewall rule and traffic matching the firewall rule flows through the router.

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 5-3 on page 5-14).
- Add LAN WAN Inbound Services screen (see Figure 5-4 on page 5-15).
- Add DMZ WAN Outbound Services screen (see Figure 5-6 on page 5-17).
- Add DMZ WAN Inbound Services screen (see Figure 5-7 on page 5-18).

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 must 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 must 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 must 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** > **Firewall Objects** from the menu. The Firewall Objects submenu tabs appear, with the Services screen in view.
2. Click the **QoS Profiles** submenu tab. The QoS Profiles screen displays. Figure 5-21 shows some profiles in the List of QoS Profiles table as an example.

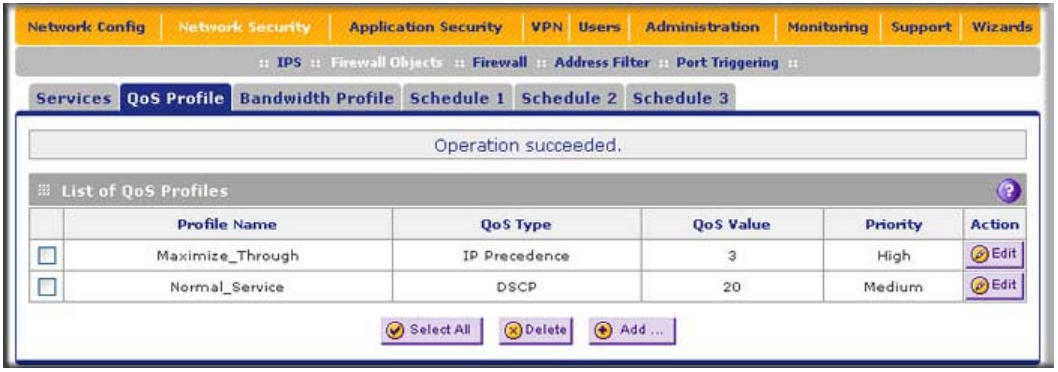


Figure 5-21

The screen displays the List of QoS Profiles table with the user-defined profiles.

3. Under the List of QoS Profiles table, click the **Add** table button. The Add QoS Profile screen displays.

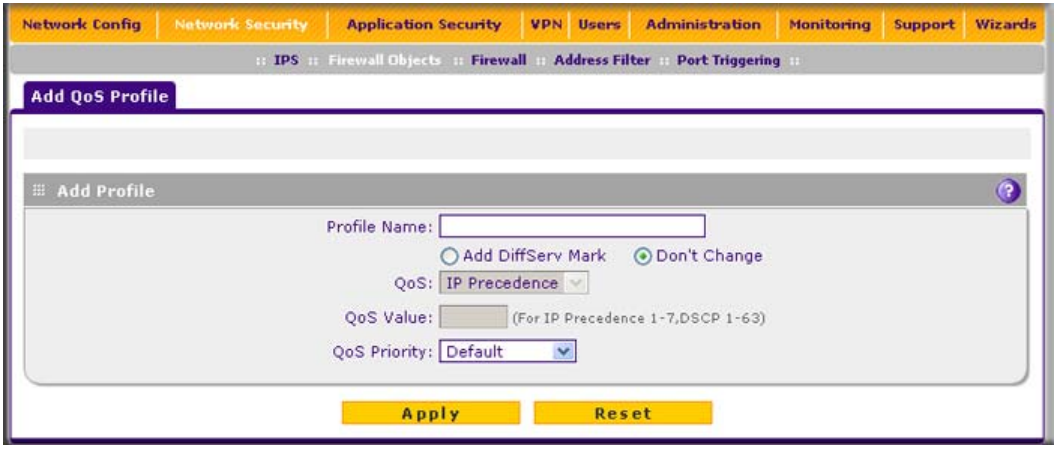


Figure 5-22

4. Enter the settings as explained in Table 5-7 on page 5-37.

Note: This document assumes that you are familiar with QoS concepts such QoS priority queues, IP Precedence, DHCP, and their values.

Table 5-7. QoS Profile Settings

Setting	Description (or Subfield and Description)	
Profile Name	A descriptive name of the QoS profile for identification and management purposes.	
Don't Change	Select the **Don't Change** radio button to ignore the QoS type (IP Precedence or DHCP) and QoS value and to set only the QoS priority.	
Add DiffServ Mark	Select the **Add DiffServ Mark** radio button 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.	
	QoS (Type)	From the **QoS** pull-down menu, 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** pull-down menu: • 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** pull-down menu, select one of the following priority queues: • **Default**. • **High**. • **Medium High**. • **Medium**. • **Low**.	

5. 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 Table 5-7).

3. Click **Apply** to save your changes. The modified QoS profile is displayed in the List of QoS Profiles table.

Creating 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.

For outbound traffic, you can apply bandwidth profiles on the available WAN interfaces in both the single WAN port mode and auto-rollover modes, and in load balancing mode on 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. For example, 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 5-3 on page 5-14).
- Add LAN WAN Inbound Services screen (see Figure 5-4 on page 5-15).

To add and enable a bandwidth profile:

1. Select **Network Security** > **Firewall Objects** from the menu. The Firewall Objects submenu tabs appear, with the Services screen in view.
2. Click the **Bandwidth Profiles** submenu tab. The Bandwidth Profiles screen displays (see Figure 5-23 on page 5-39, which shows one profile in the List of Bandwidth Profiles table as an example).

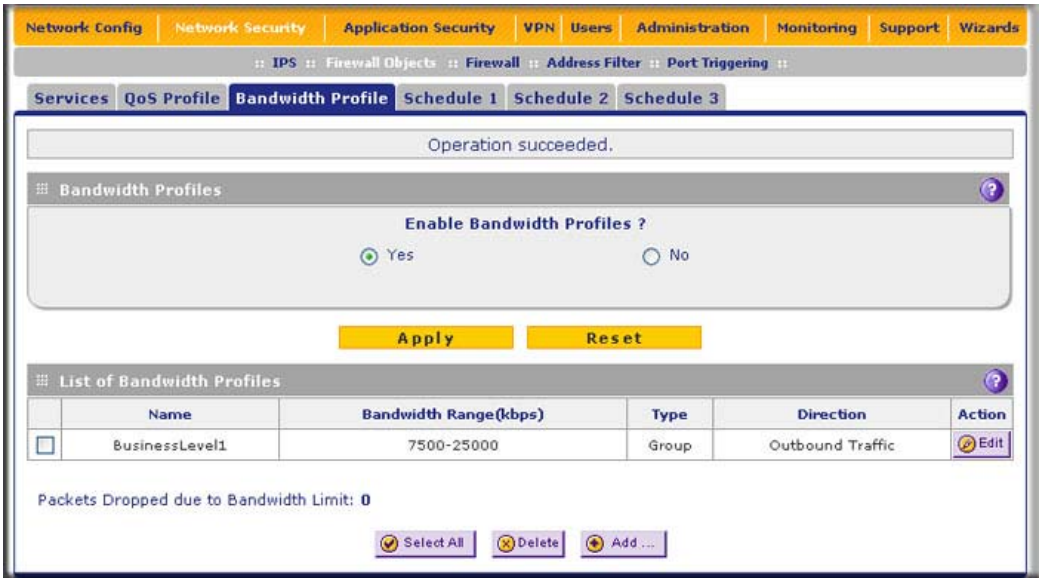


Figure 5-23

The screen displays the List of Bandwidth Profiles table with the user-defined profiles.

3. Under the List of Bandwidth Profiles table, click the **Add** table button. The Add Bandwidth Profile screen displays.

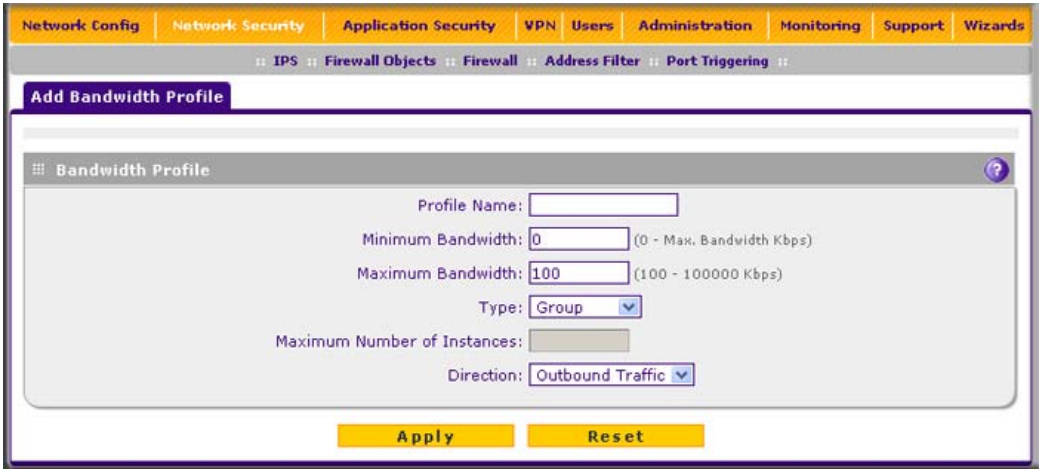


Figure 5-24

4. Enter the settings as explained in Table 5-8 on page 5-40.

Table 5-8. Bandwidth Profile Settings

Setting	Description (or Subfield and Description)	
Profile Name	A descriptive name of the bandwidth profile for identification and management purposes.	
Minimum Bandwidth	The minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.	
Maximum Bandwidth	The maximum allowed bandwidth in Kbps. The default setting and minimum setting is 100 Kbps; the maximum allowable bandwidth is 100000 Kbps.	
Type	From the **Type** pull-down menu, select the type for the bandwidth profile: • **Group**. The profile applies to all users, that is, all user 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 pull-down menu, you must specify the maximum number of class instances that can be created by the individual bandwidth profile.
Direction	From the **Direction** pull-down menu, select the traffic direction for the bandwidth profile: • **Outbound Traffic**. The profile applies to outbound traffic only. • **Inbound Traffic**. The profile applies to inbound traffic only.	

5. Click **Apply** to save your settings. The new bandwidth profile is added to the List of Bandwidth Profiles table.
6. 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.)
7. 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 Table 5-8).
3. Click **Apply** to save your changes. The modified bandwidth profile is displayed in the List of Bandwidth Profiles table.

Setting a Schedule to Block or Allow Specific Traffic

Schedules define the timeframes under which firewall rules may be applied. Three schedules, Schedule 1, Schedule 2 and Schedule3 can be defined, and any one of these can be selected when defining firewall rules.

To set a schedule:

1. Select **Network Security** > **Firewall Objects** from the menu. The Firewall Objects submenu tabs appear, with the Services screen in view.
2. Click the **Schedule 1** submenu tab. The Schedule 1 screen displays.

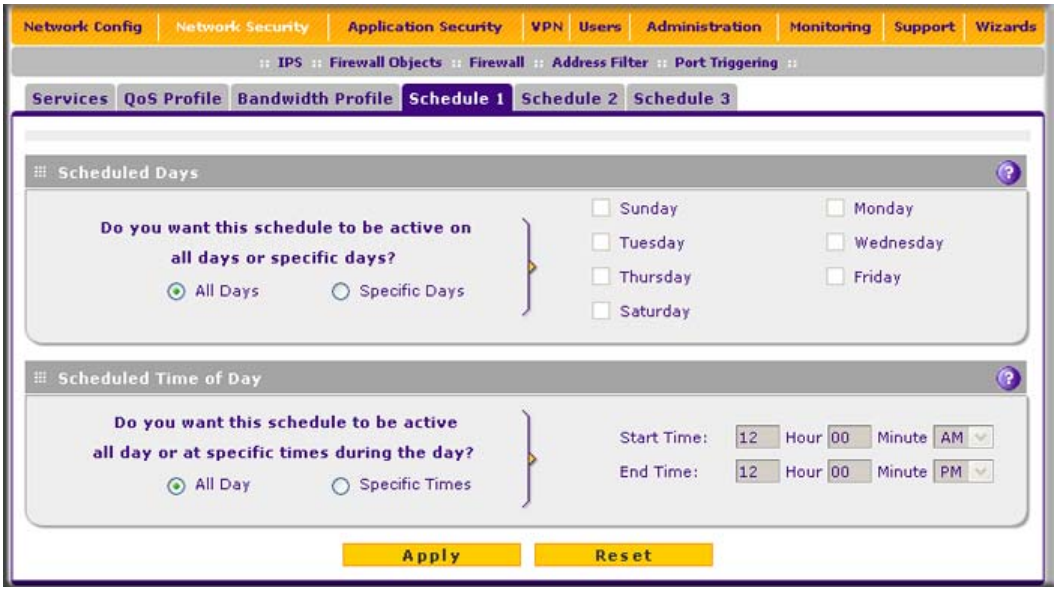


Figure 5-25

3. 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 active only on specific days.To the right of the radio buttons, select the checkbox for each day that you want the schedule to be in effect.
4. 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 active only on specific hours of the selected day or days. To the right of the radio buttons, specify the Start Time and End Time fields (Hour, Minute, AM/PM) during which the schedule is in effect.

5. Click **Apply** to save your settings to Schedule 1.

Repeat these steps to set to a schedule for Schedule 2 and Schedule 3.

Enabling 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 5-4.

To enable MAC filtering and add MAC addresses to be permitted or blocked:

1. Select **Network Security** > **Address Filter** from the menu. The Address Filter submenu tabs appear, with the Source MAC Filter screen in view (see Figure 5-26 on page 5-43, which shows one address in the MAC Addresses table as an example).

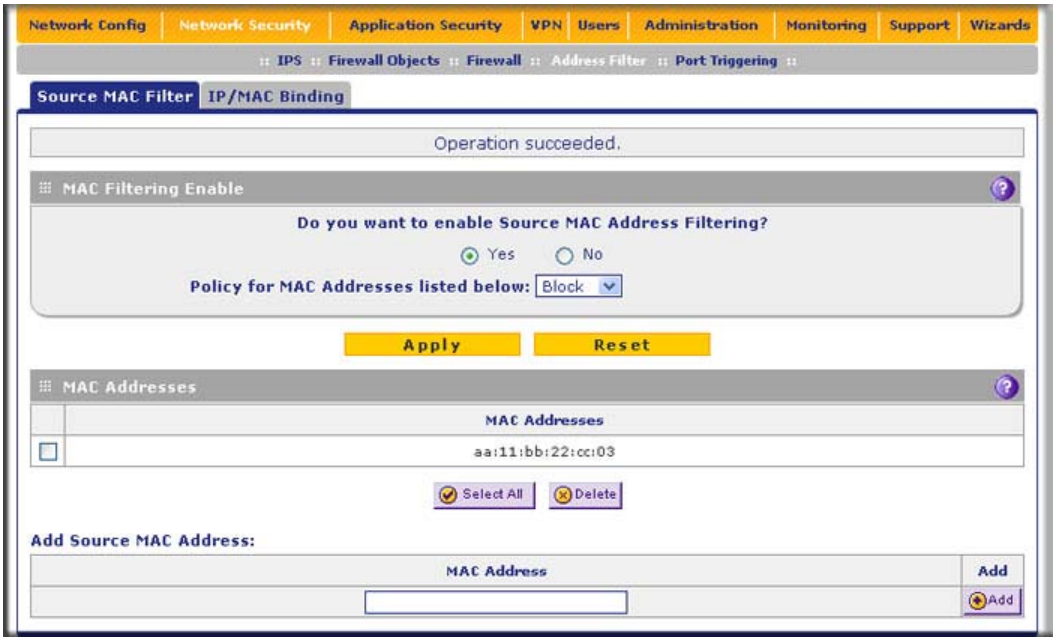


Figure 5-26

2. In the MAC Filtering Enable section, select the **Yes** radio button.
3. In the same section, select one of the following options from the pull-down menu (next to Policy for MAC Addresses listed below):
   - **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. Below Add Source MAC Address, 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 must be entered in the form xx:xx:xx:xx:xx:xx, where x is a numeric (0 to 9) or a letter between and a and f (inclusive), for example: aa:11:bb:22:cc:03.
5. Click the **Add** table button. The MAC address is added to the MAC Addresses table.
6. Click **Apply** to save your settings.

To remove one or more entries from the table:

1. Select the checkbox to the left of the MAC address that you want to delete or click the **Select All** table button to select all entries.
2. Click the **Delete** table button.

Setting up IP/MAC Bindings

IP/MAC Binding allows you to bind an IP address to a MAC address and vice-versa. Some PCs or devices are configured with static addresses. To prevent users from changing their static IP addresses, the IP/MAC Binding feature must be enabled on the UTM. If the UTM detects packets with a matching IP address but with the inconsistent MAC address (or vice-versa), 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 "Managing the Network Database" on page 4-13.

As an example, assume that three computers on the LAN are set up as follows:

- Host1: MAC address (00:01:02:03:04:05) and IP address (192.168.10.10)
- Host2: MAC address (00:01:02:03:04:06) and IP address (192.168.10.11)
- Host3: MAC address (00:01:02:03:04:07) and IP address (192.168.10.12)

If all of the above host entry examples are added to the IP/MAC Binding table, the following scenarios indicate the possible outcome.

- Host1: Matching IP & MAC address in IP/MAC Table.
- Host2: Matching IP but inconsistent MAC address in IP/MAC Table.
- Host3: Matching MAC but inconsistent IP address in IP/MAC Table.

In this example, the UTM blocks the traffic coming from Host2 and Host3, but allows the traffic coming from Host1 to any external network. The total count of dropped packets is displayed.

To set up IP/MAC bindings:

1. Select **Network Security** > **Address Filter** from the menu. The Address Filter submenu tabs appear, with the Source MAC Filter screen in view.
2. Click the **IP/MAC Binding** submenu tab. The IP/MAC Binding screen displays (see Figure 5-27 on page 5-45, which shows some bindings in the IP/MAC Binding table as an example).

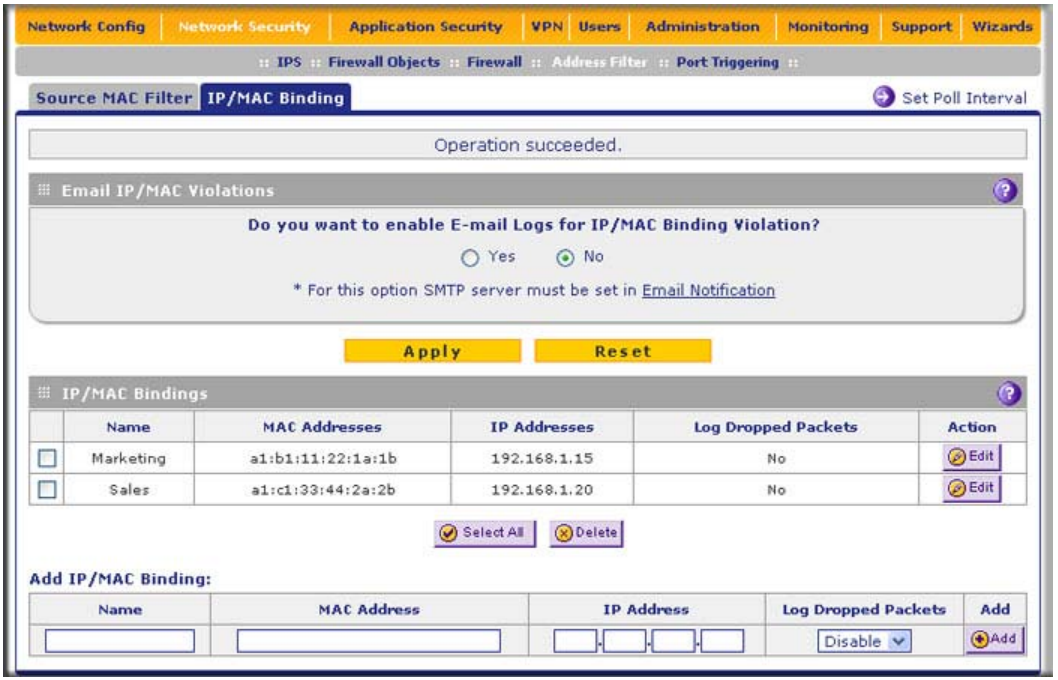


Figure 5-27

3. Enter the settings as explained in Table 5-9.

Table 5-9. IP/MAC Binding Settings

Setting	Description (or Subfield and 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 e-mailed. • **No**. IP/MAC binding violations are not e-mailed. **Note**: Click the **Firewall Logs & E-mail page** hyperlink to ensure that e-mailing of logs is enabled on the Email and Syslog screen (see "Configuring Logging, Alerts, and Event Notifications" on page 11-5).
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 5-9. IP/MAC Binding Settings (continued)

Setting	Description (or Subfield and 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 pull-down menu. The default setting is Disable.

4. Click the **Add** table button. The new IP/MAC rule is added to the IP/MAC Bindings table.
5. 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 Table 5-9).
3. Click **Apply** to save your changes. The modified IP/MAC binding is displayed in the IP/MAC Bindings table.

Configuring 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 this 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 PCs 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 requests 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 5-6.

To add a port triggering rule:

1. Select **Network Security** > **Port Triggering** from the menu. The Port Triggering screen displays. (Figure 5-28 shows a rule in the Port Triggering Rule table as an example.)

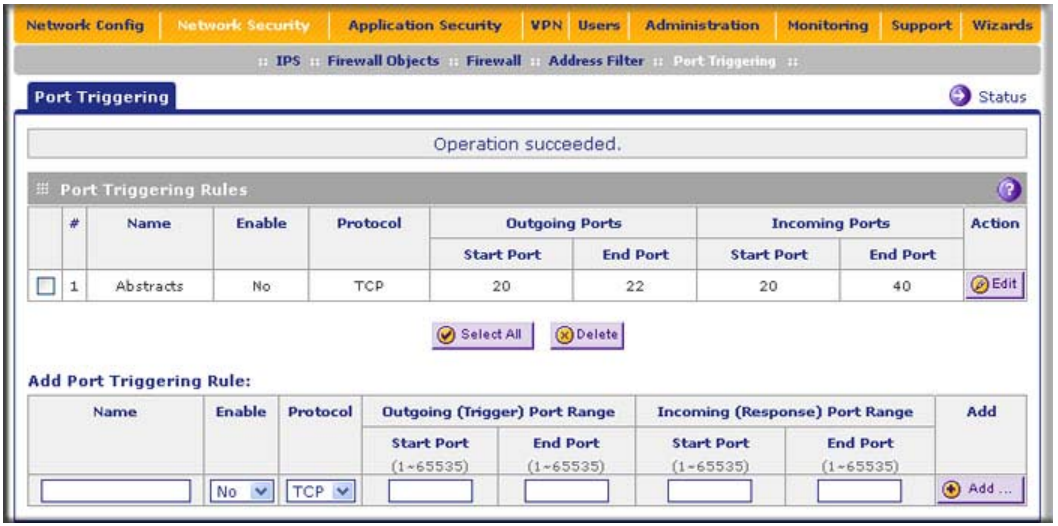


Figure 5-28

2. Below Add Port Triggering Rule, enter the settings as explained in Table 5-10 on page 5-48.

Table 5-10. Port Triggering Settings

Setting	Description (or Subfield and Description)	
Name	A descriptive name of the rule for identification and management purposes.	
Enable	From the pull-down menu, select **Yes** to enable the rule. (You can define a rule but not enable it.) The default setting is No.	
Protocol	From the pull-down menu, 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 Control Protocol (UCP).	
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 Table 5-10).
3. Click **Apply** to save your changes. The modified port triggering rule is displayed in the Port Triggering Rules table.

To display the status of the port triggering rules, click the **Status** option arrow at the top right of the Port Triggering screen. A popup window appears, displaying the status of the port triggering rules.

Figure 5-29

Using 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, e-mail, database, malware, and other attacks. The IPS differs from the malware scan mechanism (see "Configuring Web Malware Scans" on page 6-21) 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** from the menu. The IPS submenu tabs appear, with the Global (IPS) screen in view.

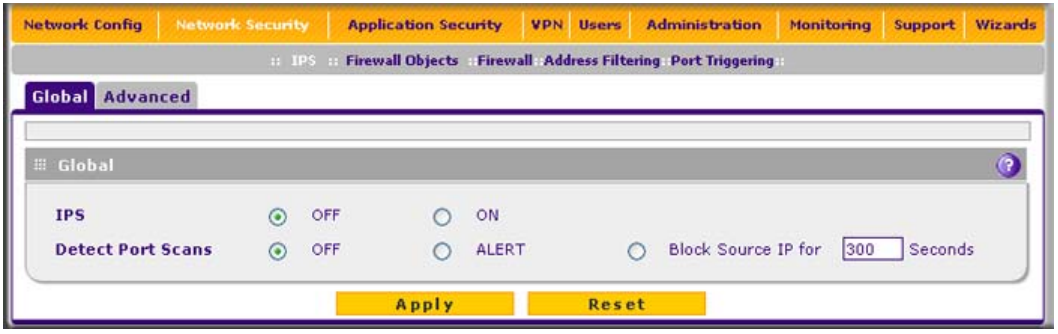


Figure 5-30

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 e-mailed 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 "Configuring Multi-Home LAN IPs on the Default VLAN" on page 4-11) 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 (IPS) screen returns to when you click the Reset button. To modify the default IPS configuration:

1. Select **Network Security** > **IPS** from the menu. The IPS submenu tabs appear, with the Global (IPS) screen in view (see Figure 5-30 on page 5-49).
2. From the IPS submenu tabs, click **Advanced**. The Advanced (IPS) screen displays see Figure 5-31 on page 5-51). This screen displays sections for the different categories of attacks such as Web, Mail, Databases, and so on.
3. In the Enabled column for each section, either select individual attacks by selecting the checkboxes to the left of the names, or select all attacks for that category by selecting the checkbox to the left of "All web attacks."
4. In the Action column for each section, either select the actions for individual attacks by making selections from the pull-down menus to the right of the names, or select a global action for all attacks for that category by making a selection from the pull-down menu to the right of "All web attacks." Some of the less familiar Web and miscellaneous attacks are explained in Table 5-11 on page 5-52.

   The pull-down menus let you make 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.

   Note: To ensure that alerts are emailed to an administrator, you must configure the e-mail notification server (see "Configuring the E-mail Notification Server" on page 11-5) and the IPS alerts (see "Configuring and Activating Update Failure and Attack Alerts" on page 11-10).

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

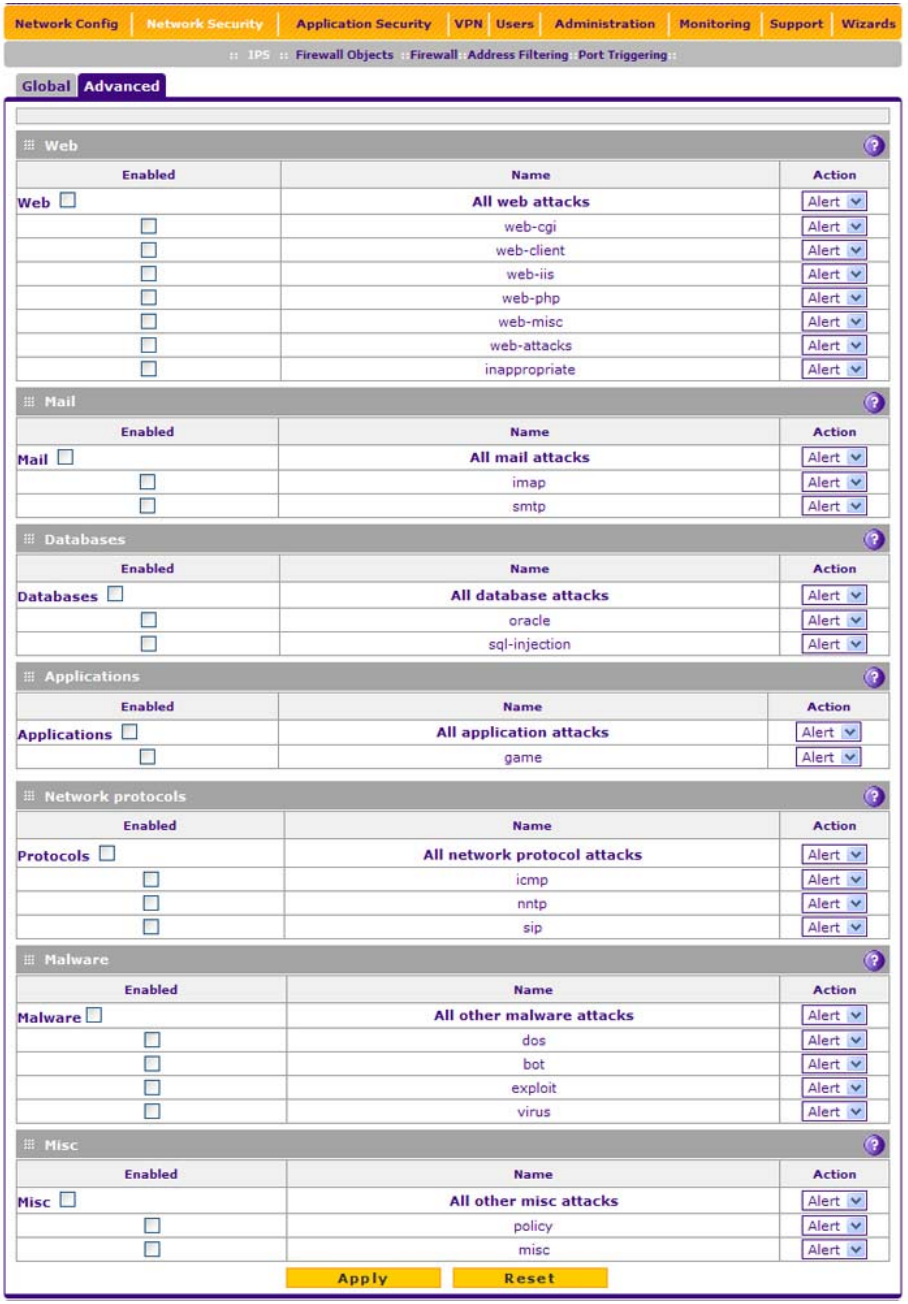

Network Config
Network Security
Application Security
VPN
Users
Administration
Monitoring
Support
Wizards
IPS
Firewall Objects
Firewall
Address Filtering
Port Triggering
Global
Advanced
Web
Enabled
Name
Action
Web
All web attacks
Alert
web-cgi
web-client
web-iis
web-php
web-misc
web-attacks
inappropriate
Mail
Mail
All mail attacks
imap
smtp
Databases
Databases
All database attacks
oracle
sql-injection
Applications
Applications
All application attacks
game
Network protocols
Protocols
All network protocol attacks
icmp
nntp
sip
Malware
Malware
All other malware attacks
dos
bot
exploit
virus
Misc
Misc
All other misc attacks
policy
misc
Apply
Reset

Figure 5-31

Table 5-11. IPS: Less Familiar Attack Names

Attack Name	Description (or Subfield and 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	Detect the behavior about visiting pornographic Web sites.
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.

Chapter 6
Content Filtering and Optimizing Scans

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

The UTM provides very extensive Web content and e-mail content filtering options, Web browsing activity reporting, e-mail anti-virus and anti-spam options, and instant alerts via e-mail. 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 "Configuring Multi-Home LAN IPs on the Default VLAN" on page 4-11) is also scanned for content and malware threats.

	**Note:** For information about how to monitor blocked content and malware threats in real-time, see "Monitoring Real-Time Traffic, Security, and Statistics" on page 11-14. For information about how to view blocked content and malware threats in the logs, see "Querying Logs and Generating Reports" on page 11-32.

Default E-mail and Web Scan Settings

For most network environments, the default scan settings and actions that are shown in Table 6-1 work well but you can adjust these to the needs of your specific environment.

Table 6-1. Default E-mail and Web Scan Settings

Scan Type	Default Scan Setting	Default Action (if applicable)
Email Server Protocols		
SMTP	Enabled	Block infected e-mail
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 (Jabber)	Allowed	
mIRC	Allowed	
MSN Messenger	Allowed	
Yahoo Messenger	Allowed	
Peer-to-Peer (P2P) Services		
BitTorrent	Allowed	
eDonkey	Allowed	
Gnutella	Allowed	
Web Objects		
Embedded Objects (ActiveX/Java/Flash	Allowed	
Javascript	Allowed	
Proxy	Allowed	
Cookies	Allowed	
Web Content Categories		
Commerce	Allowed	
Drugs and Violence	Blocked	

Table 6-1. Default E-mail and Web Scan Settings (continued)

Scan Type	Default Scan Setting	Default Action (if applicable)
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	
Politics and Religion	Allowed	
Sexual Content	Blocked	
Technology	Allowed	

a. Files or messages that are larger than 2048 KB are skipped b y default.

Configuring E-mail Protection

The UTM lets you configure the following settings to protect the network's e-mail communication:

- The e-mail protocols that are scanned for malware threats.
- Actions that are taken when infected e-mails are detected.
- The maximum file sizes that are scanned.
- Keywords, file types, and file names in e-mails that are filtered to block objectionable or high-risk content.
- Customer notifications and e-mail alerts that are sent when events are detected.
- Rules and policies for spam detection.

Customizing E-mail Protocol Scan Settings

To configure the e-mail protocols and ports to scan:

1. Select **Application Security** > **Services** from the menu. The Services screen displays (Figure 6-1 shows the upper part of the Services screen only).

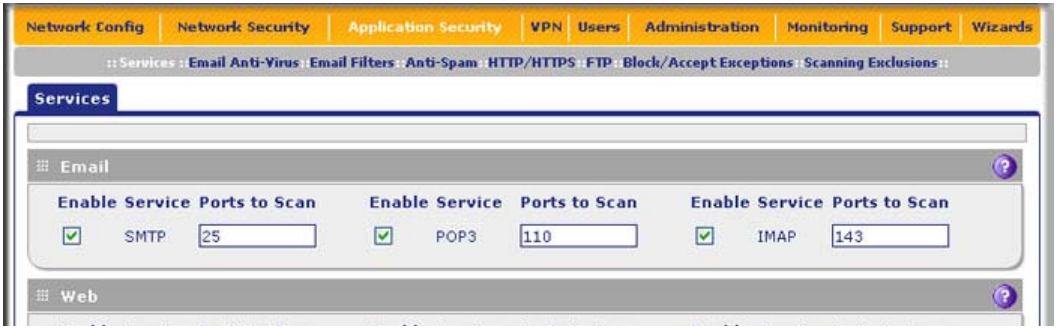


Figure 6-1

2. In the Email section of the screen, select the protocols to scan by selecting the **Enable** checkboxes 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.

	Note: If a protocol uses a port other than the standard service port (for example, port 25 for SMTP), enter this non-standard 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.

	Note: The following protocols are not supported by the UTM: SMTP over SSL using port number 465, POP3 over SSL using port number 995, and IMAP over SSL using port number 993.

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

Customizing E-mail Anti-Virus and Notification Settings

Whether or not the UTM detects an e-mail virus, you can configure it to take a variety of actions (some of the default actions are listed in Table 6-1 on page 6-2) and send notifications, e-mails, or both to the end users. To configure the e-mail anti-virus settings:

1. Select **Application Security** > **Email Anti-Virus** from the menu. The Email Anti-Virus screen displays.

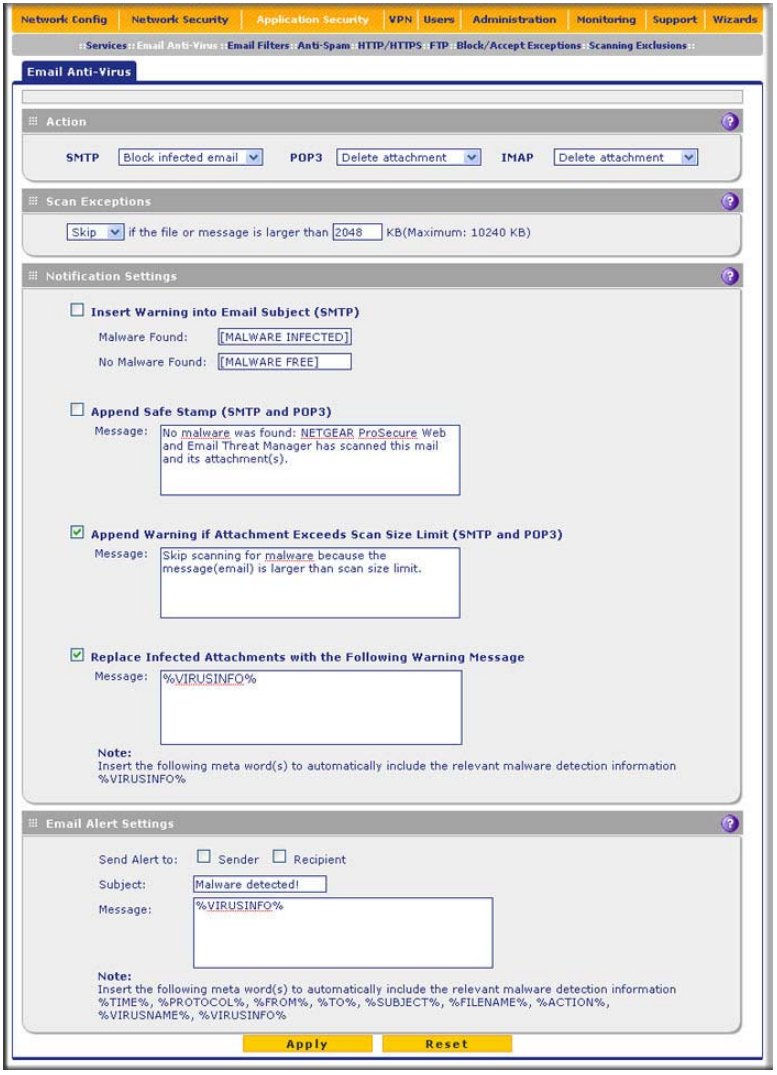


Figure 6-2

2. Enter the settings as explained in Table 6-2.

Table 6-2. E-mail Anti-Virus and Notification Settings

Setting	Description (or Subfield and Description)
Action	
SMTP	From the **SMTP** pull-down menu, specify one of the following actions when an infected e-mail is detected: • **Block infected email**. This is the default setting. The e-mail is blocked, and a log entry is created. • **Delete attachment**.The e-mail is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The e-mail is not blocked and the attachment is not deleted.
POP3	From the **POP3** pull-down menu, specify one of the following actions when an infected e-mail is detected: • **Delete attachment**. This is the default setting. The e-mail is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created.The e-mail is not blocked and the attachment is not deleted.
IMAP	From the **IMAP** pull-down menu, specify one of the following actions when an infected e-mail is detected: • **Delete attachment**. This is the default setting. The e-mail is not blocked, but the attachment is deleted, and a log entry is created. • **Log only**. Only a log entry is created. The e-mail is not blocked and the attachment is not deleted.
Scan Exceptions	
The default maximum file or message size 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 10-1). From the pull-down menu, specify one of the following actions 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.	
Notification Settings	
Insert Warning into Email Subject (SMTP)	For SMTP e-mail messages, select this checkbox to insert a warning into the e-mail 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 checkbox is deselected and no warnings are inserted.

Table 6-2. E-mail Anti-Virus and Notification Settings (continued)

Setting	Description (or Subfield and Description)
Append Safe Stamp (SMTP and POP3)	For SMTP and POP3 e-mail messages, select this checkbox to insert a default safe stamp message at the end of an e-mail. The safe stamp insertion serves as a security confirmation to the end user. You can change the default message. By default, this checkbox is deselected and no safe stamp is inserted.
The attachment(s) was not scanned for malware because it exceeded the scan size limit.	Select this checkbox to append a default warning message to an e-mail 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 checkbox is selected and a warning message is appended to the e-mail.
Replace Infected Attachments with the Following Warning Message	Select this checkbox to replace an e-mail 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 example below). By default, this checkbox is selected and a warning message replaces an infected e-mail. **Note**: Make sure that you keep the %VIRUSINFO% meta word in a message to enable the UTM to insert the proper malware information. The following is an example message where the %VIRUSINFO% meta word is replaced with the EICAR test virus: This attachment contains malware: File 1.exe contains malware EICAR. Action: Delete.”
Email Alert Settings **Note**: Ensure that the E-mail Notification Server (see “Configuring the E-mail Notification Server” on page 11-5) is configured before you specify the e-mail alert settings.	
Send alert to	In addition to inserting an warning message to replace an infected e-mail, you can configure the UTM to send a notification e-mail to the sender, the recipient, or both by selecting the corresponding checkbox or checkboxes. By default, both checkboxes are deselected and no notification e-mail is sent.

Table 6-2. E-mail Anti-Virus and Notification Settings (continued)

Setting	Description (or Subfield and Description)
Subject	The default subject line for the notification e-mail 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% meta word in a message to enable the UTM to insert the proper malware information. In addition to the %VIRUSINFO% meta word, you can insert the following meta words in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.

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

E-mail Content Filtering

The UTM provides several options to filter unwanted content from e-mails. You can filter content from e-mails 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 e-mails with password-protected attachments.

Several types of e-mail blocking are available:

- **Keyword blocking**. You can specify words that, should they appear in the e-mail subject line, cause that e-mail to be blocked by the UTM.
- **Password-protected attachments**. You can block e-mails based on password-protected attachments such as ZIP or RAR attachments.
- **File extension blocking**. You can block e-mails 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 e-mails based on the names of attached files. Such names can include, for example, names of known malware threat such as the Netsky worm (which normally arrives as netsky.exe).

To configure e-mail content filtering:

1. Select **Application Security** > **Email Filters** from the menu. The Email Filters screen displays.

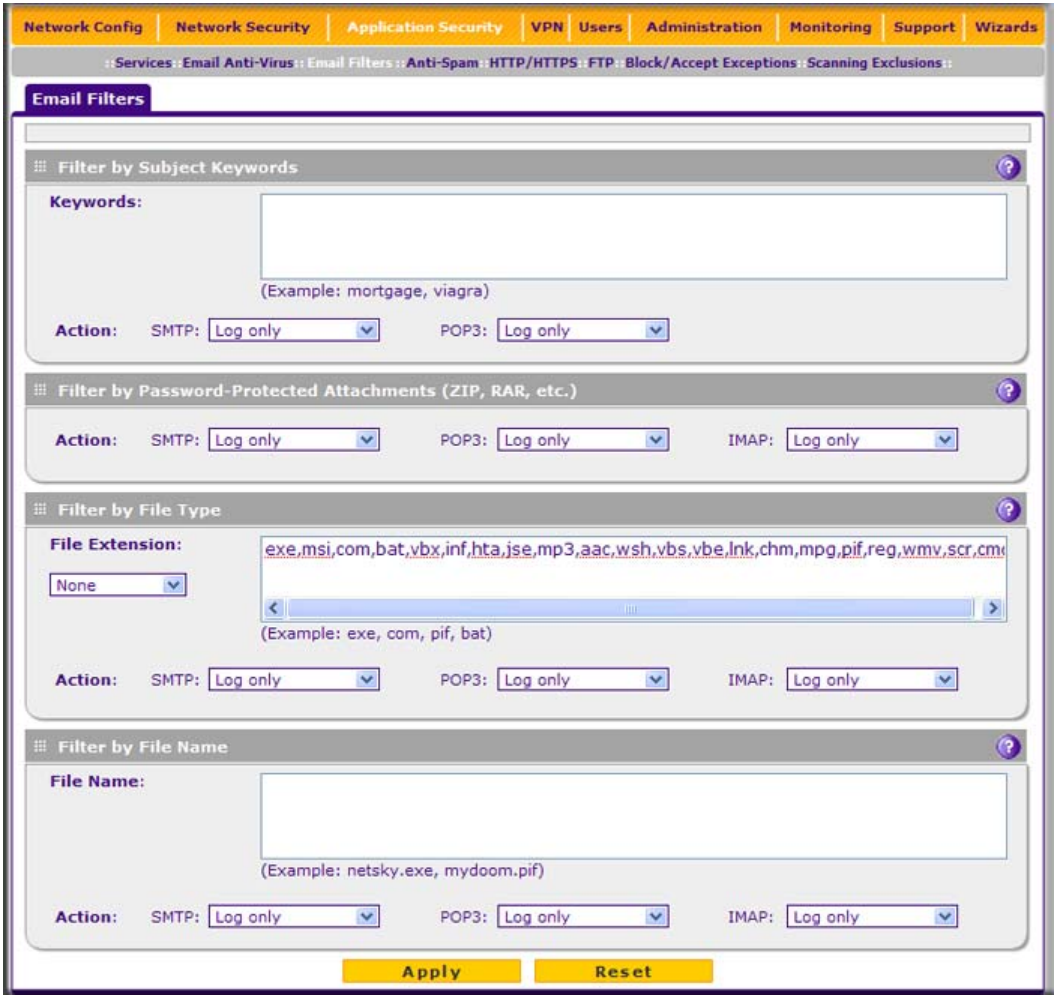


Figure 6-3

2. Enter the settings as explained in Table 6-3.

Table 6-3. E-mail Filter Settings

Setting	Description (or Subfield and Description)	
Filter by Subject Keywords		
Keywords	Enter keywords that should be detected in the e-mail subject line. Use commas to separate different keywords. The total maximum length of this field is 2048 characters, excluding duplicate words and delimiter commas.	
Action	SMTP	From the **SMTP** pull-down menu, specify one of the following actions when a keyword that is defined in the Keywords field is detected: • **Block email**. The e-mail is blocked, and a log entry is created. • **Log only**. This is the default setting. Only a log entry is created. The e-mail is not blocked.
	POP3	From the **POP3** pull-down menu, specify one of the following actions when a keyword that is defined in the Keywords field is detected: • **Block email**. The e-mail is blocked, and a log entry is created. • **Log only**. This is the default setting. Only a log entry is created. The e-mail is not blocked.
Filter by Password-Protected Attachments (ZIP, RAR, etc.)		
Action	SMTP	From the **SMTP** pull-down menu, specify one of the following actions when a password-protected attachment to an e-mail is detected: • **Block email**. The e-mail is blocked, and a log entry is created. • **Delete attachment**. The e-mail 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 e-mail is not blocked and the attachment is not deleted.
	POP3	From the **POP3** pull-down menu, specify one of the following actions when a password-protected attachment to an e-mail is detected: • **Delete attachment**. The e-mail 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 e-mail is not blocked and the attachment is not deleted.
	IMAP	From the **IMAP** pull-down menu, specify one of the following actions when a password-protected attachment to an e-mail is detected: • **Delete attachment**. The e-mail 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 e-mail is not blocked and the attachment is not deleted.

Table 6-3. E-mail Filter Settings (continued)

Setting	Description (or Subfield and Description)	
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 pull-down menu 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.	
Action	SMTP	From the pull-down menu, specify an action when an e-mail attachment with a file extension that is defined in the File Extension field is detected. The pull-down menu selections and defaults are the same as the ones for the "Filter by Password-Protected Attachments (ZIP, RAR, etc.)" section above.
	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 pull-down menu, specify an action when an e-mail attachment with a name that is defined in the File Name field is detected. The pull-down menu selections and defaults are the same as the ones for the "Filter by Password-Protected Attachments (ZIP, RAR, etc.)" section above.
	POP3	
	IMAP	

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

Protecting Against E-mail Spam

The UTM integrates multiple anti-spam technologies to provide comprehensive protection against unwanted e-mail. You can enable all or a combination of these anti-spam technologies. The UTM implements these spam prevention technologies in the following order:

1. **Whitelist**. E-mails from the specified sources or to the specified recipients are not considered spam and are accepted.
2. **Blacklist**. E-mails from the specified sources are considered spam and are blocked.

3. **Real-time blacklist**. E-mails from known spam sources that are collected by blacklist providers are blocked.
4. **Distributed Spam Analysis**. E-mails 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 e-mail originates from a whitelisted source, the UTM delivers the e-mail 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 e-mail is whitelisted, the e-mail is still scanned by the UTM's anti-malware engines.

You can configure these anti-spam options in conjunction with content filtering to optimize blocking of unwanted mails.

Note: E-mails that are processed through the UTM over an authenticated e-mail connection between a client and a mail server are not checked for spam.

Note: An e-mail has been checked for spam by the UTM contains an "X-STM-SMTP" (for SMTP e-mails) or "X-STM-POP3" (for POP-3 e-mails) tag in its header.

Setting Up the Whitelist and Blacklist

You can specify e-mails that are accepted or blocked based on the originating IP address, domain, and e-mail address by setting up the whitelist and blacklist. You can also specify e-mails that are accepted based on the destination domain and e-mail address.

The whitelist ensures that e-mail from listed (that is, trusted) sources and recipients are not mistakenly tagged as spam. E-mails going to and from these sources and recipients are delivered to their destinations immediately, without being scanned by the anti-spam engines. This can help to speed up the system and network performance. The blacklist, on the other hand, lists sources from which all e-mail 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 e-mail source is on both the blacklist and the whitelist, the e-mail is not scanned by the anti-spam engines.

To configure the whitelist and blacklist:

1. Select **Application Security** > **Anti-Spam** from the menu. The Anti-Spam submenu tabs appear, with the Whitelist/Blacklist screen in view.

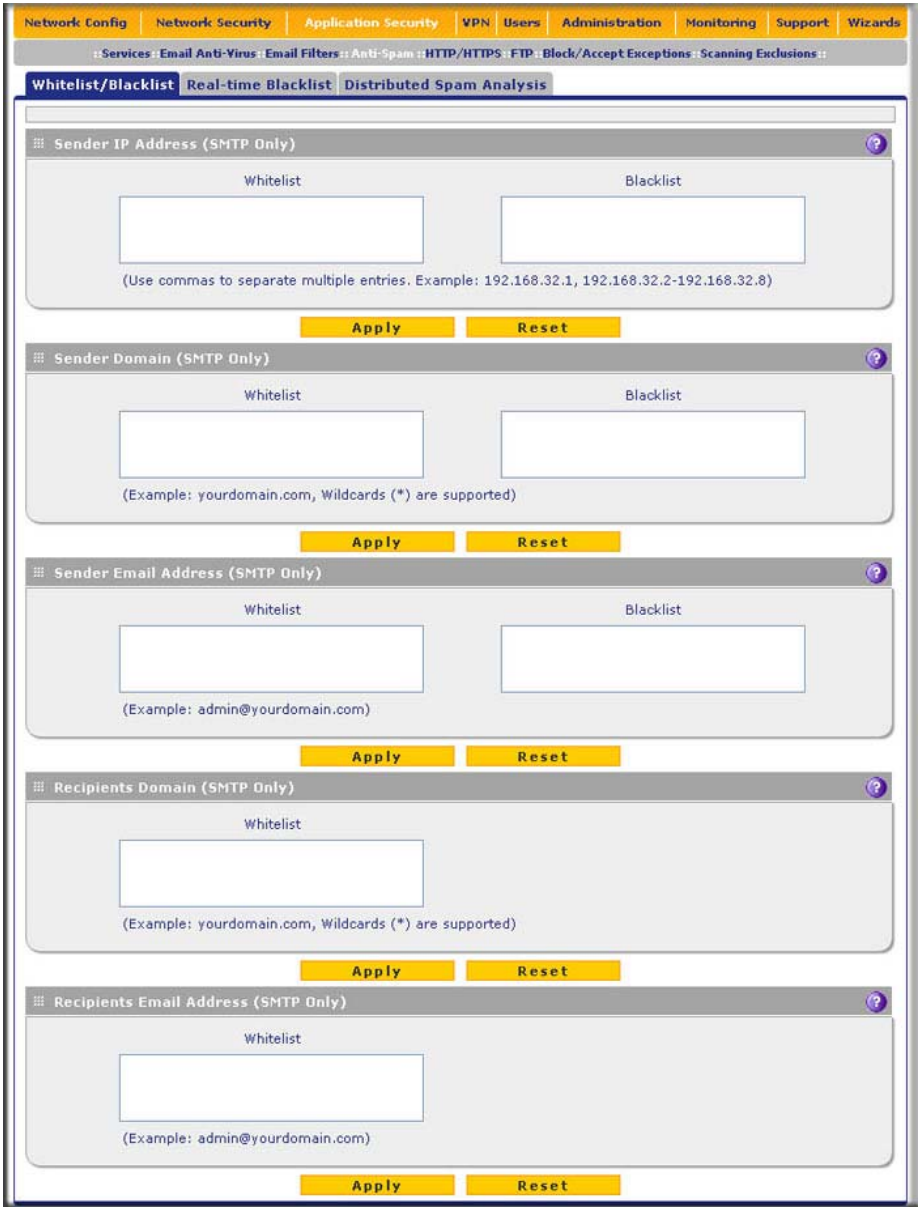


Figure 6-4

2. Enter the settings as explained in Table 6-3.

Table 6-4. Whitelist/Blacklist Settings

Setting	Description (or Subfield and Description)
Sender IP Address	
Whitelist	Enter the source IP addresses from which e-mails can be trusted.
Blacklist	Enter the source IP addresses from which e-mails are blocked.
Click **Apply** to save your settings or click **Reset** to clear all entries from these fields.	
Sender Domain	
Whitelist	Enter the sender e-mail domains from which e-mails can be trusted.
Blacklist	Enter the sender e-mail domains from which e-mails are blocked.
Click **Apply** to save your settings or click **Reset** to clear all entries from these fields.	
Sender Email Address	
Whitelist	Enter the e-mail addresses from which e-mails can be trusted.
Blacklist	Enter the e-mail addresses from which e-mails are blocked.
Click **Apply** to save your settings or click **Reset** to clear all entries from these fields.	
Recipients Domain	
Whitelist	Enter the sender e-mail domains of the recipients to which e-mails can be safely delivered.
Click **Apply** to save your settings or click **Reset** to clear all entries from this field.	
Recipients Email Address	
Whitelist	Enter the e-mail addresses of the recipients to which e-mails 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 dash to indicate a range (for example, 192.168.32.2-192.168.32.8.)

Configuring 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** from the menu. The Anti-Spam submenu tabs appear, with the Whitelist/Blacklist screen in view.
2. Click the **Real-time Blacklist** submenu tab. The Real-time Blacklist screen displays.

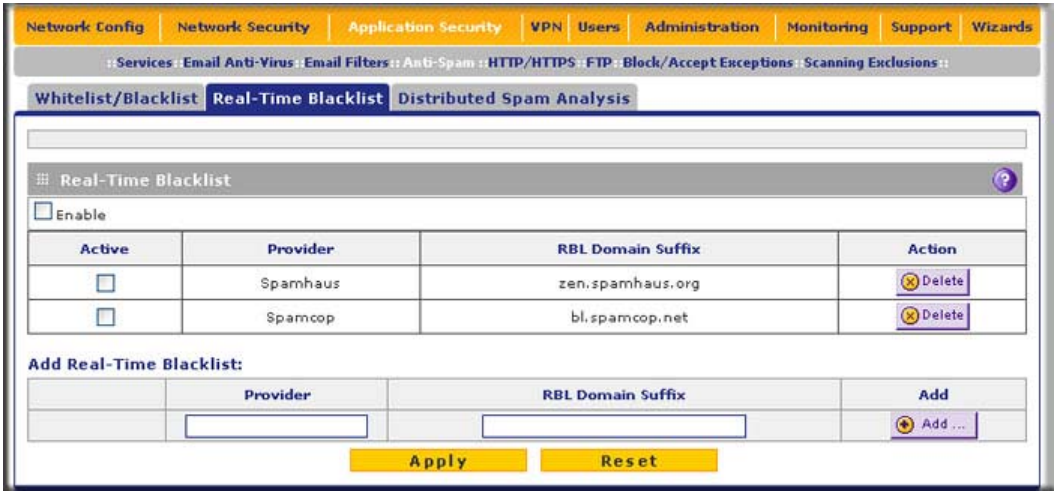


Figure 6-5

3. Select the **Enable** checkbox enable the Real-Time Blacklist function.
4. Select the **Active** checkboxes to the left of the default blacklist providers (Spamhaus, and Spamcop) that you want to activate.
5. 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.

Configuring Distributed Spam Analysis

Spam, phishing, and other e-mail-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 which 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 by analyzing 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 e-mail is spam for SMTP and POP3 e-mails. Any e-mail 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 must be connected to the Internet for the spam analysis to be performed correctly.

To configure Distributed Spam Analysis and the anti-spam engine settings:

1. Select **Application Security** > **Anti-Spam** from the menu. The Anti-Spam submenu tabs appear, with the Whitelist/Blacklist screen in view.
2. Click the **Distributed Spam Analysis** submenu tab. The Distributed Spam Analysis screen displays (see Figure 6-6 on page 6-17).

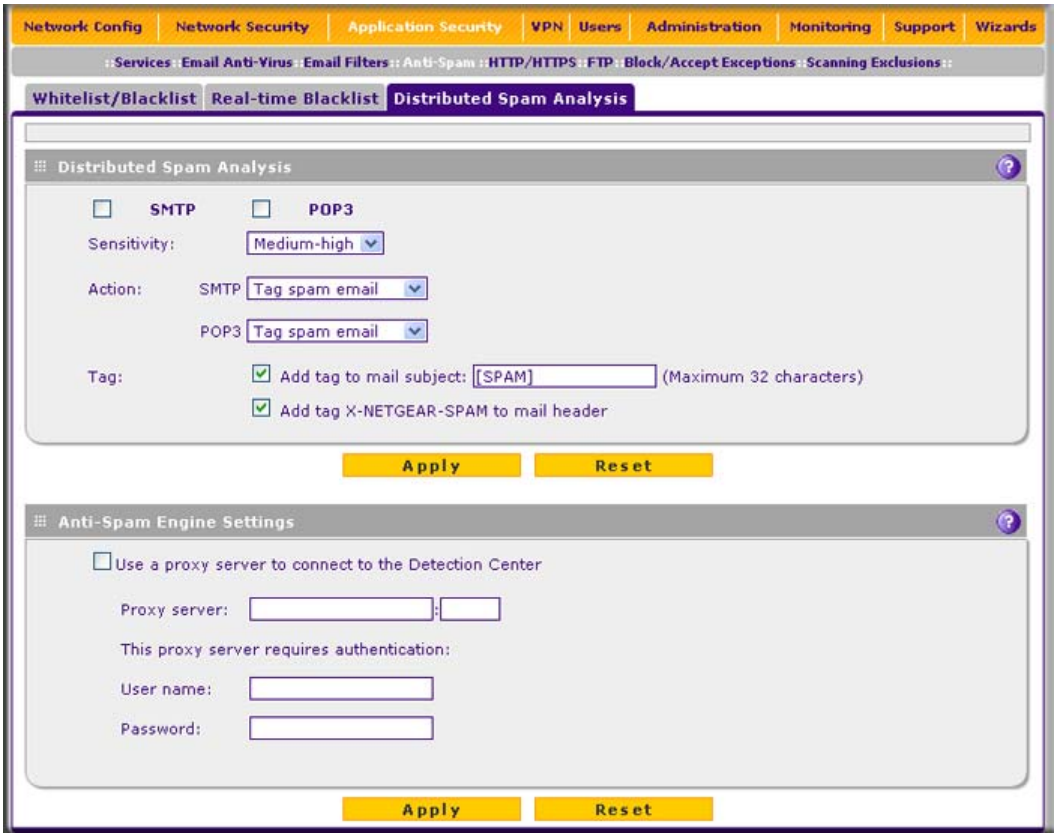


Figure 6-6

3. Enter the settings as explained in Table 6-5.

Table 6-5. Distributed Spam Analysis Settings

Setting	Description (or Subfield and Description)
Distributed Spam Analysis	
SMTP	Select the **SMTP** checkbox to enable Distributed Spam Analysis for the SMTP protocol. (You can enable Distributed Spam Analysis for both SMTP and POP3.)
POP3	Select the **POP3** checkbox to enable Distributed Spam Analysis for the POP3 protocol. (You can enable Distributed Spam Analysis for both SMTP and POP3.)

Table 6-5. Distributed Spam Analysis Settings (continued)

Setting	Description (or Subfield and Description)	
Sensitivity	From the **Sensitivity** pull-down menu, select the level of sensitivity for the anti-spam engine that performs the analysis: **Low**. **Medium-Low**. **Medium**. **Medium High**. This is the default setting. **High**. **Note**: A low sensitivity allows more e-mails to pass through but increases the risk of spam messages. A high sensitivity allows fewer e-mails to pass through but diminishes the risk of spam messages.	
Action	SMTP	From the **SMTP** pull-down menu, select the action that is taken when spam is detected by the anti-spam engine: • **Tag spam email**. This is the default setting. • **Block spam email**.
	POP3	The only option is to block spam e-mail.
Tag	Add tag to mail subject	When the option “Tag spam email” is selected from the Action pull-down menu (see above), select this checkbox to add a tag to the e-mail 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 the option “Tag spam email” is selected from the Action pull-down menu (see above), select this checkbox to add the “X-NETGEAR-SPAM” tag to the e-mail header. The default setting is to add the default tag to the e-mail header.
Anti-Spam Engine Settings		
Use a proxy server to connect to the Detection Center	Select this checkbox 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.

4. 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.

Configuring 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 services, and peer-to-peer services 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 e-mail alerts that are sent when events are detected.
- Schedules that determine when content filtering is active.

Customizing Web Protocol Scan Settings and Services

You can specify the Web protocols (HTTP, HTTPS, and FTP) that are scanned for malware threats and the instant messaging and peer-to-peer applications 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, only enable scanning of 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 10-1.

To configure the Web protocols, ports, and applications to scan:

1. Select **Application Security** > **Services** from the menu. The Services screen displays (see Table 6-7 on page 6-20).

Note: For information about e-mail protocols and ports, see "Customizing E-mail Protocol Scan Settings" on page 6-4.

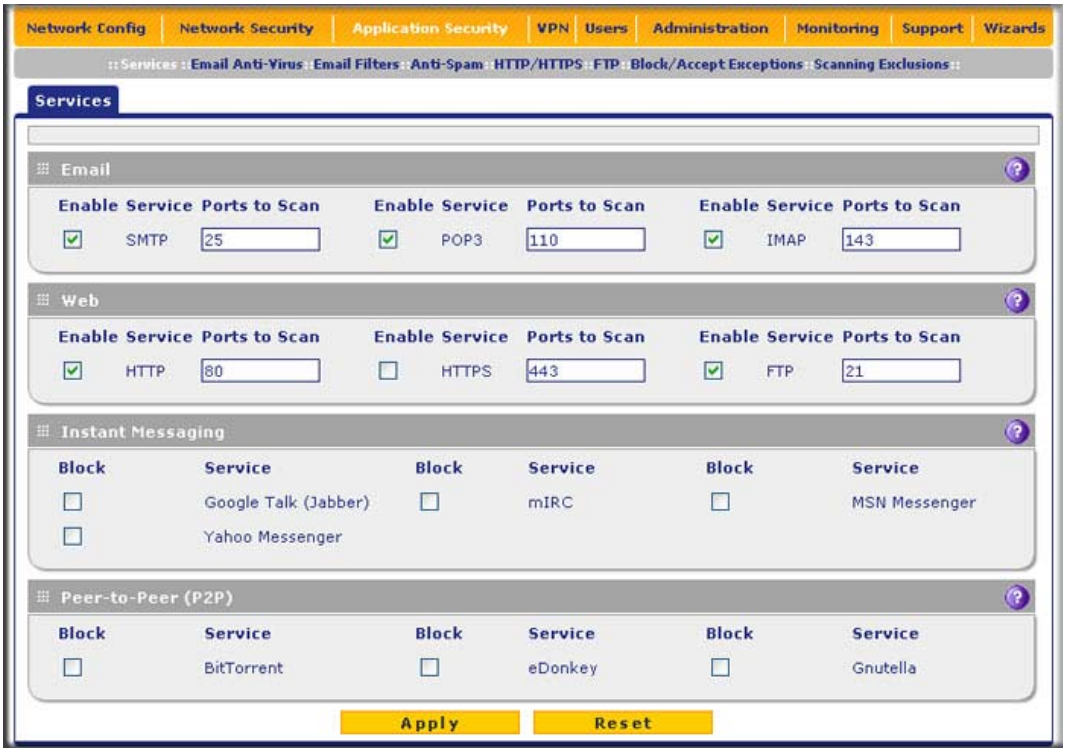


Figure 6-7

2. Enter the settings as explained in Table 6-5.

Table 6-6. Web Protocol, Instant Messaging, and Peer-to-Peer Settings

Setting	Description (or Subfield and Description)
Web	
HTTP	Select the **HTTP** checkbox to enable Hypertext Transfer Protocol (HTTP) scanning. This service is enabled by default and uses default port 80.
HTTPS	Select the **HTTPS** checkbox 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** checkbox to enable File Transfer Protocol (FTP). This service is enabled by default and uses default port 21.

Table 6-6. Web Protocol, Instant Messaging, and Peer-to-Peer Settings (continued)

Setting	Description (or Subfield and Description)
Note: If a protocol uses a port other than the standard service port (for example, port 80 for HTTP), enter this non-standard 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 (Jabber)	Select the corresponding checkboxes to block any of these common instant messaging services, all of which are allowed by default. **Note:** For Instant Messaging services, the following services can be blocked: logging in, sharing files, sharing video, sharing audio, and text messaging.
Yahoo messenger	
mIRC	
MSN Messenger	
Peer-to-Peer (P2P)	
BitTorrent	Select the corresponding checkboxes to block any of these common peer-to-peer file sharing services, all of which are allowed by default.
eDonkey	
Gnutella	

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

Configuring 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 6-1 on page 6-2) and send notifications, e-mails, or both to the end users.

To configure the Web-based malware settings:

1. Select **Application Security** > **HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view (see Figure 6-8 on page 6-22).

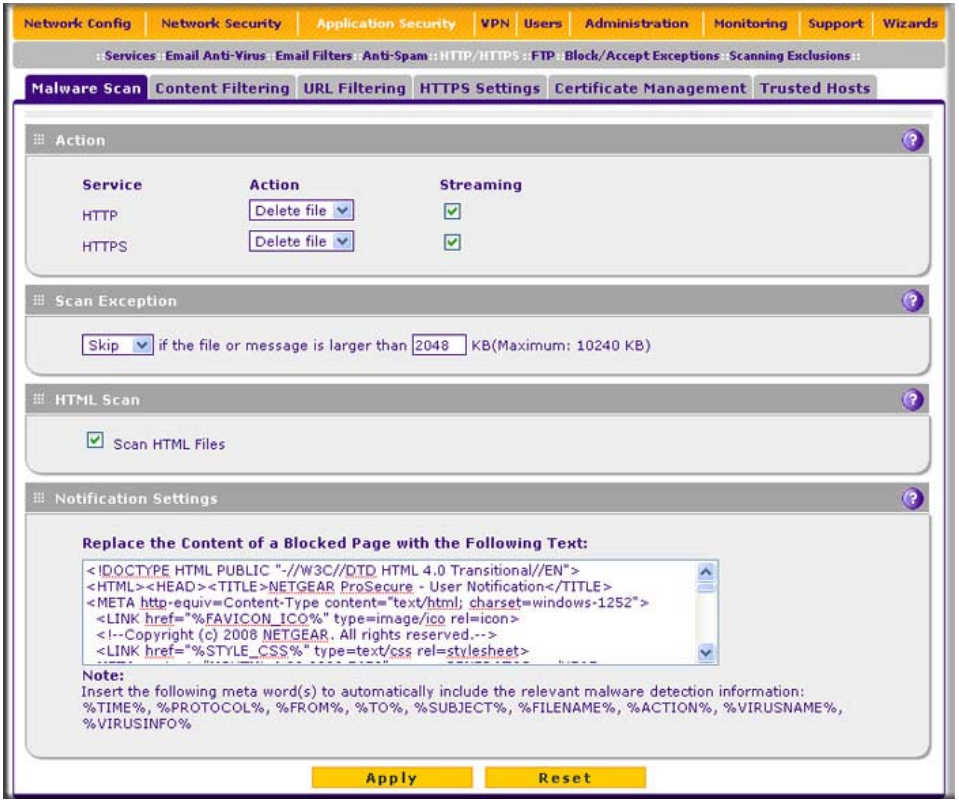


Figure 6-8

2. Enter the settings as explained in Table 6-2.

Table 6-7. Malware Scan Settings

Setting	Description (or Subfield and Description)	
Action		
HTTP and HTTPS	Action	From the **HTTP** or **HTTPS** pull-down menu, specify one of the following actions 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.
	Streaming	Select the **Streaming** checkbox 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 6-7. Malware Scan Settings (continued)

Setting	Description (or Subfield and Description)
Scan Exception	
The default maximum file or object size that are 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 10-1). From the pull-down menu, specify one of the following actions 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	elect this checkbox 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% meta word in a message to enable the UTM to insert the proper malware information. In addition to the %VIRUSINFO% meta word, you can insert the following meta words in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.	

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

Configuring Web Content Filtering

If you want to restrict internal LAN users from access 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 E-mail and Web Scan Settings" on page 6-2, all requested traffic from any Web site is allowed. You can specify a message such as "Blocked by NETGEAR" that is displayed on screen if a LAN user attempts to access a blocked site (see the Notification Settings section that is described at the bottom of Table 6-8 on page 6-28).

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 Web site 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 Web sites 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 “Configuring Web URL Filtering” on page 6-30), 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 Java scripts. Even sites on the whitelist (see “Configuring Web URL Filtering” on page 6-30) 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 “Specifying Trusted Hosts” on page 6-37). 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 "Configuring Web URL Filtering" on page 6-30). 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** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.
2. Click the **Content Filtering** submenu tab. The Content Filtering screen displays. Because of the large size of this screen, it is presented in this manual in three figures (Figure 6-9 on this page, Figure 6-10 on page 6-26, and Figure 6-11 on page 6-27).

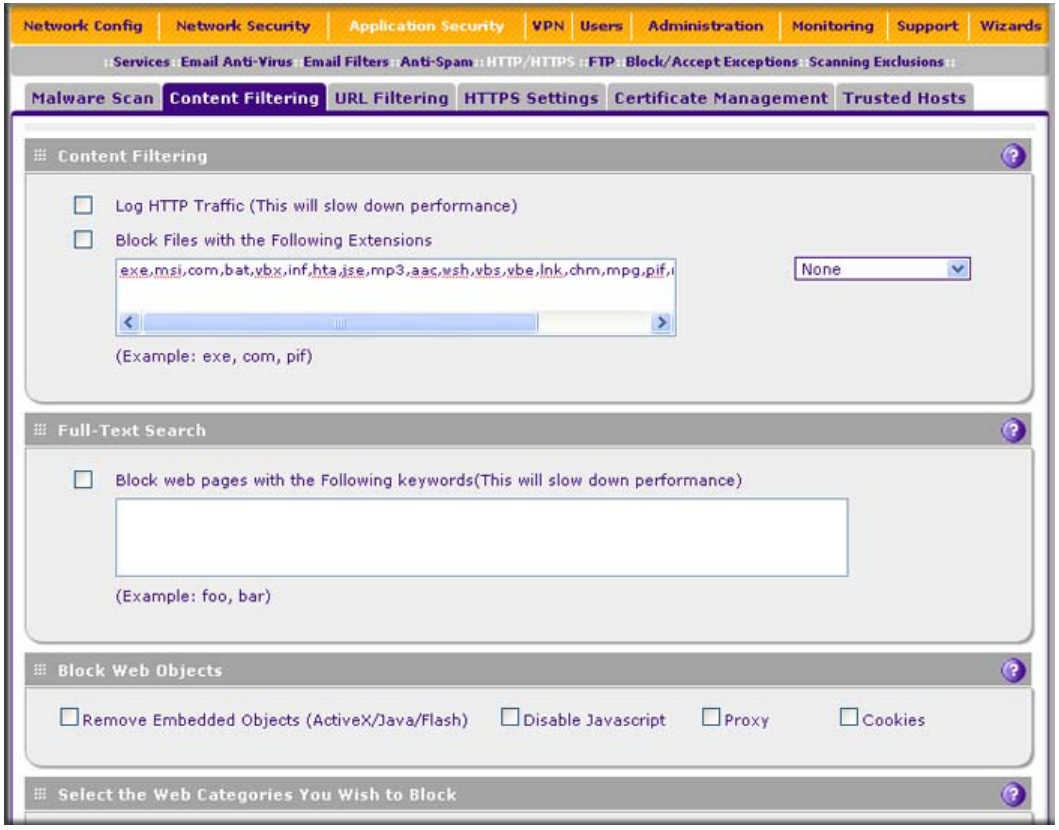


Figure 6-9 [Content Filtering, screen 1 of 3]

Figure 6-10 [Content Filtering, screen 2 of 3]

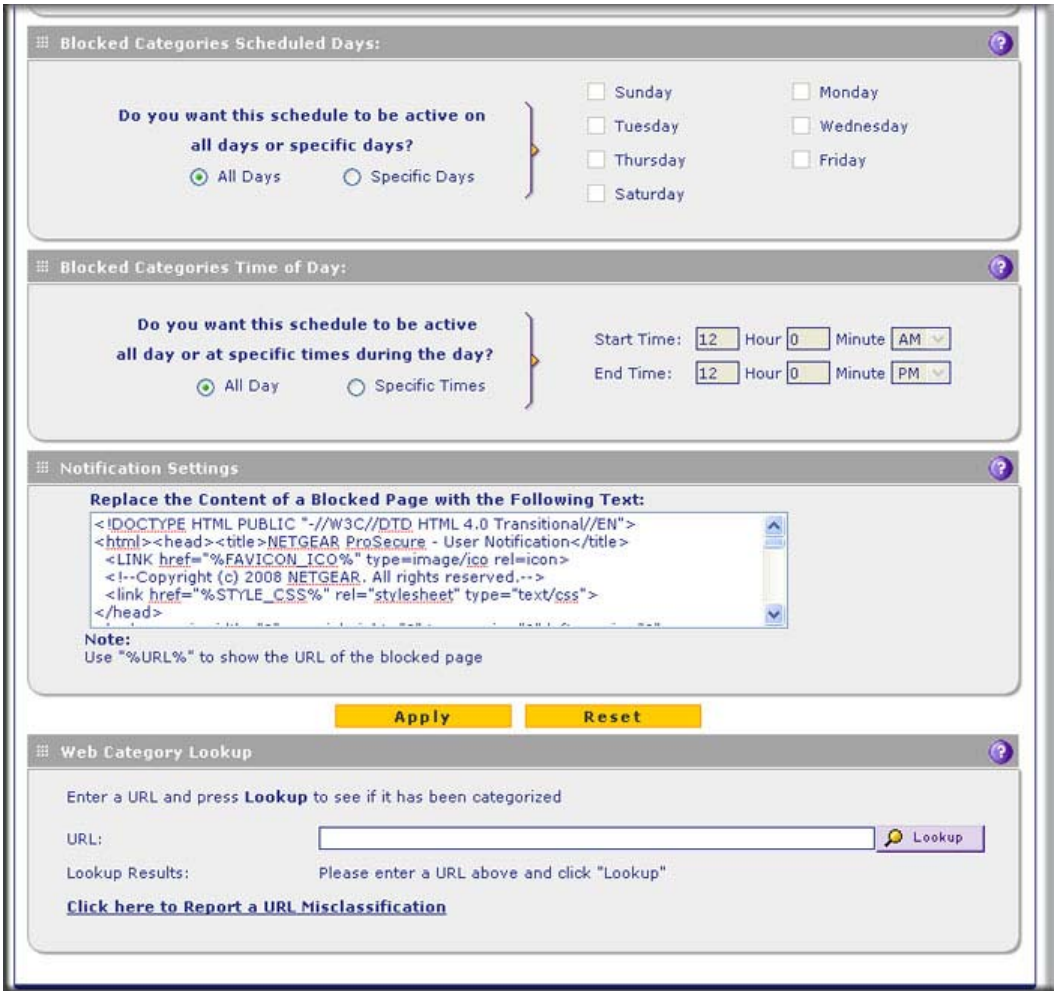


Figure 6-11 [Content Filtering, screen 3 of 3]

3. Enter the settings as explained in Table 6-8 on page 6-28.

Table 6-8. Content Filtering Settings

Setting	Description (or Subfield and Description)
Content Filtering	
Log HTTP Traffic	Select this checkbox to log HTTP traffic. For information about how to view the logged traffic, see "Querying Logs and Generating Reports" on page 11-32. By default, HTTP traffic is not logged. **Note**: Logging HTTP traffic might affect the UTM's performance (see "Performance Management" on page 10-1).
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 pull-down menu 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**: This is keyword blocking.	
Block web pages with the Following keywords	Select the checkbox 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 10-1).
Block Web Objects Select any or all of the following checkboxes:	
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 Web sites, 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 6-8. Content Filtering Settings (continued)

Setting	Description (or Subfield and Description)
Select the Web Categories You Wish to Block	
Select the **Enable Blocking** checkbox to enable blocking of Web categories. By default, this checkbox is deselected. Select the checkboxes 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 6-1 on page 6-2 for information about the Web categories that are blocked by default. Categories that are preceded by a green rectangular are allowed by default; categories that are preceded by a pink rectangular 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 active only on specific days. To the right of the radio buttons, select the checkbox 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 active only on specific hours of the selected day or days. To the right of the radio buttons, specify 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% **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% meta words 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.	

Table 6-8. Content Filtering Settings (continued)

Setting	Description (or Subfield and 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 appears 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 must be categorized from the pull-down menu. Then enter the **Submit** button.

4. 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 hyperlink to submit a URL misclassifiation. To submit a misclassified or uncategorized URL to NETGEAR for analysis, click on the **Click here to Report a URL Misclassification** hyperlink. A second screen opens that allows you to select from pull-down menus up to two categories in which you think that the URL could be categorized. Then click the **Submit** button.

Configuring Web URL Filtering

If you want to allow or block internal LAN users from access 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** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.
2. Click the **URL Filtering** submenu tab. The URL Filtering screen displays. (Figure 6-12 shows some examples.)

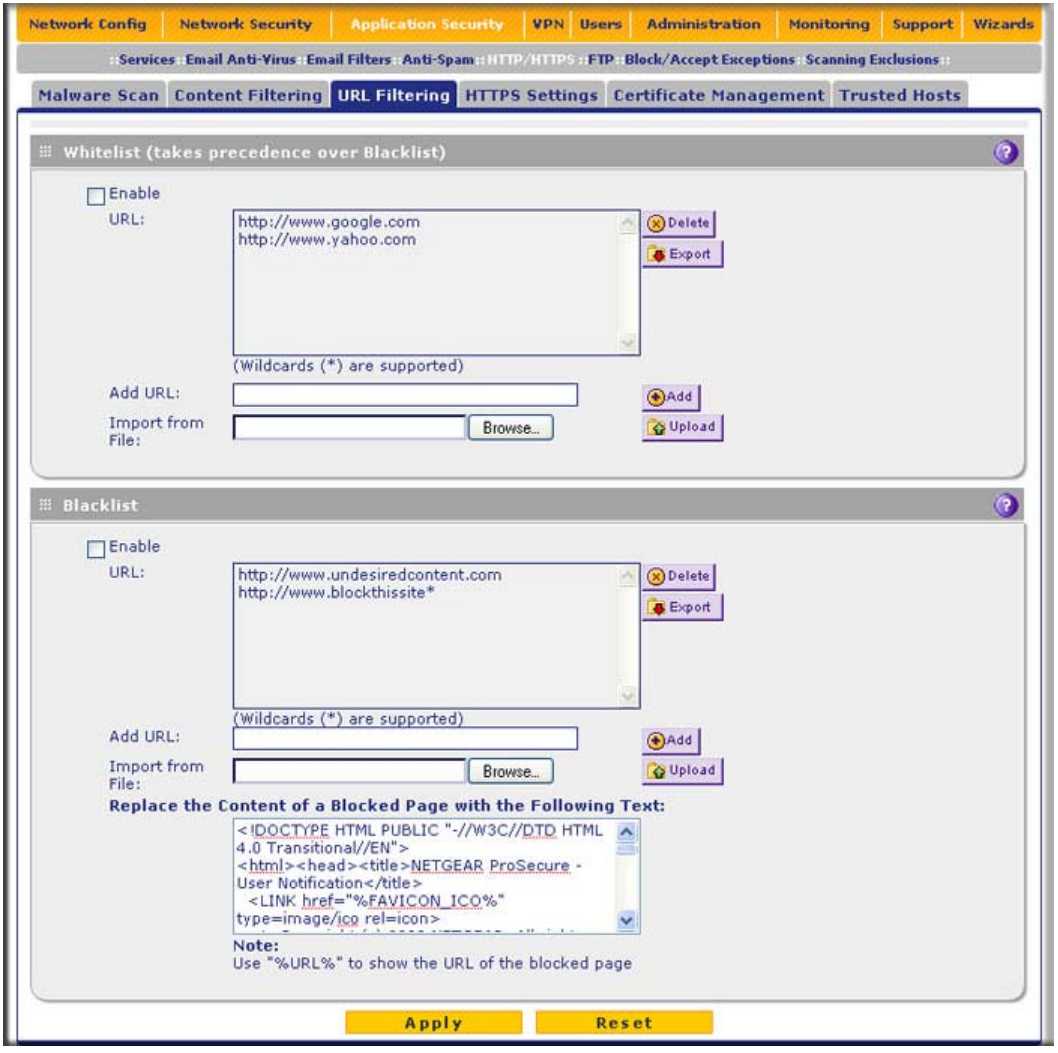


Figure 6-12

3. Enter the settings as explained in Table 6-9.

Table 6-9. URL Filtering Settings

Setting	Description (or Subfield and Description)	
Whitelist		
Enable	Select this checkbox 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 below). 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.	
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 checkbox to block the URLs that are listed in the URL field. Users attempting to access these URLs receive a notification (see below).	

Table 6-9. URL Filtering Settings (continued)

Setting	Description (or Subfield and Description)	
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 below). 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 blocked and any URL that ends with “.com” is blocked.	
	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.	
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% **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% meta word in the text to enable the UTM to insert the blocked URL in the notification text.	

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

HTTPS Scan Settings

HTTPS traffic is encrypted traffic that cannot be scanned otherwise the data stream would not be secure. However, the UTM can scan HTTPS traffic that is transmitted through an HTTP proxy, that is, HTTPS traffic is scanned as a proxy between the HTTPS client and the HTTPS server. Figure 6-13 shows the HTTPS scanning traffic flow.

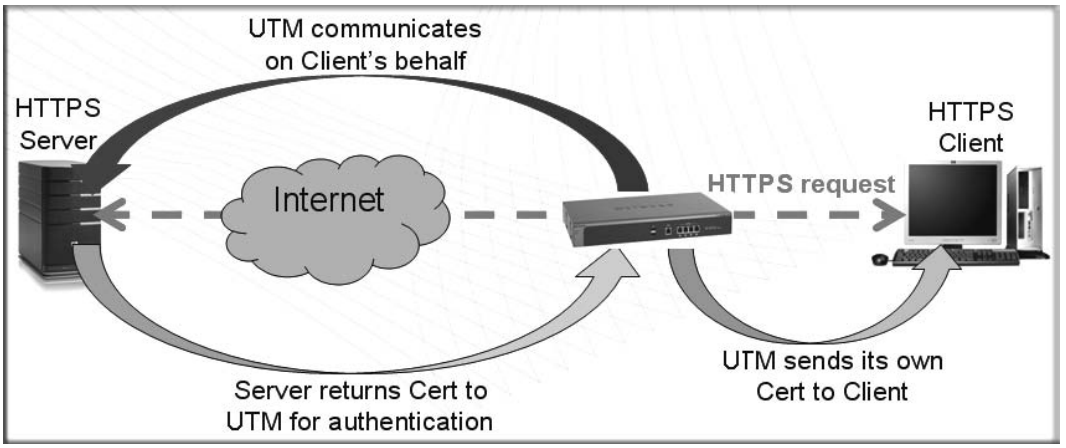


Figure 6-13

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 Web site?

If one of these is not satisfied, a security alert message appears in the browser window (see Figure 6-14).

Figure 6-14

However, even when a certificate is trusted or still valid, or when the name of a certificate does match the name of the Web site, a security alert message still appears 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 appearing, install a root certificate on the client PC. The root certificate can be downloaded from the UTM's Manager Login screen (see Figure 2-1 on page 2-3).

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 must 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 "Managing Digital Certificates" on page 9-17.

You can specify trusted hosts for which the UTM bypasses HTTPS traffic scanning. For more information, see "Specifying Trusted Hosts" on page 6-37.

To configure the HTTPS scan settings:

1. Select **Application Security** > **HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.
2. Click the **HTTPS Settings** submenu tab. The HTTPS Settings screen displays.

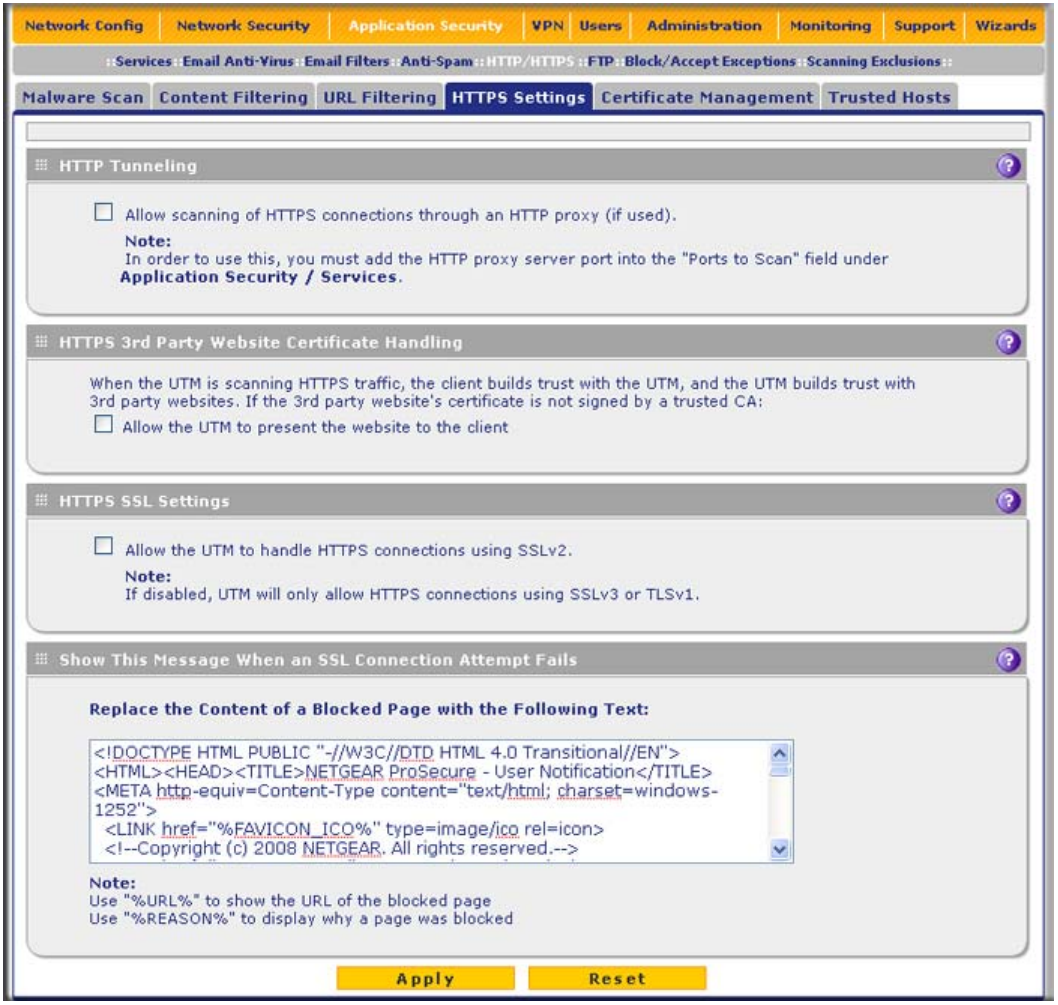


Figure 6-15

3. Enter the settings as explained in Table 6-10 on page 6-37.

Table 6-10. HTTPS Settings

Setting	Description (or Subfield and Description)
HTTP Tunneling	
Select this checkbox to allow scanning of HTTPS connections through an HTTP proxy, which is disabled by default. Traffic from trusted hosts is not scanned (see "Specifying Trusted Hosts" on page 6-37). **Note**: For HTTPS scanning to occur properly, you must add the HTTP proxy server port in the Ports to Scan field for the HTTPS service on the Services screen (see "Customizing Web Protocol Scan Settings and Services" on page 6-19).	
HTTPS 3rd Party Website Certificate Handling	
Select the **Allow the UTM to present the website to the client** checkbox to allow a Secure Sockets Layer (SSL) connection with a valid certificate that is not signed by a trusted certificate authority (CA). The default setting is to block such as a connection.	
HTTPS SSL Settings	
Select the **Allow the UTM to handle HTTPS connections using SSLv2** checkbox to allow HTTPS connections using SSLv2, SSLv3, or TLSv1. If this checkbox is deselected, 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% meta words in a message to enable the UTM to insert the proper URL information and the reason of the rejection.	

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

Note: For information about certificates that are used for SSL connections and HTTPS traffic, see "Managing Digital Certificates" on page 9-17.

Specifying 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 "Managing Self Certificates" on page 9-20.

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 must 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** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.
2. Click the **Trusted Hosts** submenu tab. The Trusted Hosts screen displays. (Figure 6-16 shows some examples.)

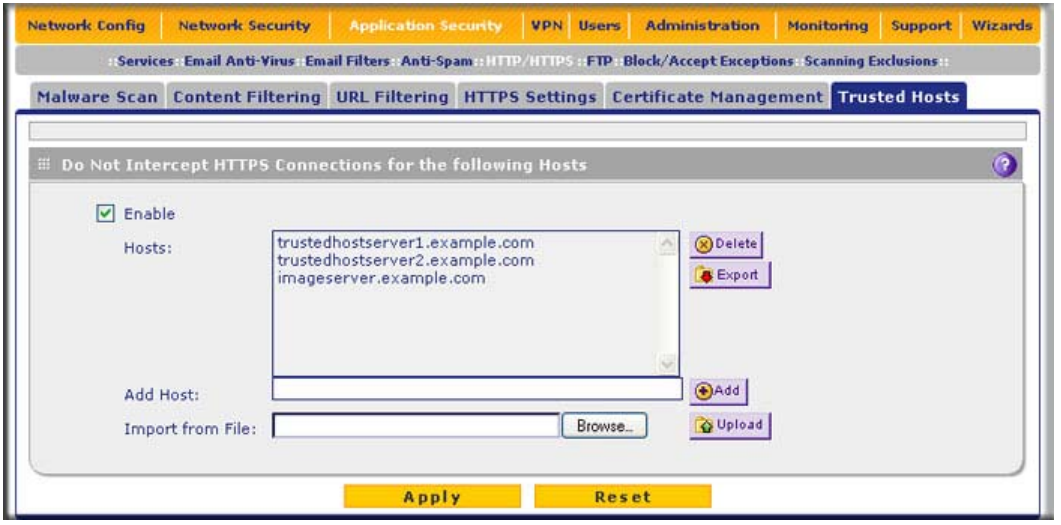


Figure 6-16

3. Enter the settings as explained in Table 6-11.

Table 6-11. Trusted Hosts Settings

Setting	Description (or Subfield and Description)	
Do Not Intercept HTTPS Connections for the following Hosts		
Enable	Select this checkbox 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 Host field.	
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 below). 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 Host field.	
Import from File	To import a list with trusted hosts into the Host 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 Host field. **Note**: Any existing hosts in the Host field are overwritten when you import a list of hosts from a file.	

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

Configuring 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** from the menu. The FTP screen displays.

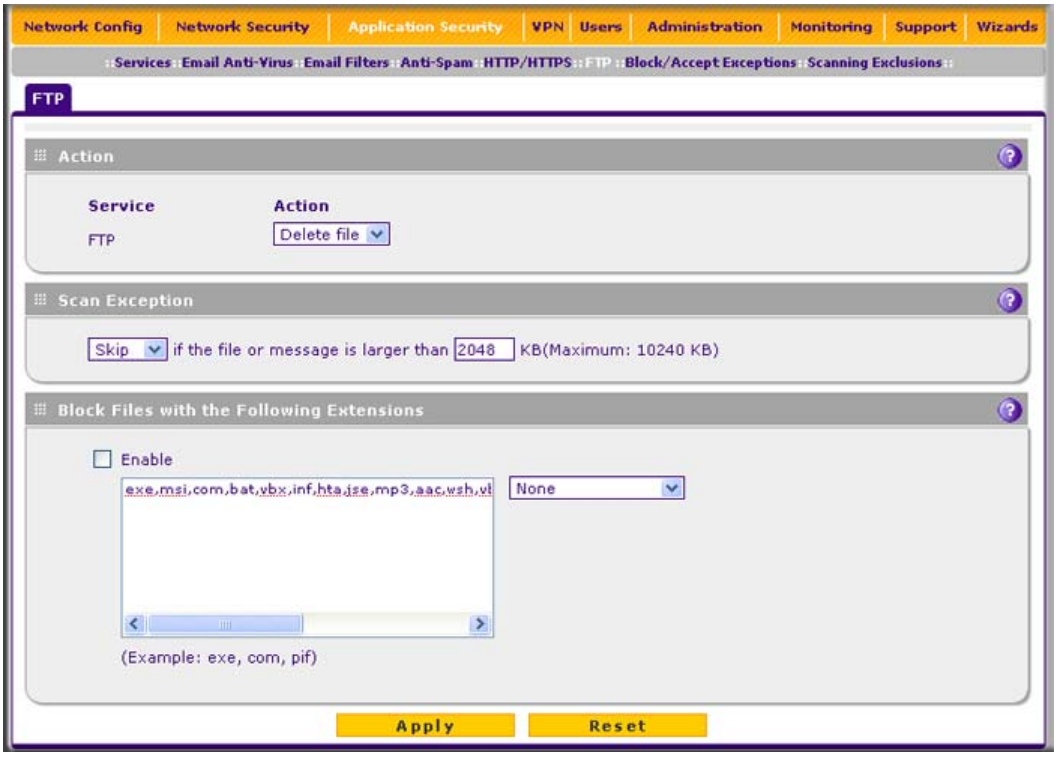


Figure 6-17

2. Enter the settings as explained in Table 6-12.

Table 6-12. FTP Scan Settings

Setting	Description (or Subfield and Description)	
Action		
FTP	Action	From the **FTP** pull-down menu, specify one of the following actions 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.

Table 6-12. FTP Scan Settings (continued)

Setting	Description (or Subfield and Description)
Scan Exception	
The default maximum file or object size 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 10-1). From the pull-down menu, specify one of the following actions 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.	
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 pull-down menu 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.

Setting Web Access Exceptions and Scanning Exclusions

After you have specified which content the UTM filters, you can set exception rules for users of certain LAN groups. Similarly, 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.

Setting Web Access Exception Rules

You can set exception rules for members of a LAN group to allow access to applications, Web categories, and URLs that you have blocked for all other users, or the other way around, to block access to applications, Web categories, and URLs that you have allowed access to for all other users. To specify members of a LAN group and to customize LAN group names, see "Managing Groups and Hosts (LAN Groups)" on page 4-12.

To set Web access exception rules:

1. Select **Application Security** > **Block/Accept Exceptions** from the menu. The Block/Accept Exceptions screen displays. This screen shows the Exceptions table, which is empty if you have not specified any exception rules. (Figure 6-18 shows three exception rules in the Exceptions table as an example.)

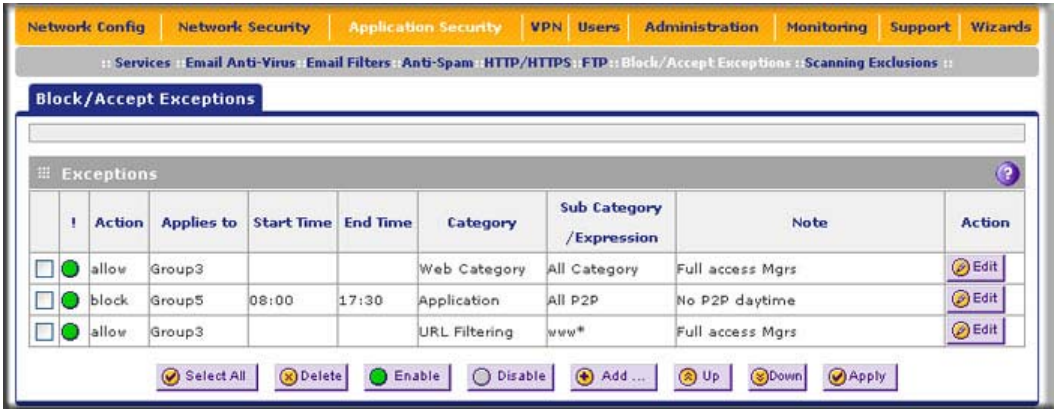


Figure 6-18

2. Under the Exceptions table, click the **Add** table button to specify an exception rule. The Add or Edit Block/Accept Exceptions screen displays.

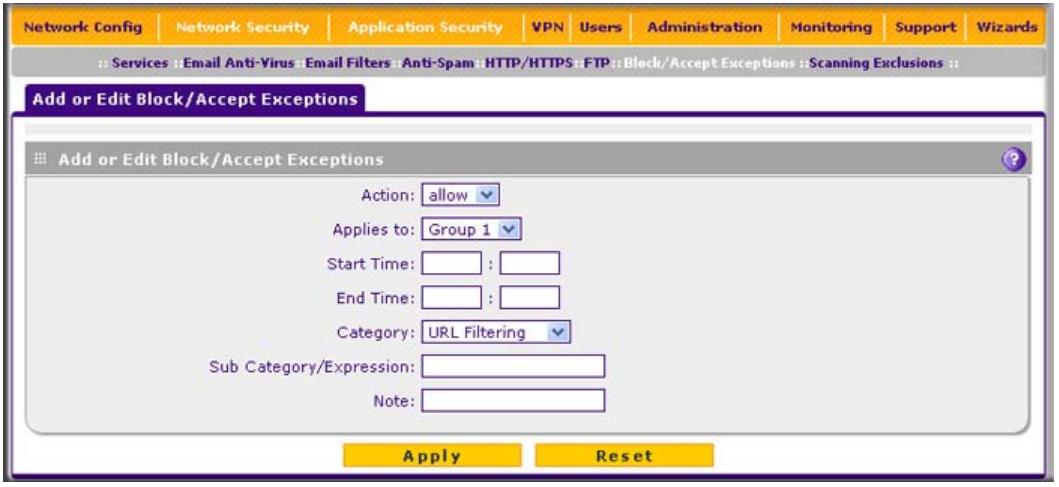


Figure 6-19

3. Enter the settings as explained in Table 6-13.

Table 6-13. Add and Edit Block Scanning Exception Settings

Setting	Description (or Subfield and Description)
Action	From the pull-down menu, 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.
Applies to	The group to which the exception applies. you can configure groups in "Managing Groups and Hosts (LAN Groups)" on page 4-12.
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	From the pull-down menu, select the category to which the action applies: • **URL Filtering**. The action applies to a URL. Enter the URL in the Subcategory/ Expression field. • **Web category**. The action applies to a Web category. Select a category from the Subcategory/Expression pull-down menu. • **Application**. The action applies to an application. Select an application from the Subcategory/Expression pull-down menu.
Subcategory/ Expression	The nature of the Subcategory/Expression field depends on your selection from the Category pull-down menu. • **When you select URL Filtering**: The Subcategory/Expression field becomes a blank field in which you can enter a full or partial URL. • **When you select Web category**: The Subcategory/Expression field becomes a pull-down menu that lets you select a Web category. • **When you select Application**: The Subcategory/Expression field becomes a pull-down menu that lets you select an application.
Notes	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.
5. Select the checkbox to the left of the rule that you want to enable or click the **Select All** table button to select all rules.
6. Click the **Apply** table button to enable the selected rule or rules.

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 Exceptions screen displays (see Figure 6-18 on page 6-42).

2. Modify the settings that you wish to change (see Table 6-13 on page 6-43).
3. Click **Apply** to save your changes. The modified exception rule is displayed in the Exceptions table.

To delete or disable one or more exception rules:

1. Select the checkbox to the left of the 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 grey circle, indicating that the rule is or rules are disabled. (By default, when a rule is added to the table, it is automatically 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. To change the position of the rules in the table, click 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.

Setting Scanning Exclusions

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** from the menu. The Scanning Exclusions screen displays. This screen shows the Scanning Exclusions table, which is empty if you have not specified any exclusions. (Figure 6-20 on page 6-45 shows one exclusion rule in the table as an example.)

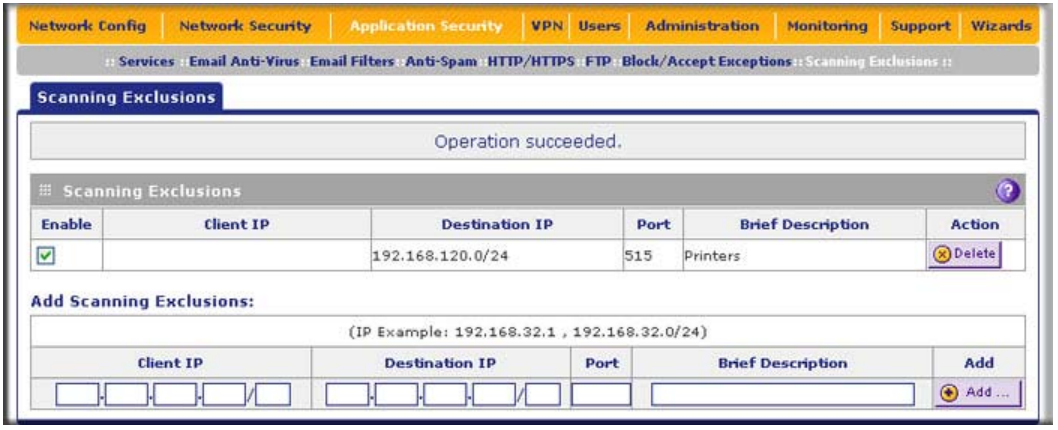


Figure 6-20

2. In the Add Scanning Exclusions section of the screen, specify an exclusion rule as explained in Table 6-14.

Table 6-14. Add Scanning Exclusion Settings

Setting	Description (or Subfield and Description)
Client IP	The client IP address and optional subnet mask that are excluded from all scanning.
Destination IP	The destination IP address and optional subnet mask that are excluded from all scanning.
Port	The port number that is excluded from all scanning.
Brief Description	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 checkbox 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.

Chapter 7
Virtual Private Networking Using IPsec Connections

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 (Dual-WAN Port Models Only)

On the dual-WAN port models only, if both of the 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 must be configured.

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. A 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 (VPNs)” on page B-9 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 “Configuring Dynamic DNS” on page 3-19. For information about WAN mode configuration, see “Configuring the WAN Mode (Required for Dual-WAN Port Models Only)” on page 3-9.

The diagrams and table below show how the WAN mode selection relates to VPN configuration.

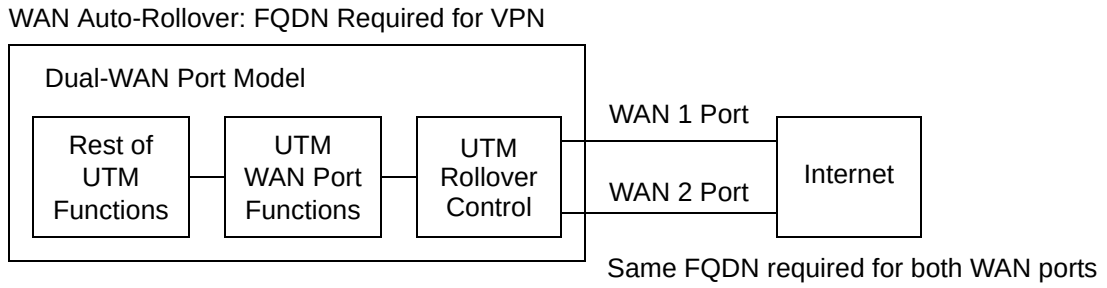


Figure 7-1

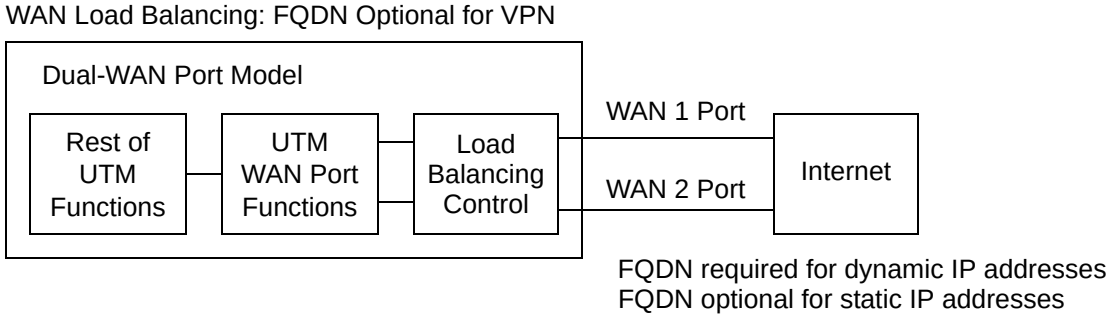


Figure 7-2

Table 7-1 summarizes the WAN addressing requirements (FQDN or IP address) for a VPN tunnel in either dual WAN mode.

Table 7-1. 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 7-1. IP Addressing for VPNs in Dual WAN Port Systems

Configuration and WAN IP address		Rollover Mode[a]	Load Balancing Mode
VPN “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. All tunnels must be re-established after a rollover using the new WAN IP address.

Using 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 section below 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 all settings on both sides of the VPN tunnel 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 multi-vendor VPN interoperability.

Creating Gateway-to-Gateway VPN Tunnels with the Wizard

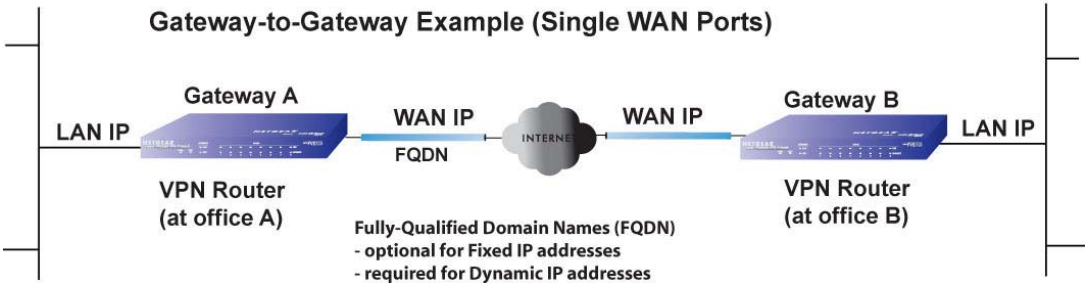


Figure 7-3

To set up a gateway-to-gateway VPN tunnel using the VPN Wizard.

1. Select **VPN** > **IPsec VPN** from the menu. The IPsec VPN submenu tabs appear, with the IKE Policies screen in view.
2. Click the **VPN Wizard** submenu tab. The VPN Wizard screen displays (see Figure 7-4 on page 7-5, which contains some examples for the dual-WAN port models). The WAN1 and WAN2 radio buttons are shown on the VPN Wizard screen for the dual-WAN port models but not on the VPN Wizard screen for the single-WAN port models.

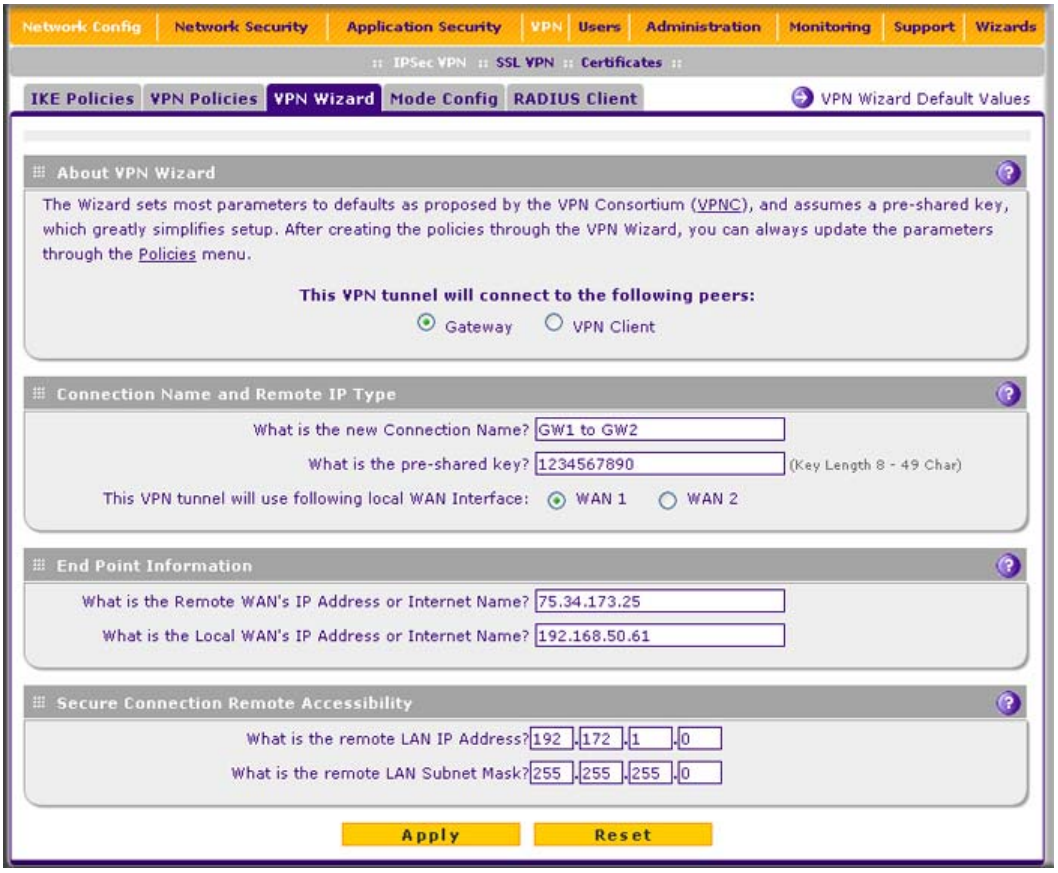


Figure 7-4

To view the wizard default settings, click the **VPN Wizard Default Values** option arrow at the top right of the screen. A popup window appears (see Figure 7-5 on page 7-6) displaying the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.

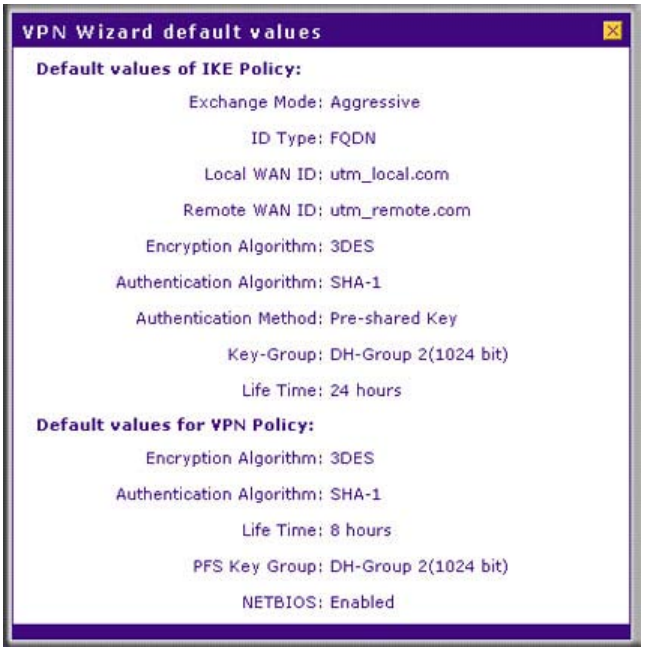


Figure 7-5

3. Select the radio buttons and complete the fields and as explained Table 7-2.

Table 7-2. (IPsec) VPN Wizard Settings for a Gateway-to-Gateway Tunnel

Setting	Description (or Subfield and 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 appears 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 must be entered both here and on the remote VPN gateway. This key must have a minimum length of 8 characters and should not exceed 49 characters.

Table 7-2. (IPsec) VPN Wizard Settings for a Gateway-to-Gateway Tunnel (continued)

Setting	Description (or Subfield and Description)
This VPN tunnel will use following local WAN Interface (dual-WAN port models only)	For the dual-WAN port models only, select one of the two radio buttons (**WAN1** or **WAN2**) to specify which local WAN interface the VPN tunnel uses as the local endpoint. **Note**: If a dual-WAN port model is configured to function in WAN auto-rollover mode, after completing the wizard, you must manually update the VPN policy to enable VPN rollover. For more information, see "Manually Adding or Editing a VPN Policy" on page 7-33.
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 must 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 assure tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keepalive which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive. For more information, see "The VPN Policies Screen" on page 7-31.

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.

4. 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.

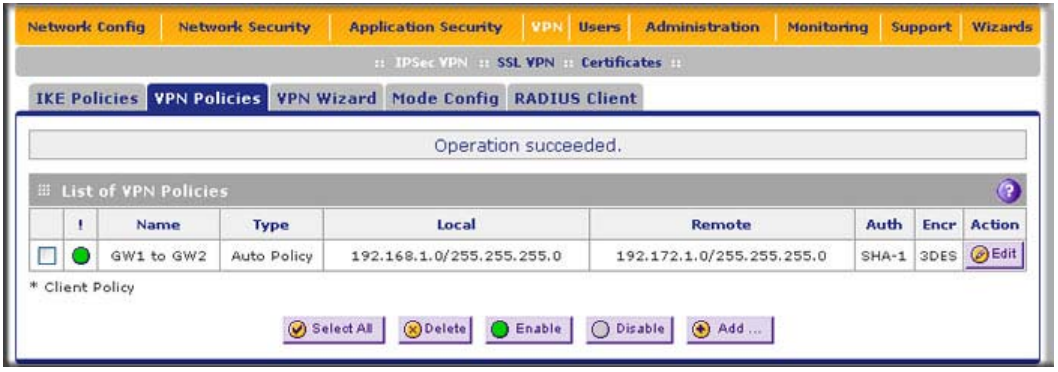


Figure 7-6

5. Configure a VPN policy on the remote gateway that allows connection to the UTM.
6. Activate the IPsec VPN connection:
   a. Select **Monitoring** > **Active Users & VPNs** from the menu. The Active Users & VPNs submenu tabs appear, with the Active Users screen in view.
   b. Click the **IPSec VPN Connection Status** submenu tab. The IPSec VPN Connection Status screen displays.

Figure 7-7

   c. Locate the policy in the table, and click the **Connect** table button. The IPsec VPN connection should become active.

Note: When using FQDNs, if the dynamic DNS service is slow to update their 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.

Creating a Client to Gateway VPN Tunnel

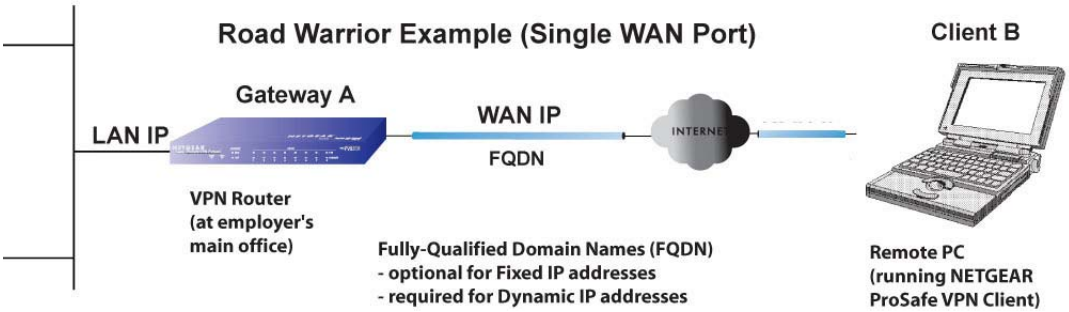


Figure 7-8

Follow the steps in the following sections to configure a VPN client tunnel:

- “Using the VPN Wizard Configure the Gateway for a Client Tunnel” on page 7-9.
- “Using the NETGEAR VPN Client Security Policy Editor to Create a Secure Connection” on page 7-12.

Using the VPN Wizard 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** from the menu. The IPsec VPN submenu tabs appear, with the IKE Policies screen in view.
2. Click the **VPN Wizard** submenu tab. The VPN Wizard screen displays (see Figure 7-9 on page 7-10, which contains some examples for a dual-WAN port model). The WAN1 and WAN2 radio buttons are shown on the VPN Wizard screen for the dual-WAN port models but not on the VPN Wizard screen for the single-WAN port models.

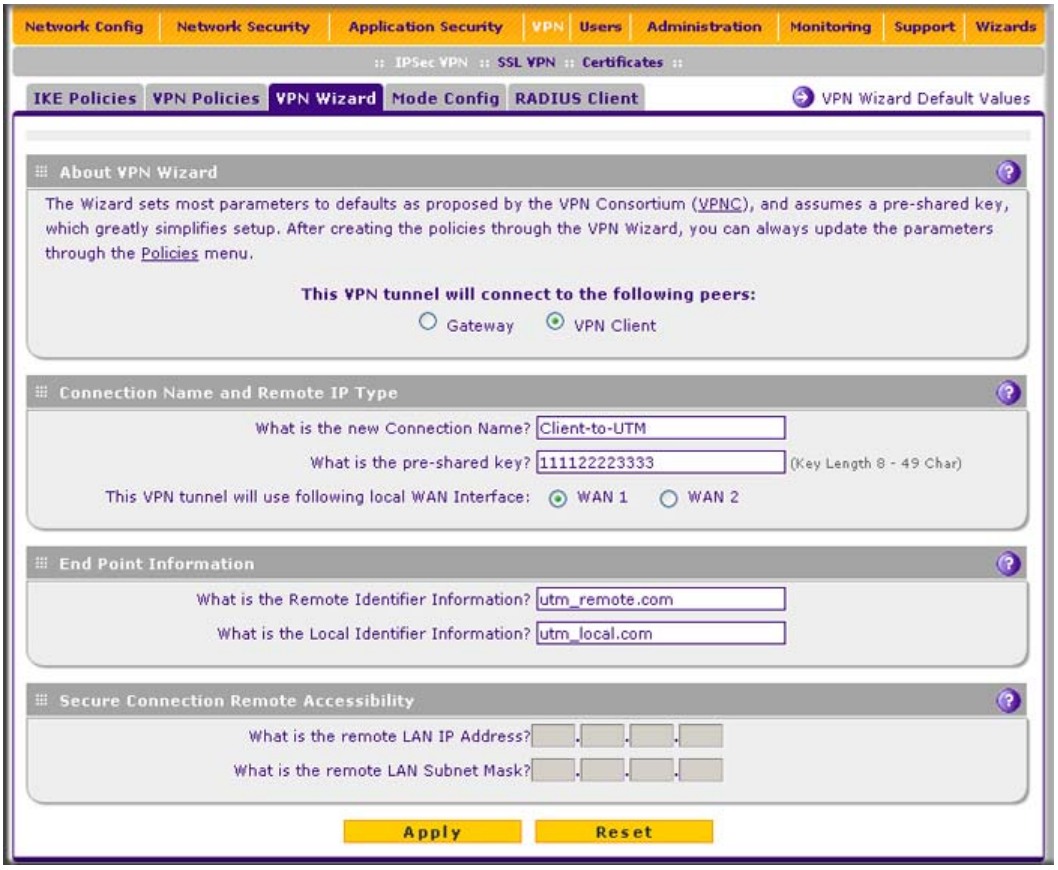


Figure 7-9

To display the wizard default settings, click the **VPN Wizard Default Values** option arrow at the top right of the screen. A popup window appears (see Figure 7-5 on page 7-6), displaying the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.

3. Select the radio buttons and complete the fields and as explained Table 7-3.

Table 7-3. (IPsec) VPN Wizard Settings for a Client-to-Gateway Tunnel

Setting	Description (or Subfield and 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) appear 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 must be entered both here and on the remote VPN gateway, or the remote VPN client. This key must have a minimum length of 8 characters and should not exceed 49 characters.
This VPN tunnel will use following local WAN Interface (dual-WAN port models only)	For the dual-WAN port models only, select one of the two radio buttons (**WAN1** or **WAN2**) to specify which local WAN interface the VPN tunnel uses as the local endpoint. **Note**: If a dual-WAN port model is configured to function in WAN auto-rollover mode, after completing the wizard, you must manually update the VPN policy to enable VPN rollover. For more information, see "Manually Adding or Editing a VPN Policy" on page 7-33.
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 a FQDN is not supported.

4. 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.

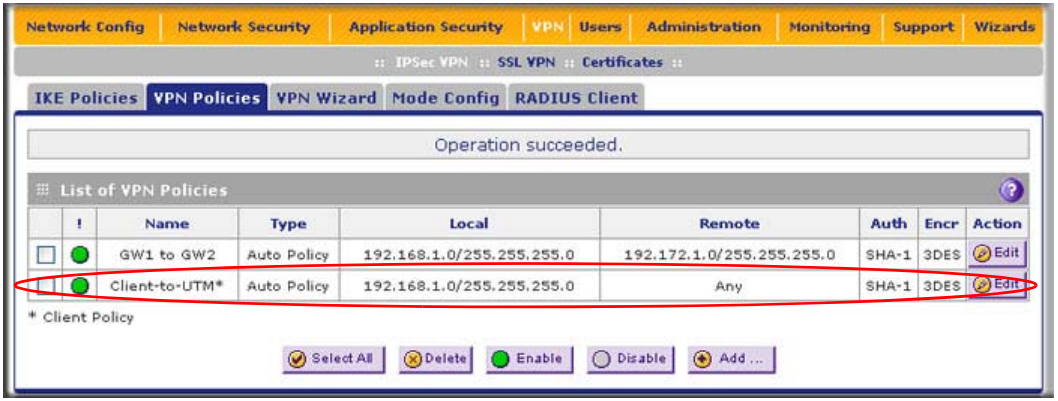


Figure 7-10

	Note: When using FQDNs, if the dynamic DNS service is slow to update their 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.

Using the NETGEAR VPN Client Security Policy Editor to Create a Secure Connection

From a PC with the NETGEAR ProSafe VPN Client installed, configure a VPN client policy to connect to the UTM:

1. Right-click on the VPN client icon in your Windows toolbar, select **Security Policy Editor**. Then, select **Options** > **Secure**, and verify that the Specified Connections selection is enabled (see Figure 7-11 on page 7-13).

Figure 7-11

2. In the upper left of the Policy Editor window, click the **New Connection** icon (the first icon on the left) to open a new connection. Give the new connection a name; in this example, we are using UTM_SJ.

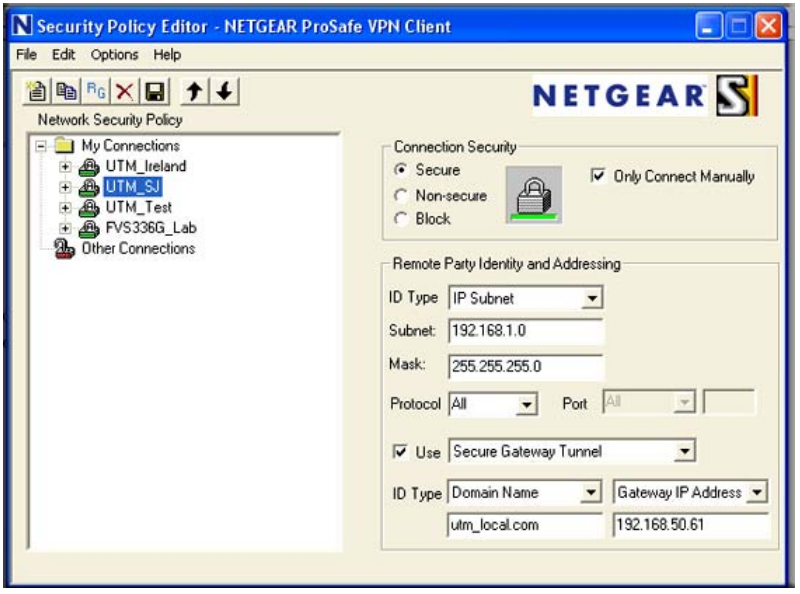


Figure 7-12

3. Enter the settings as explained in Table 7-4.

Table 7-4. Security Policy Editor: Remote Party Settings

Setting	Description (or Subfield and Description)	
Connection Security	Select the **Secure** radio button. If you want to connect manually only, select the **Only Connect Manually** checkbox.	
ID Type	From the pull-down menu, select **IP Subnet**.	
Subnet	Enter the LAN IP subnet address of the UTM that is displayed on the UTM's VPN Policies screen (see Figure 7-10 on page 7-12). In this example, the subnet address is 192.168.1.0.	
Mask	Enter the LAN IP subnet mask of the UTM that is displayed on the UTM's VPN Policies screen (see Figure 7-10 on page 7-12). In this example, the subnet mask is 255.255.255.0.	
Protocol	From the pull-down menu, select **All**.	
Use	Select the **Use** checkbox. Then, from the pull-down menu, select **Secure Gateway Tunnel**.	
ID Type	Left pull-down menu	From the left pull-down menu, select **Domain Name**. Then, below, enter the local FQDN that you entered on the UTM's VPN Wizard screen (see Figure 7-9 on page 7-10). In this example, the domain name is utm_local.com.
	Right pull-down menu	From the right pull-down menu, select **Gateway IP Address**. Then, below, enter the IP address of the WAN interface that you selected on the UTM's VPN Wizard screen (see Figure 7-9 on page 7-10). In this example, the WAN IP address is 192.168.50.61. **Note**: You can find the WAN IP address on the Connection Status screen for the selected WAN port. For more information, see "Viewing the WAN Ports Status" on page 11-27.

4. Click on the disk icon to save the configuration, or select **File** > **Save** from the Security Policy Editor menu.

5. In the left frame, click **My Identity**. The screen adjusts.

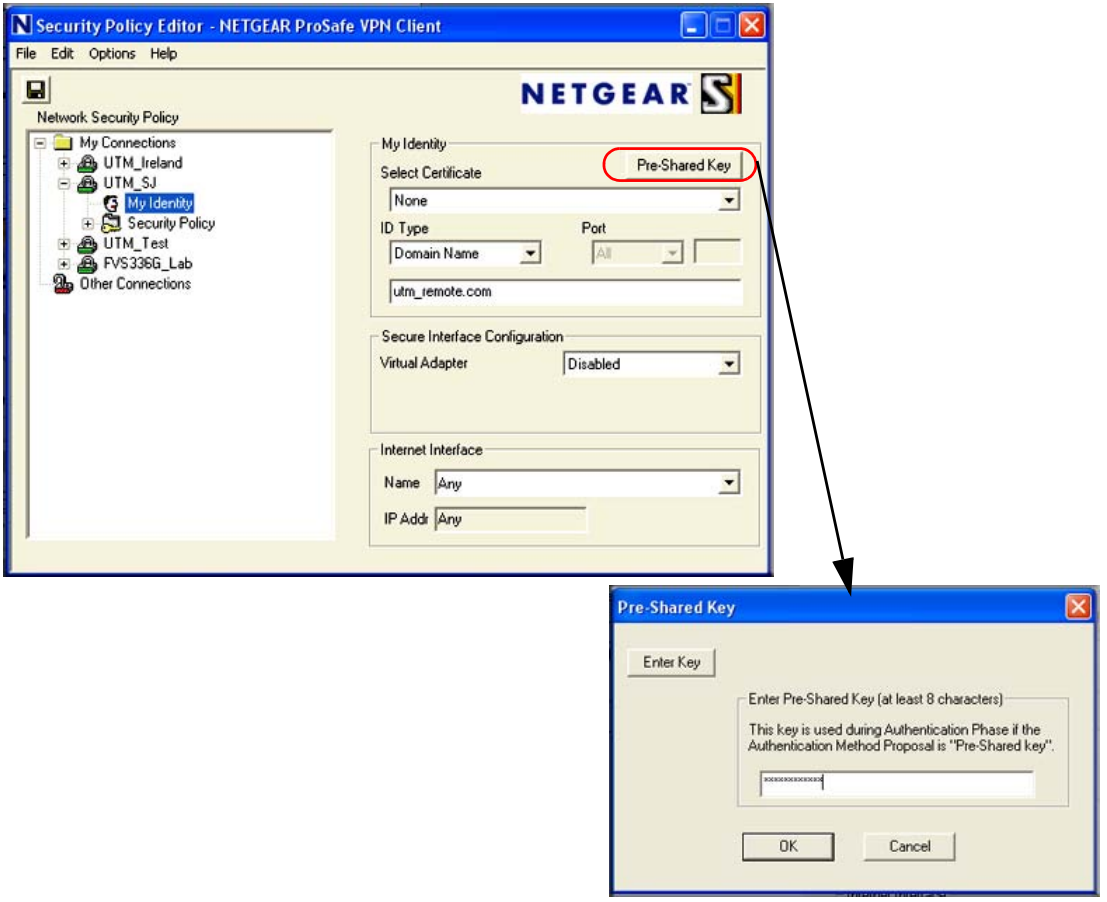


Figure 7-13

6. Enter the settings as explained in Table 7-5.

Table 7-5. Security Policy Editor: My Identity Settings

Setting	Description (or Subfield and Description)	
Select Certificate	From the pull-down menu, select **None**. The Pre-Shared Key window appears.	
	Pre-Shared Key	Enter the same pre-shared key that you specified on the UTM's VPN Wizard screen (see Figure 7-9 on page 7-10). In this example, the pre-shared key is 111122223333. However, the pre-shared key is masked for security.

Table 7-5. Security Policy Editor: My Identity Settings (continued)

Setting	Description (or Subfield and Description)
ID Type	From the pull-down menu, select **Domain Name**. Then, below, enter the remote FQDN that you entered on the UTM's VPN Wizard screen (see Figure 7-9 on page 7-10). In this example, the domain name is utm_remote.com.
Secure Interface Configuration	Leave the default setting, which is the **Disabled** selection from the Virtual Adapter pull-down menu.
Internet Interface	Leave the default setting, which is the **Any** selection from the Name pull-down menu.

7. Click on the disk icon to save the configuration, or select **File** > **Save** from the Security Policy Editor menu.

8. In the left frame, click **Security Policy**. The screen adjusts.

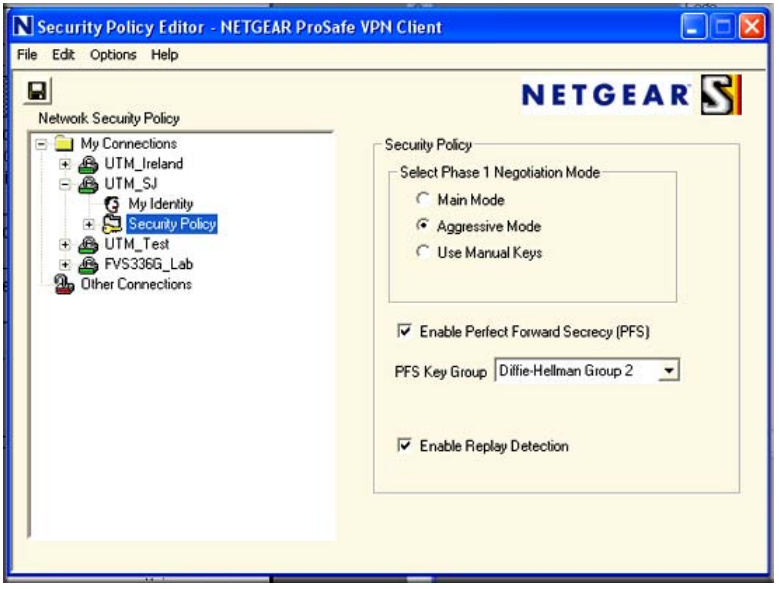


Figure 7-14

9. Enter the settings as explained in Table 7-6.

Table 7-6. Security Policy Editor: Security Policy Settings

Setting	Description (or Subfield and Description)
Select Phase 1 Negotiation Mode	Select the **Aggressive Mode** radio button.
Enable Perfect Forward Secrecy (PFS)	Select the **Enable Perfect Forward Secrecy (PFS)** checkbox. From the pull-down menu below, select **Diffie-Hellman Group 2**.
Enable Replay Detection	Leave the default setting, which is selection of the **Enable Replay Detection** checkbox.

10. Click on the disk icon to save the configuration, or select **File** > **Save** from the Security Policy Editor menu

11. Close the VPN ProSafe VPN client.

Note: You do not need to open or change the settings on the Authentication (Phase 1) screen or its accompanying Proposal 1 and Proposal 2 screens, nor on the Key Exchange (Phase 2) screen or its accompanying Proposal 1 screen. Leave the default settings for these screens.

Testing the Connections and Viewing 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.

Testing the VPN Connection

To test a client connection and view the status and log information, follow these steps.

To test the client connection, from your PC, right-click on the VPN client icon in your Windows toolbar, and then select the VPN connection that you want to test. In the example that is shown in Figure 7-15 on page 7-18, select **Connect...** > **My Connections\UTM_SJ**.

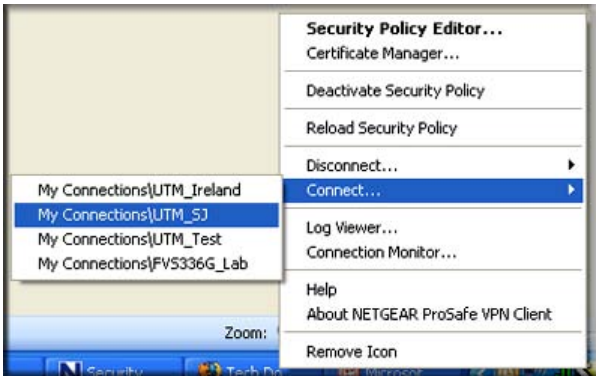


Figure 7-15

In the example that is shown in Figure 7-15, you should receive the message “Successfully connected to My Connections\UTM_SJ” within 30 seconds.

The VPN client icon in the system tray should say On: 

NETGEAR VPN Client Status and Log Information

To view more detailed additional status and troubleshooting information from the NETGEAR VPN client:

- Right-click the VPN Client icon in the system tray and select **Log Viewer** (see Figure 7-2 on page 7-2).

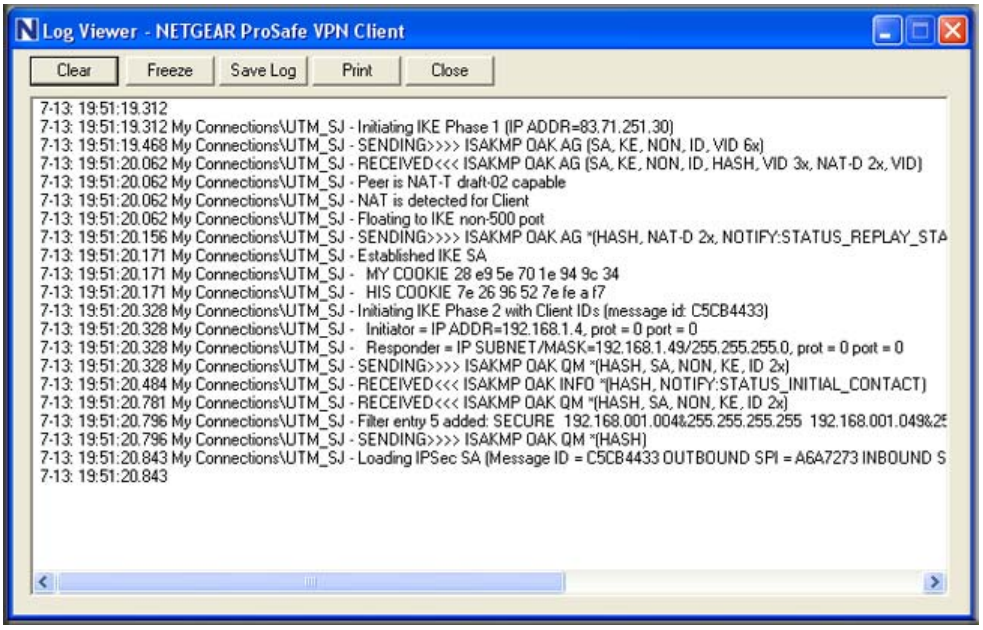


Figure 7-16

- Right-click the VPN Client icon in the system tray and select **Connection Monitor**.

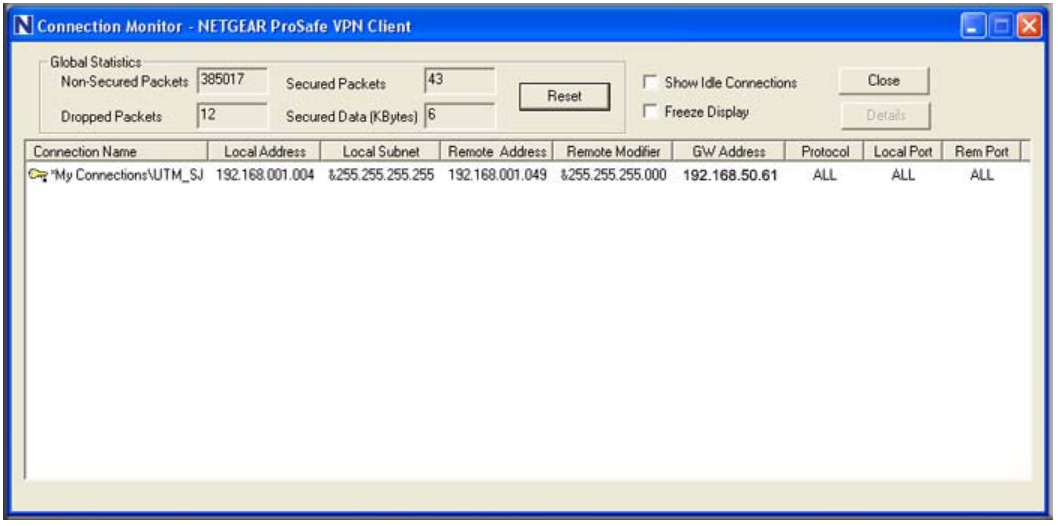


Figure 7-17

The VPN client system tray icon provides a variety of status indications, which are listed below.

Table 7-7. Status Indications for the VPN Client System Tray Icon

System Tray Icon	Status
	The client policy is deactivated.
	The client policy is deactivated but not connected.
	The client policy is activated and connected. A flashing vertical bar indicates traffic on the tunnel.

Viewing the UTM IPsec VPN Connection Status

To review the status of current IPsec VPN tunnels:

1. Select **Monitoring** > **Active Users & VPNs** from the main menu. The Active Users & VPN submenu tabs appear, with the Active Users screen in views
2. Click the **IPSec VPN Connection Status** submenu tab. The IPSec VPN Connection Status screen displays. (Figure 7-18 shows an IPSec SA as an example.)

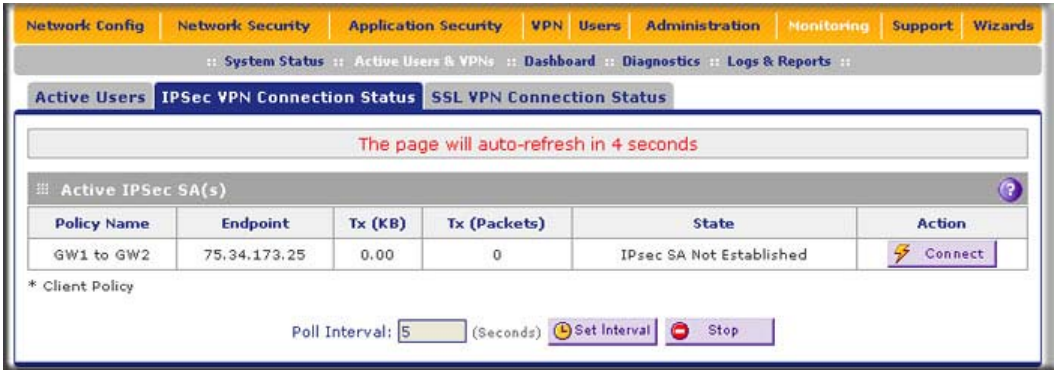


Figure 7-18

The Active IPsec SAs table lists each active connection with the information that is described in Table 7-8. 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 7-8. IPsec VPN Connection Status Information

Item	Description (or Subfield and 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 statu 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.

Viewing the UTM IPsec VPN Log

To query the IPsec VPN log:

1. Select **Monitoring** > **Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Logs Query** submenu tab. The Logs Query screen displays.
3. From the Log Type pull-down menu, select **IPSEC VPN**. The IPsec VPN logs display (see Figure 7-19 on page 7-22).

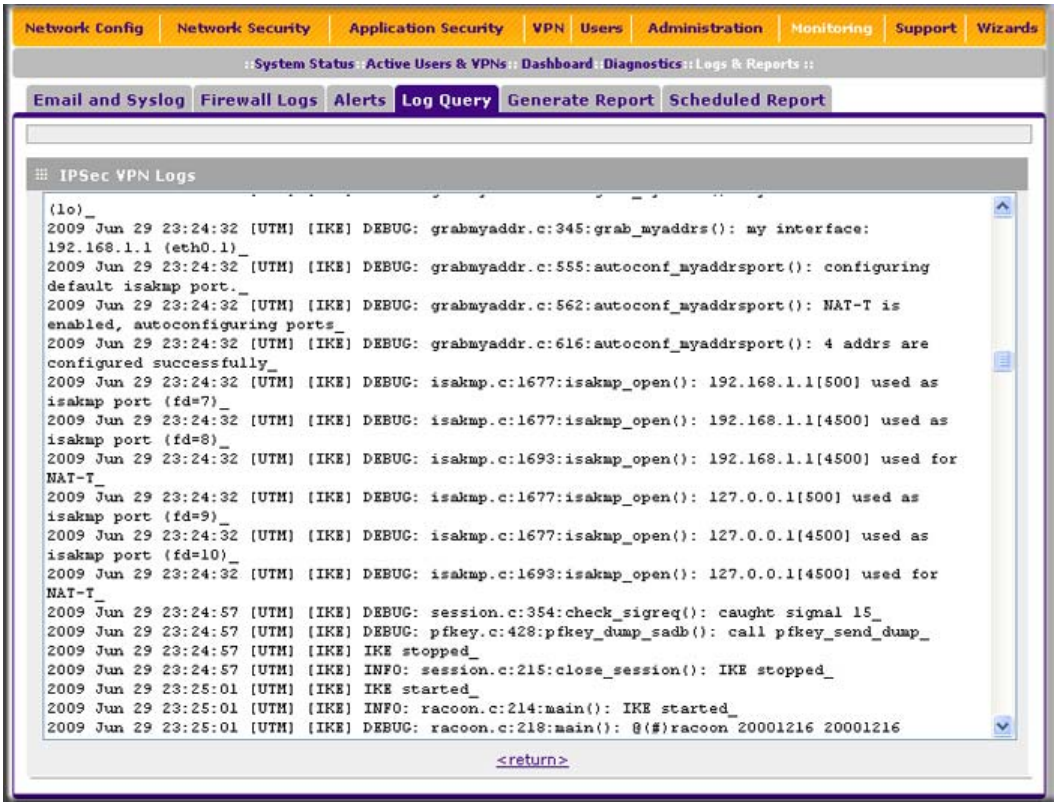


Figure 7-19

Managing 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.

Managing 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”) must use the IKE negotiation protocol.
- A manually generated VPN policies (“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 7-23 on page 7-34) 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 7-23 on page 7-34) 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.

The IKE Policies Screen

To access the IKE Policies screen:

Select **VPN** > **IPSec VPN** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view (Figure 7-20 on page 7-24 shows some examples).

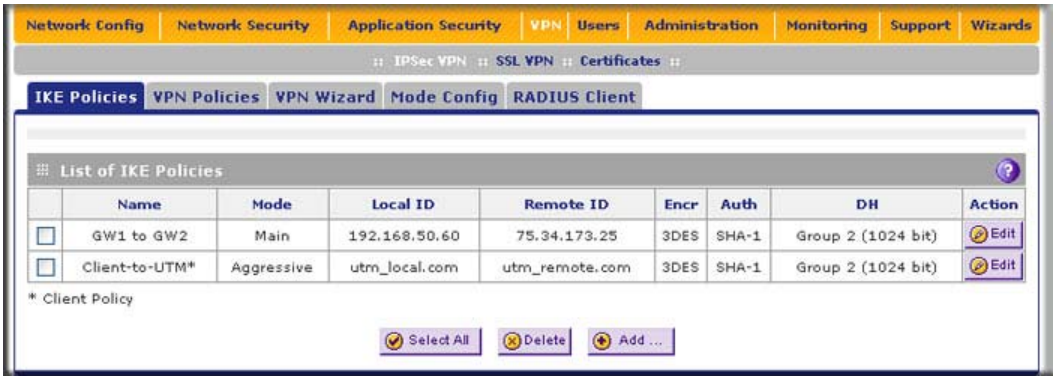


Figure 7-20

Each policy contains the data that are explained in Table 7-9 These fields are explained in more detail in Table 7-10 on page 7-27.

Table 7-9. List of IKE Policies Information

Item	Description (or Subfield and 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 must have this value as its remote ID.
Remote ID	The IKE/ISAKMP identifier of the remote endpoint, which must have this value as its Local ID.
Encr	The encryption algorithm that is used for the IKE security association (SA). This setting must match the setting on the remote endpoint.
Auth	The authentication algorithm that is used for the IKE SA. This setting must match the setting on the remote endpoint.
DH	The Diffie-Hellman (DH) group that is used when exchanging keys. This setting must match the setting on the remote endpoint.

To delete one or more IKE polices:

1. Select the checkbox to the left of the policy that you want to delete or click the **Select All** table button to select all IKE policies.
2. Click the **Delete** table button.

To add or edit an IKE policy, see “Manually Adding or Editing an IKE Policy on this page.

	Note: You cannot delete or edit an IKE policy for which the VPN policy is active. You first must disable or delete the VPN policy before you can delete or edit the IKE policy.

	Note: To gain a more complete understanding of the encryption, authentication and DH algorithm technologies, see the link to “Virtual Private Networking Basics” in Appendix E.

Manually Adding or Editing an IKE Policy

To manually add an IKE policy:

1. Select **VPN** > **IPSec VPN** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view (see Figure 7-20 on page 7-24).
2. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays (see Figure 7-21 on page 7-26, which shows a dual-WAN port model screen). The WAN1 and WAN2 radio buttons (next to Select Local Gateway) are shown on the Add IKE Policy screen for the dual-WAN port models but not on the Add IKE Policy screen for the single-WAN port models.

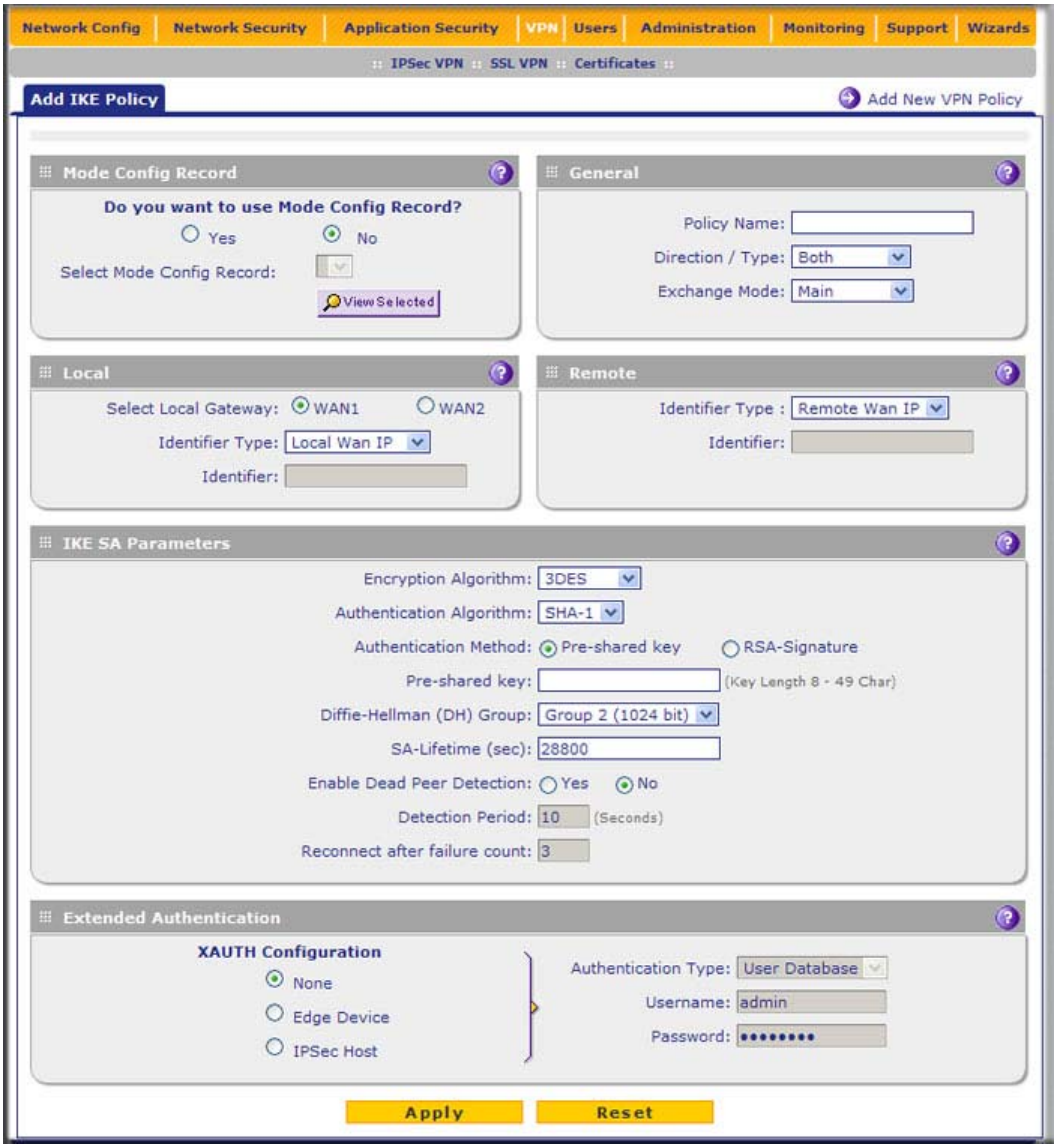

Network Config
Network Security
Application Security
VPN
Users
Administration
Monitoring
Support
Wizards
IPSec VPN
SSL VPN
Certificates
Add IKE Policy
Add New VPN Policy
Mode Config Record
Do you want to use Mode Config Record?
Yes
No
Select Mode Config Record:
View Selected
General
Policy Name:
Direction / Type:
Both
Exchange Mode:
Main
Local
Select Local Gateway:
WAN1
WAN2
Identifier Type:
Local Wan IP
Identifier:
Remote
Identifier Type :
Remote Wan IP
Identifier:
IKE SA Parameters
Encryption Algorithm:
3DES
Authentication Algorithm:
SHA-1
Authentication Method:
Pre-shared key
RSA-Signature
Pre-shared key:
(Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group:
Group 2 (1024 bit)
SA-Lifetime (sec):
28800
Enable Dead Peer Detection:
Yes
No
Detection Period:
10
(Seconds)
Reconnect after failure count:
3
Extended Authentication
XAUTH Configuration
None
Edge Device
IPSec Host
Authentication Type:
User Database
Username:
admin
Password:
Apply
Reset

Figure 7-21

3. Complete the fields, select the radio buttons, and make your selections from the pull-down menus as explained Table 7-10.

Table 7-10. Add IKE Policy Settings

Item	Description (or Subfield and 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 7-43. Select one of the following radio buttons: • **Yes**. IP addresses are assigned to remote VPN clients. You must select a Mode Config record from the pull-down menu. **Note**: 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 ends are defined by their FQDNs. • **No**. Disables Mode Config for this IKE policy. **Note**: An XAUTH configuration via an edge device is not possible without Mode Config and is therefore disabled too. For more information about XAUTH, see "Configuring Extended Authentication (XAUTH)" on page 7-38.	
	Select Mode Config Record	From the pull-down menu, select one of the Mode Config records that you defined on the Add Mode Config Record screen (see "Configuring Mode Config Operation on the UTM" on page 7-43). **Note**: Click the **View Selected** button to open the Selected Mode Config Record Details popup window,
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 pull-down menu, 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 pull-down menu, select the exchange more 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 a FQDN or a User FQDN name as the local ID and/or remote ID (see the sections below), the aggressive mode is automatically selected.	

Table 7-10. Add IKE Policy Settings (continued)

Item	Description (or Subfield and Description)	
Local		
Select Local Gateway (dual-WAN port models only)	For the dual-WAN port models only, select a radio button to specify the WAN1 or WAN2 interface.	
Identifier Type	From the pull-down menu, select one of the following ISAKMP identifiers to be used by the UTM, and then specify the identifier in the field below: • **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 e-mail 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 pull-down menu, enter the IP address, e-mail address, FQDN, or distinguished name.
Remote		
Identifier Type	From the pull-down menu, select one of the following ISAKMP identifiers to be used by the remote endpoint, and then specify the identifier in the field below: • **Local 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 e-mail 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 pull-down menu, enter the IP address, e-mail address, FQDN, or distinguished name.
IKE SA Parameters		
Encryption Algorithm	From the pull-down menu, 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-bits key size. • **AES-192**. AES with a 192-bits key size. • **AES-256**. AES with a 256-bits key size.	

Table 7-10. Add IKE Policy Settings (continued)

Item	Description (or Subfield and Description)	
Authentication Algorithm	From the pull-down menu, select one of the following two 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.	
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 Certificate that you uploaded on the Certificates screen (see "Managing Self Certificates" on page 9-20). The Pre-shared key is masked out when you select the RSA-Signature option.	
	Pre-shared key	A key with a minimum length of 8 characters 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 pull-down menu, select one of the following three strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**. **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 must occur. The default is 28800 seconds (8 hours).	
Enable Dead Peer Detection **Note**: See also "Configuring Keepalives and Dead Peer Detection" on page 7-55.	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 must enter the detection period and the maximum number of times that the UTM attempts to reconnect (see below). • **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 times that the UTM attempts to reconnect after a DPD situation. When the maximum number of times is exceeded, the IPsec connection is terminated.

Table 7-10. Add IKE Policy Settings (continued)

Item	Description (or Subfield and Description)	
Extended Authentication		
XAUTH Configuration **Note**: For more information about XAUTH and its authentication modes, see "Configuring XAUTH for VPN Clients" on page 7-39.	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 mode that is available for this configuration is 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 pull-down menu, select one of the following authentication types: • **User Database**. XAUTH occurs through the UTM's user database. Users must be added through the Add User screen (see "User Database Configuration" on page 7-40). • **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 7-40. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see "RADIUS Client Configuration" on page 7-40.
	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** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view (see Figure 7-20 on page 7-24).
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 field as the Add IKE Policy screen (see Figure 7-21 on page 7-26).
3. Modify the settings that you wish to change (see Table 7-10).

4. Click **Apply** to save your changes. The modified IKE policy is displayed in the List of IKE Policies table.

Managing 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 by using 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 must manually enter all settings on the remote VPN endpoint (unless the remote VPN endpoint also has a VPN Wizard).

In addition, a Certificate Authority (CA) can also be used to perform authentication (see "Managing Digital Certificates" on page 9-17). To use a CA, each VPN gateway must 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.

The 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. The rules for VPN policy use are:

1. Traffic covered by a policy is automatically sent via a VPN tunnel.
2. 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.)
3. The VPN tunnel is created according to the settings in the security association (SA).
4. The remote VPN endpoint must have a matching SA, otherwise it refuses the connection.

To access the VPN Policies screen:

1. Select **VPN** > **IPSec VPN** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view.

2. Click the **VPN Policies** submenu tab. The VPN Policies screen displays. (Figure 7-22 shows some examples.)

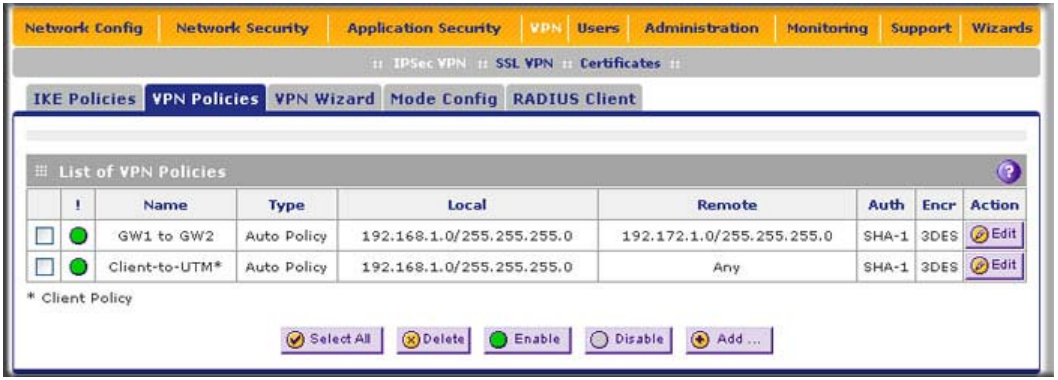


Figure 7-22

Each policy contains the data that are explained in Table 7-11. These fields are explained in more detail in Table 7-12 on page 7-35.

Table 7-11. List of VPN Policies Information

Item	Description (or Subfield and Description)
! (Status)	Indicates whether the policy is enabled (green circle) or disabled (grey circle). To enable or disable a policy, select the checkbox adjacent to the circle and click the **Enable** or **Disable** table button, as required.
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 local LAN. Traffic must be from (or to) these addresses to be covered by this policy. (The subnet address is supplied as the default IP address when using the VPN Wizard).
Remote	IP address or address range of the remote network. Traffic must 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 must match the setting on the remote endpoint.
Encr	The encryption algorithm that is used for the VPN tunnel. This setting must match the setting on the remote endpoint.

To delete one or more VPN polices:

1. Select the checkbox to the left of the 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 ore more VPN policies:

1. Select the checkbox to the left of the policy that you want to delete or click the **Select All** table button to select all IKE Policies.
2. Click the **Enable** or **Disable** table button.

To add or edit a VPN policy, see "Manually Adding or Editing a VPN Policy" on this page.

Note: You cannot delete or edit an IKE policy for which the VPN policy is active. You first must disable or delete the VPN policy before you can delete or edit the IKE policy.

Manually Adding or Editing a VPN Policy

To manually add a VPN policy:

1. Select **VPN** > **IPSec VPN** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view (see Figure 7-20 on page 7-24).
2. Click the **VPN Policies** submenu tab. The VPN Policies screen displays (see Figure 7-22 on page 7-32).
3. Under the List of VPN Policies table, click the **Add** table button. The Add VPN Policy screen displays (see Figure 7-23 on page 7-34, which shows a dual-WAN port model screen). The WAN1 and WAN2 radio buttons (next to Select Local Gateway) are shown on the Add VPN Policy screen for the dual-WAN port models but not on the Add VPN Policy screen for the single-WAN port models.

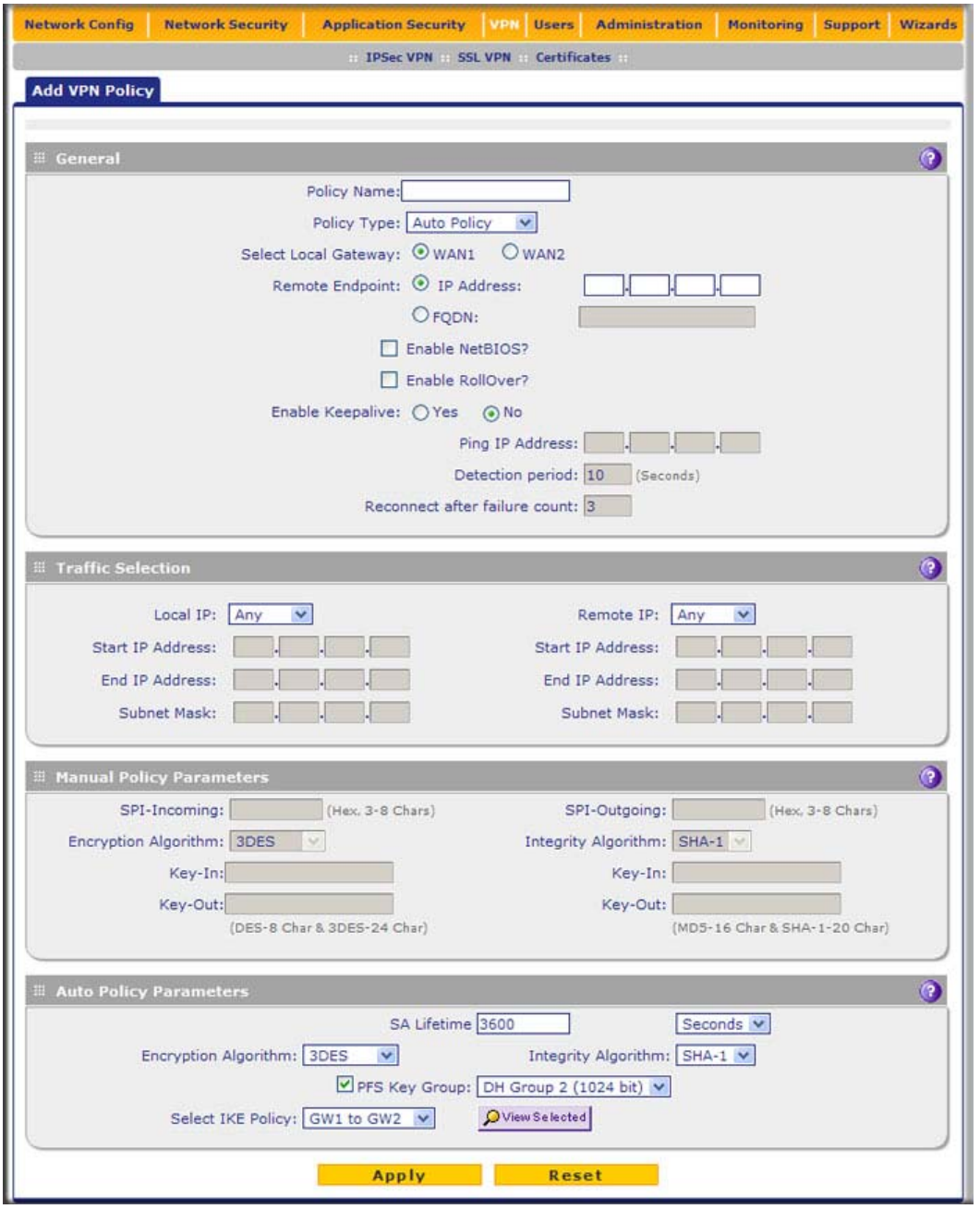

Network Config
Network Security
Application Security
VPN
Users
Administration
Monitoring
Support
Wizards
IPSec VPN
SSL VPN
Certificates
Add VPN Policy
General
Policy Name:
Policy Type: Auto Policy
Select Local Gateway: WAN1 WAN2
Remote Endpoint: IP Address:
FQDN:
Enable NetBIOS?
Enable RollOver?
Enable Keepalive: Yes No
Ping IP Address:
Detection period: 10 (Seconds)
Reconnect after failure count: 3
Traffic Selection
Local IP: Any
Start IP Address:
End IP Address:
Subnet Mask:
Remote IP: Any
Start IP Address:
End IP Address:
Subnet Mask:
Manual Policy Parameters
SPI-Incoming: (Hex. 3-8 Chars)
Encryption Algorithm: 3DES
Key-In:
Key-Out:
(DES-8 Char & 3DES-24 Char)
SPI-Outgoing: (Hex. 3-8 Chars)
Integrity Algorithm: SHA-1
Key-In:
Key-Out:
(MD5-16 Char & SHA-1-20 Char)
Auto Policy Parameters
SA Lifetime 3600 Seconds
Encryption Algorithm: 3DES
Integrity Algorithm: SHA-1
PFS Key Group: DH Group 2 (1024 bit)
Select IKE Policy: GW1 to GW2
View Selected
Apply
Reset

Figure 7-23

4. Complete the fields, select the radio buttons and checkboxes, and make your selections from the pull-down menus as explained Table 7-12.

Table 7-12. Add VPN Policy Settings

Item	Description (or Subfield and 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 pull-down menu, 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 must be specified, including the ones in the Manual Policy Parameters section of the screen.	
Select Local Gateway (dual-WAN port models only)	For the dual-WAN port models only, select a radio button to specify the WAN1 or WAN2 interface.	
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 checkbox to allow NetBIOS broadcasts to travel over the VPN tunnel. For more information about NetBIOS, see "Configuring NetBIOS Bridging with IPsec VPN" on page 7-59. This feature is disabled by default.	
Enable RollOver?	Select this checkbox 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.	
Enable Keepalive **Note**: See also "Configuring Keepalives and Dead Peer Detection" on page 7-55.	Select a radio button to specify if Keepalive is enabled: • **Yes**. This feature is enabled: periodically, the UTM sends ping packets to the remote endpoint to keep the tunnel alive. You must enter the ping IP address, detection period, and the maximum number of times that the UTM attempts to reconnect (see below). • **No**. This feature is disabled. This is the default setting.	
	Ping IP Address	The IP address that the UTM pings. The address must be of a host that can respond to ICMP ping requests.
	Detection period	The period in seconds between the ping packets. The default setting is 10 seconds.
	Reconnect after failure count	The number of consecutive missed responses that are considered a tunnel connection failure. The default setting is 3 missed responses.

Table 7-12. Add VPN Policy Settings (continued)

Item	Description (or Subfield and Description)
Traffic Selection	
Local IP	From the pull-down menu, select the address or addresses that are part of the VPN tunnel on the UTM: • **Any**. All PCs and devices on the network. **Note**: You cannot select Any for both the UTM and the remote endpoint. • **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.
Remote IP	From the pull-down menu, select the address or addresses that are part of the VPN tunnel on the remote endpoint. The menu choices are the same as for the Local IP pull-down menu (see above).
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).
Encryption Algorithm	From the pull-down menu, 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-bits key size. • **AES-192**. AES with a 192-bits key size. • **AES-256**. AES with a 256-bits key size.
Key-In	The encryption key for he 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 he outbound policy. The length of the key depends on the selected encryption algorithm. The required key lengths are the same as for the Key-In (se above).
SPI-Outgoing	The Security Parameters Index (SPI) for the outbound policy. Enter a hexadecimal value between 3 and 8 characters (for example: 0x1234).

Table 7-12. Add VPN Policy Settings (continued)

Item	Description (or Subfield and Description)
Integrity Algorithm	From the pull-down menu, 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.
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.
Key-Out	The integrity key for he outbound policy. The length of the key depends on the selected integrity algorithm. The required key lengths are the same as for the Key-In (se above).
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 must be renegotiated. From the pull-down menu, 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 pull-down menu, 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-bits key size. • **AES-192**. AES with a 192-bits key size. • **AES-256**. AES with a 256-bits key size.
Integrity Algorithm	From the pull-down menu, 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.

Table 7-12. Add VPN Policy Settings (continued)

Item	Description (or Subfield and Description)
PFS Key Group	Select this checkbox to enable Perfect Forward Secrecy (PFS), and then select a Diffie-Hellman (DH) group from the pull-down menu. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the pull-down menu, select one of the following three strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**.
Select IKE Policy	Select an existing IKE policy that defines the characteristics of the Phase-1 negotiation. Click the **view selected** button to display the selected IKE policy.

5. 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** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view.
2. Click the **VPN Policies** submenu tab. The VPN Policies screen displays (see Figure 7-22 on page 7-32).
3. 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 field as the Add VPN Policy screen (see Figure 7-23 on page 7-34).
4. Modify the settings that you wish to change (see Table 7-12).
5. Click **Apply** to save your changes. The modified VPN policy is displayed in the List of VPN Policies table.

Configuring 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, and 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 must specify the authentication type that must be used during verification of the credentials of the remote VPN gateways: 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 must 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.

Configuring XAUTH for VPN Clients

Once the XAUTH has been enabled, you must establish user accounts on the User Database to be authenticated against XAUTH, or you must 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 must be disabled before you can modify the IKE policy.

To enable and configure XAUTH:

1. Select **VPN** > **IPSec VPN** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view (see Figure 7-20 on page 7-24).
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 field as the Add IKE Policy screen (see Figure 7-21 on page 7-26).
3. Locate the Extended Authentication section on the screen.

4. Complete the fields, select the radio buttons, and make your selections from the pull-down menus as explained Table 7-13.

Table 7-13. Extended Authentication Settings

Item	Description (or Subfield and 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 mode that is available for this configuration is 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 pull-down menu, select one of the following authentication types: • **User Database**. XAUTH occurs through the UTM's user database. Users must be added through the Add User screen (see "User Database Configuration" on page 7-40). • **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 7-40. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see "RADIUS Client Configuration" on page 7-40.
Username	The user name for XAUTH.
Password	The password for XAUTH.

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

User Database Configuration

When XAUTH is enabled in an Edge Device configuration, users must 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 must be added to the List of Users table on the Users screen, as described in "Configuring User Accounts" on page 9-9.

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 must provide authentication information such as a user name and password or some encrypted response using his 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** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view.
2. Click the **RADIUS Client** submenu tab. The RADIUS Client screen displays.

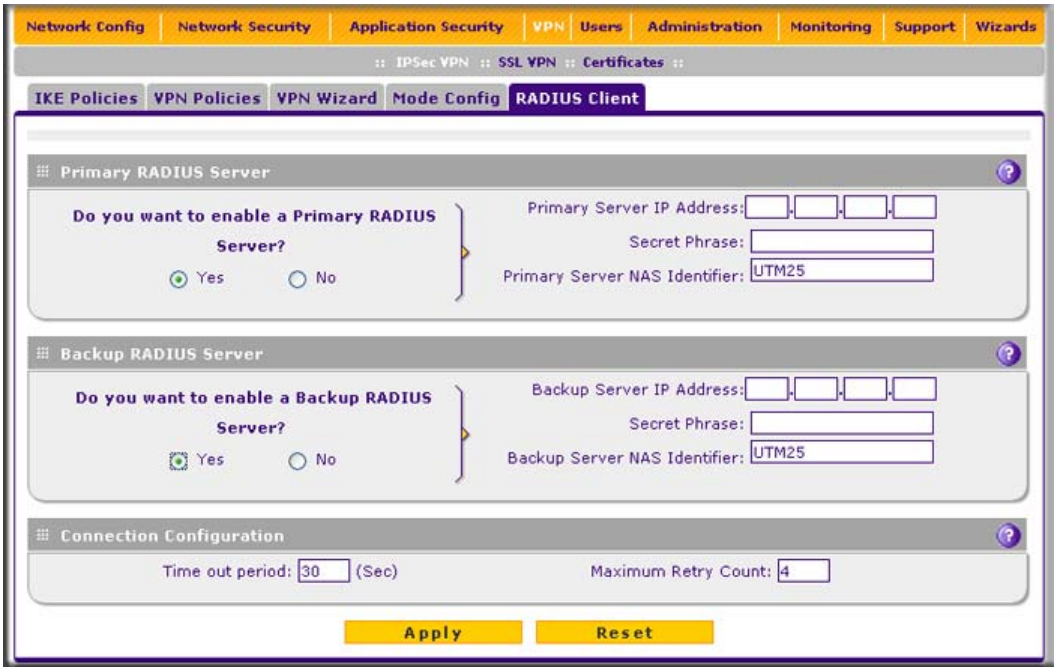


Figure 7-24

3. Complete the fields and select the radio buttons as explained Table 7-14.

Table 7-14. RADIUS Client Settings

Item	Description (or Subfield and Description)
Primary RADIUS Server	
Select the **Yes** radio button to enable and configure the primary RADIUS server, and then enter the settings for the three fields below. The default setting is that the No radio button is selected.	
Primary Server IP Address	The IP address of the primary RADIUS server.
Secret Phrase	The a shared secret phrase to authenticate the transactions between the client and the primary RADIUS server. The same Secret Phrase must be configured on both the client and the server.
Primary Server NAS Identifier	The primary Network Access Server (NAS) identifier that must be present in a RADIUS request. **Note**: The UTM functions as a NAS, allowing network access to external users after verification of their authentication information. In a RADIUS transaction, the NAS must 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 must enter in this field.
Backup RADIUS Server	
Select the **Yes** radio button to enable and configure the backup RADIUS server, and then enter the settings for the three fields below. 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	The a shared secret phrase to authenticate the transactions between the client and the backup RADIUS server. The same Secret Phrase must be configured on both the client and the server.
Backup Server NAS Identifier	The backup Network Access Server (NAS) identifier that must be present in a RADIUS request. **Note**: See the Note above 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.

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

Note: You select the RADIUS authentication protocol (PAP or CHAP) on the Edit IKE Policy screen or Add IKE Policy screen (see "Configuring XAUTH for VPN Clients" on page 7-39).

Assigning 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 assign IP addresses to remote users, including a network access IP address, subnet mask, WINS server, and DNS address from the UTM. 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 7-26 on page 7-45).

Note: After configuring a Mode Config record, you must manually configure an IKE policy and select the newly-created Mode Config record from the 'Select Mode Config Record' pull-down menu (see "Configuring Mode Config Operation on the UTM" on page 7-43. 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 liftetime for the connection has timed out.

Configuring Mode Config Operation on the UTM

To configure Mode Config on the UTM, you first must create a Mode Config record, and then select the Mode Config record for an IKE policy:

1. Select **VPN** > **IPSec VPN** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view.

2. Click the **Mode Config** submenu tab. The Mode Config screen displays.

Figure 7-25

As an example, the screen shows two Mode Config records with the names EMEA Sales and NA Sales:

- For EMEA Sales, a first pool (172.169.100.1 through 172.169.100.99) and second pool (182.183.200.1 through 172.183.200.99) are shown.
- For NA Sales, a first pool (172.173.100.50 through 172.173.100.90), a second pool (182.185.210.1 through 182.185.210.99), and a third pool (172.210.220.80 through 172.210.220.99) are shown.

3. Under the List of Mode Config Records table, click the **Add** table button. The Add Mode Config Record screen displays (see Figure 7-26 on page 7-45).

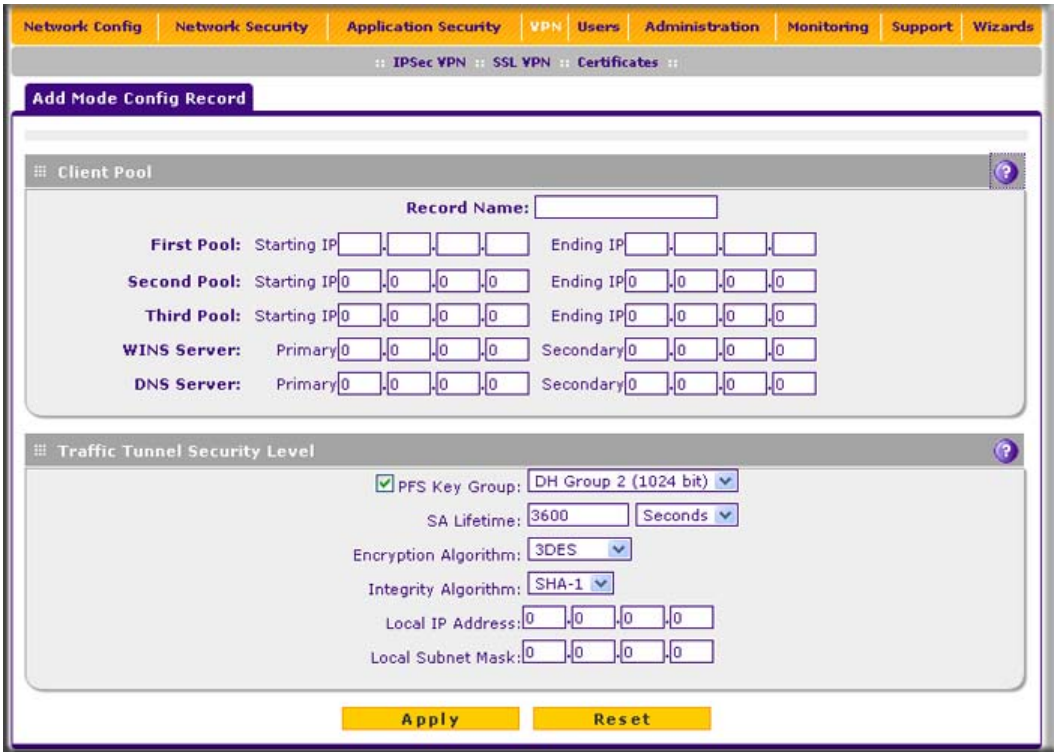


Figure 7-26

4. Complete the fields, select the checkbox, and make your selections from the pull-down menus as explained Table 7-15.

Table 7-15. Add Mode Config Record Settings

Item	Description (or Subfield and Description)
Client Pool	
Record Name	A descriptive name of the Mode Config record for identification and management purposes.
First Pool Second Pool Third 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 options. 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. **Note**: Any IP pool should not be within the local network IP addresses. Use a different range of private IP addresses such as 172.173.xxx.xx.

Table 7-15. Add Mode Config Record Settings (continued)

Item	Description (or Subfield and 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 setting work well for a Mode Config configuration.	
PFS Key Group	Select this checkbox to enable Perfect Forward Secrecy (PFS), and then select a Diffie-Hellman (DH) group from the pull-down menu. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the pull-down menu, 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 must be renegotiated. From the pull-down menu, 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 pull-down menu, 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-bits key size. • **AES-192**. AES with a 192-bits key size. • **AES-256**. AES with a 256-bits key size.
Integrity Algorithm	From the pull-down menu, 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. Typically, this is the UTM's LAN subnet, such as 192.168.1.0. **Note**: If you do not specify a local IP address, the UTM's default LAN subnet is used.
Local Subnet Mask	The local subnet mask. Typically, this is 255.255.255.0.

5. 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.

6. Select **VPN** > **IPSec VPN** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view (see Figure 7-20 on page 7-24).

7. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays. (Figure 7-27 shows the upper part only of a dual-WAN port model screen.) The WAN1 and WAN2 radio buttons (next to Select Local Gateway) are shown on the Add IKE Policy screen for the dual-WAN port models but not on the Add IKE Policy screen for the single-WAN port models.

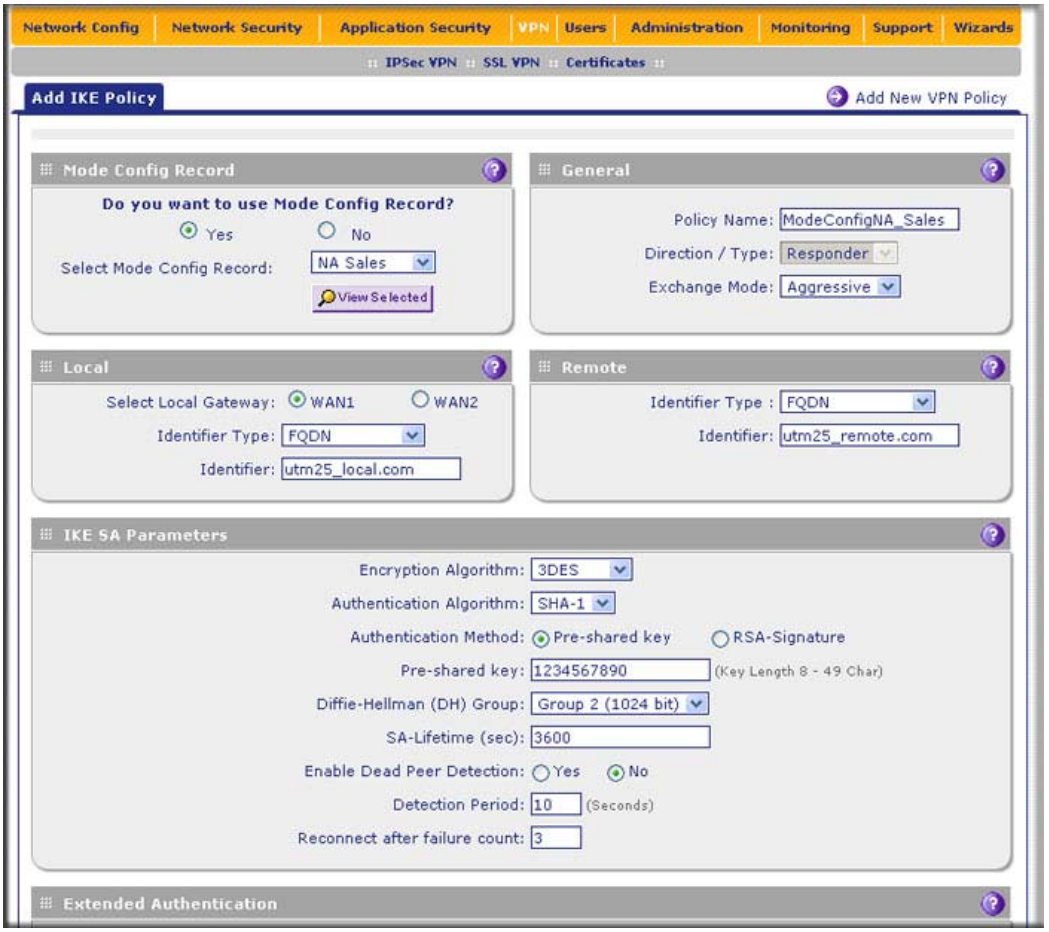


Figure 7-27

8. On the Add IKE Policy screen, complete the fields, select the radio buttons, and make your selections from the pull-down menus as explained Table 7-16.

Note: The settings that are explained in Table 7-16 are specifically for a Mode Config configuration. Table 7-10 on page 7-27 explains the general IKE policy settings.

Table 7-16. Add IKE Policy Settings for a Mode Config Configuration

Item	Description (or Subfield and 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 and disables the Main mode. Mode Config also requires that both the local and remote ends are defined by their FQDNs.	
	Select Mode Config Record	From the pull-down menu, select the Mode Config record that you created in step 5 above. In this example, we are using NA Sales.
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	Responder is automatically selected when you select the Mode Config record (see above). 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 (see above).	
Local		
Select Local Gateway (dual-WAN port models only)	For the dual-WAN port models only, select a radio button to specify the WAN1 or WAN2 interface.	
Identifier Type	From the pull-down menu, select **FQDN**. **Note**: Mode Config requires that the UTM (that is, the local end) is defined by a FQDN.	
	Identifier	Enter a FQDN for the UTM. In this example, we are using utm25_local.com.

Table 7-16. Add IKE Policy Settings for a Mode Config Configuration (continued)

Item	Description (or Subfield and Description)	
Remote		
Identifier Type	From the pull-down menu, select **FQDN**. **Note**: Mode Config requires that the remote end is defined by a FQDN.	
	Identifier	Enter the FQDN for the remote end. This must be a FQDN that is not used in any other IKE policy. In this example, we are using utm25_remote.com.
IKE SA Parameters **Note**: Generally, the default settings work well for a Mode Config configuration.		
Encryption Algorithm	From the pull-down menu, select the **3DES** algorithm to negotiate the security association (SA).	
Authentication Algorithm	From the pull-down menu, 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 field below.	
	Pre-shared key	A key with a minimum length of 8 characters no more than 49 characters. Do not use a double quote (“) in the key. In this example, we are using 12345678910.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. From the pull-down menu, 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 must occur. The default is 28800 seconds (8 hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (1 hour).	
Enable Dead Peer Detection **Note**: See also “Configuring Keepalives and Dead Peer Detection” on page 7-55.	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 must enter the detection period and the maximum number of times that the UTM attempts to reconnect (see below). • **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.
	Reconnect after failure count	The maximum number of times that the UTM attempts to reconnect after a DPD situation. When the maximum number of times is exceeded, the IPsec connection is terminated. The default setting is 3 IKE connection failures.

Table 7-16. Add IKE Policy Settings for a Mode Config Configuration (continued)

Item	Description (or Subfield and Description)	
Extended Authentication		
XAUTH Configuration **Note**: For more information about XAUTH and its authentication modes, see "Configuring XAUTH for VPN Clients" on page 7-39.	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 mode that is available for this configuration is 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 pull-down menu, select one of the following authentication types: • **User Database**. XAUTH occurs through the UTM's user database. Users must be added through the Add User screen (see "User Database Configuration" on page 7-40). • **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 7-40. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see "RADIUS Client Configuration" on page 7-40.
	Username	The user name for XAUTH.
	Password	The password for XAUTH.

9. Click **Apply** to save your settings. The IKE policy is added to the List of IKE Policies table.

Configuring the ProSafe VPN Client for Mode Config Operation

From a client PC running NETGEAR ProSafe VPN Client software, configure the remote VPN client connection for Mode Config operation:

1. Right-click on the VPN client icon in your Windows toolbar, select **Security Policy Editor**. Then, select **Options** > **Secure**, and verify that the Specified Connections selection is enabled (see Figure 7-11 on page 7-13).

2. In the upper left of the Policy Editor window, click the **New Connection** icon (the first icon on the left) to open a new connection. Give the new connection a name; in this example, we are using ModeConfigTest.

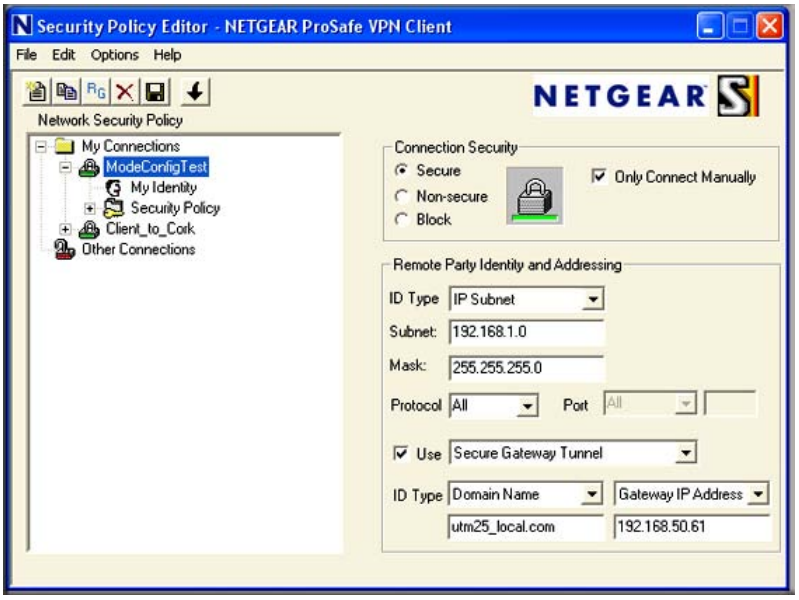


Figure 7-28

3. Enter the settings as explained in Table 7-17.

Table 7-17. Security Policy Editor: Remote Party, Mode Config Settings

Setting	Description (or Subfield and Description)
Connection Security	Select the **Secure** radio button. If you want to connect manually only, select the **Only Connect Manually** checkbox.
ID Type	From the pull-down menu, select **IP Subnet**.
Subnet	Enter the LAN IP subnet address that you specified on the Add Mode Config Record in the Local IP Address field. If you left the Local IP Address field blank, enter the UTM's default IP subnet address. In this example, we are using 192.168.1.0.
Mask	Enter the LAN IP subnet mask that you specified on the Add Mode Config Record in the Local Subnet Mask field. If you left the Local Subnet Mask field blank, enter the UTM's default IP subnet mask. In this example, we are using 255.255.255.0.
Protocol	From the pull-down menu, select **All**.

Table 7-17. Security Policy Editor: Remote Party, Mode Config Settings (continued)

Setting	Description (or Subfield and Description)	
Use	Select the **Use** checkbox. Then, from the pull-down menu, select **Secure Gateway Tunnel**.	
ID Type	Left pull-down menu	From the left pull-down menu, select **Domain Name**. Then, below, enter the local FQDN that you specified in the UTM's Mode Config IKE policy. In this example, we are using utm25_local.com.
	Right pull-down menu	From the right pull-down menu, select **Gateway IP Address**. Then, below, enter the IP address of the WAN interface that you selected on the UTM's VPN Wizard screen (see Figure 7-9 on page 7-10). In this example, the WAN IP address is 192.168.50.61. **Note**: You can find the WAN IP address on the Connection Status screen for the selected WAN port. For more information, see "Viewing the WAN Ports Status" on page 11-27.

4. Click on the disk icon to save the configuration, or select **File** > **Save** from the Security Policy Editor menu.

5. In the left frame, click **My Identity**. The screen adjusts.

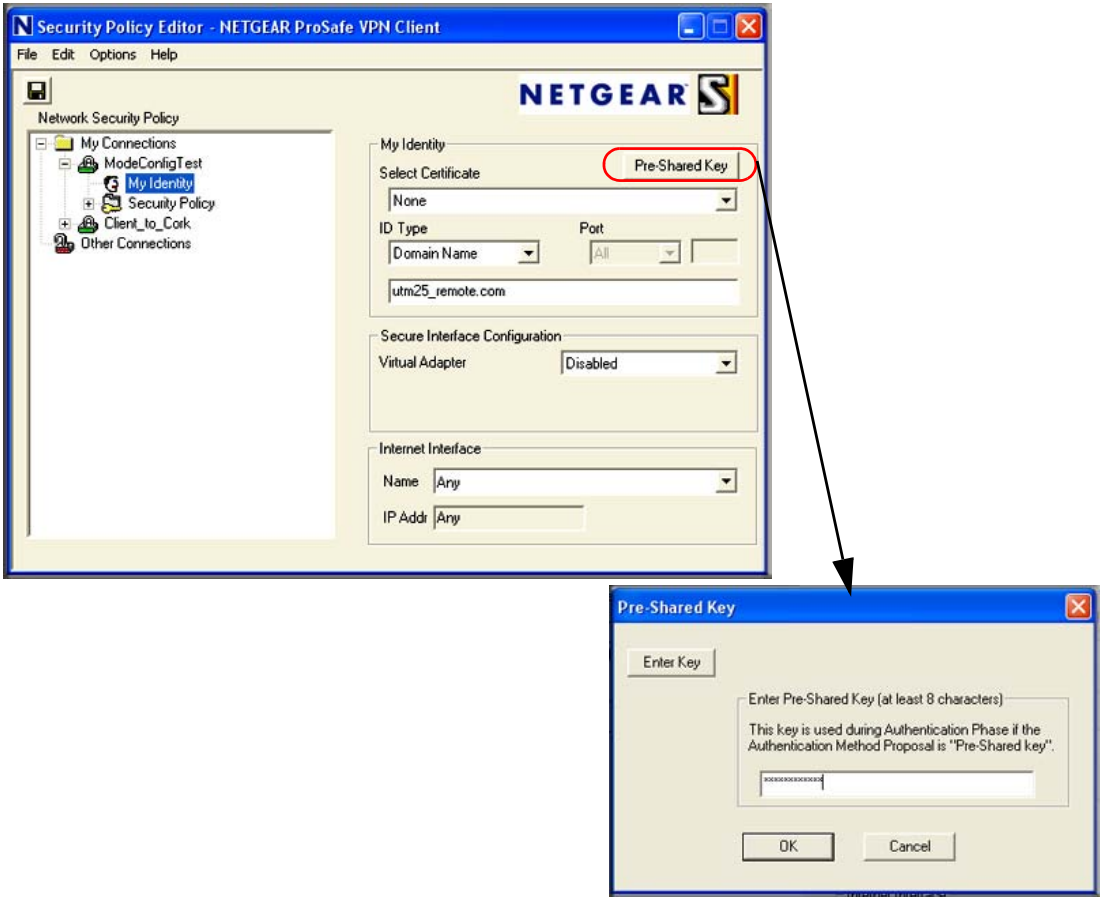


Figure 7-29

6. Enter the settings as explained in Table 7-18.

Table 7-18. Security Policy Editor: My Identity, Mode Config Settings

Setting	Description (or Subfield and Description)	
Select Certificate	From the pull-down menu, select **None**. The Pre-Shared Key window appears.	
	Pre-Shared Key	Enter the same pre-shared key that you specified on the UTM's VPN Wizard screen (see Figure 7-9 on page 7-10). In this example, the pre-shared key is 12345678910. However, the pre-shared key is masked for security.

Table 7-18. Security Policy Editor: My Identity, Mode Config Settings (continued)

Setting	Description (or Subfield and Description)
ID Type	From the pull-down menu, select **Domain Name**. Then, below, enter the remote FQDN that you specified in the UTM's Mode Config IKE policy. In this example, we are using utm25_remote.com.
Secure Interface Configuration	Select **Preferred** from the Virtual Adapter pull-down menu.
Internet Interface	Leave the default setting, which is the **Any** selection from the Name pull-down menu.

7. Click on the disk icon to save the configuration, or select **File** > **Save** from the Security Policy Editor menu.
8. In the left frame, click **Security Policy**. The screen adjusts.

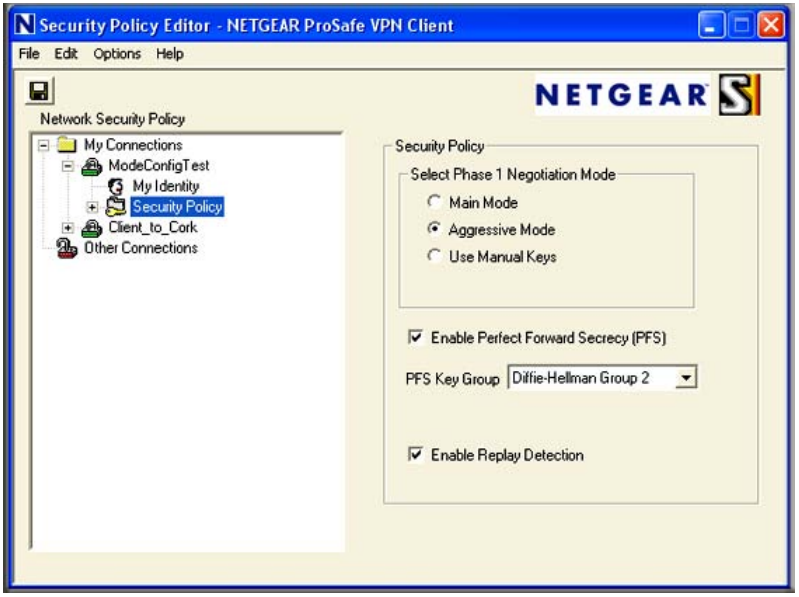


Figure 7-30

9. Enter the settings as explained in Table 7-19.

Table 7-19. Security Policy Editor: Security Policy, Mode Config Settings

Setting	Description (or Subfield and Description)
Select Phase 1 Negotiation Mode	Select the **Aggressive Mode** radio button.
Enable Perfect Forward Secrecy (PFS)	Select the **Enable Perfect Forward Secrecy (PFS)** checkbox. From the pull-down menu below, select **Diffie-Hellman Group 2**.
Enable Replay Detection	Leave the default setting, which is selection of the **Enable Replay Detection** checkbox.

10. Click on the disk icon to save the configuration, or select **File** > **Save** from the Security Policy Editor menu.
11. Close the VPN ProSafe VPN client.

Testing the Mode Config Connection

To test the connection:

1. Right-click on the VPN client icon in the Windows toolbar and click Connect. The connection policy you configured appears; in this example “My Connections\ModeConfigTest”.
2. Click on the connection. For this example, the message “Successfully connected to MyConnections/ModeConfigTest” is displayed within 30 seconds, and the VPN client icon in the toolbar displays “On”.
3. From the client PC, ping a computer on the UTM LAN.

Configuring Keepalives 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 Keepalive 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 must also support DPD. Keepalive, though less reliable than DPD, does not require any support from the peer device.

Configuring Keepalives

The Keepalive feature maintains the IPSec SA by sending periodic ping requests to a host across the tunnel and monitoring the replies. To configure the Keepalive feature on a configured VPN policy:

1. Select **VPN** > **IPSec VPN** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view.
2. Click the **VPN Policies** submenu tab. The VPN Policies screen displays (see Figure 7-22 on page 7-32).
3. 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. (Figure 7-31 shows only the top part of the screen with the General section).

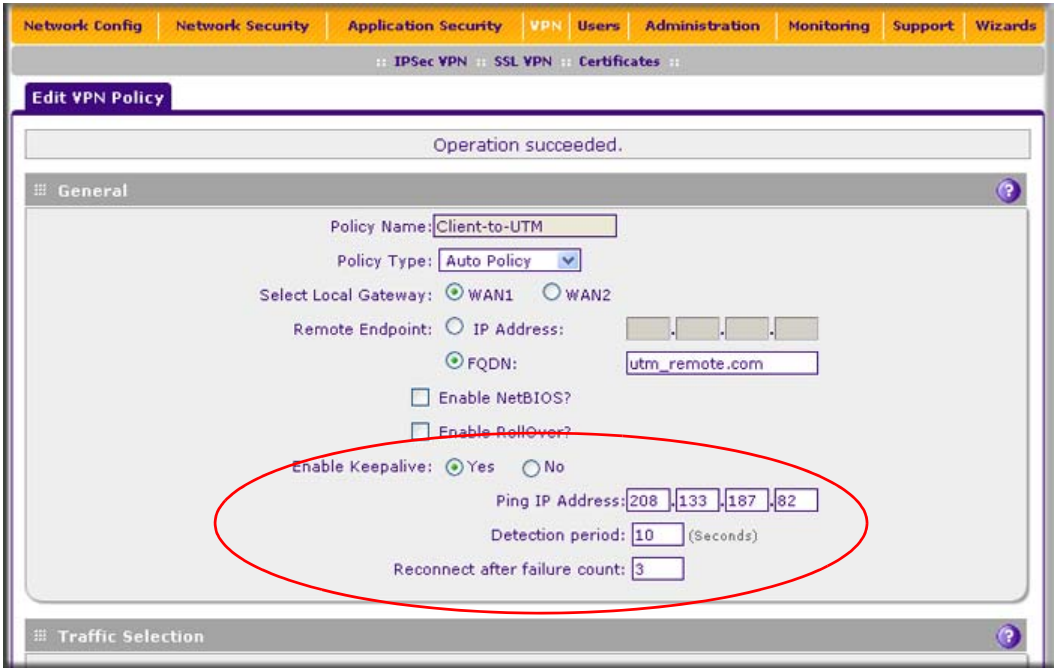


Figure 7-31

4. Enter the settings as explained in Table 7-20.

Table 7-20. Keepalive Settings

Item	Description (or Subfield and Description)	
General		
Enable Keepalive	Select the **Yes** radio button to enable the Keepalive feature. Periodically, the UTM sends ping packets to the remote endpoint to keep the tunnel alive. You must enter the ping IP address, detection period, and the maximum number of times that the UTM attempts to reconnect (see below).	
	Ping IP Address	The IP address that the UTM pings. The address must be of a host that can respond to ICMP ping requests.
	Detection period	The period in seconds between the ping packets. The default setting is 10 seconds.
	Reconnect after failure count	The number of consecutive missed responses that are considered a tunnel connection failure. The default setting is 3 missed responses.

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

Configuring Dead Peer Connection

The Dead Peer Detection (DPD) feature maintains 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** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view (see Figure 7-20 on page 7-24).
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. (Figure 7-31 on page 7-56 shows only the top part of the screen with the General section).

3. In the IKE SA Parameters section of the screen, locate the DPD fields.

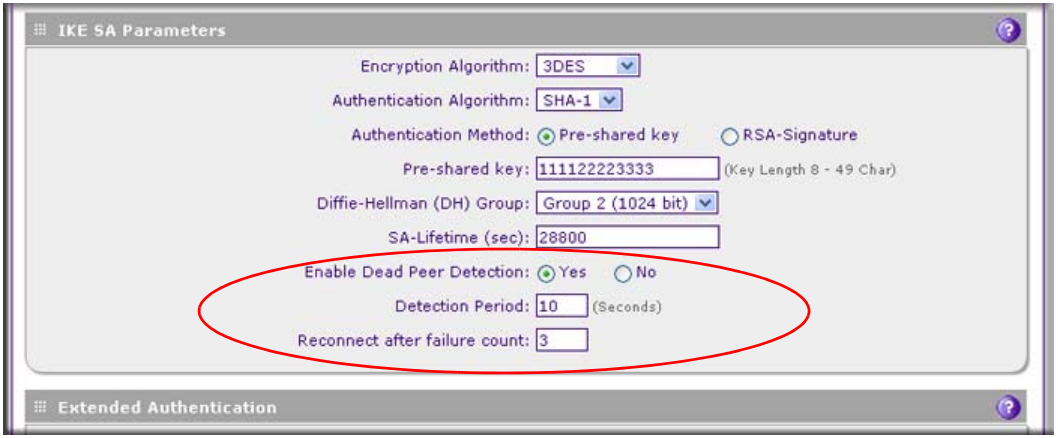


Figure 7-32

4. Select the radio button and complete the fields as explained Table 7-21.

Table 7-21. Dead Peer Detection Settings

Item	Description (or Subfield and 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 must enter the detection period and the maximum number of times that the UTM attempts to reconnect (see below).	
	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 times that the UTM attempts to reconnect after a DPD situation. When the maximum number of times is exceeded, the IPsec connection is terminated. The default setting is 3 IKE connection failures.

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

Configuring 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 normally 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** from the menu. The IPsec VPN submenu tabs appear with the IKE Policies screen in view.
2. Click the **VPN Policies** submenu tab. The VPN Policies screen displays (see Figure 7-22 on page 7-32).
3. 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. (Figure 7-31 shows only the top part of the screen with the General section).

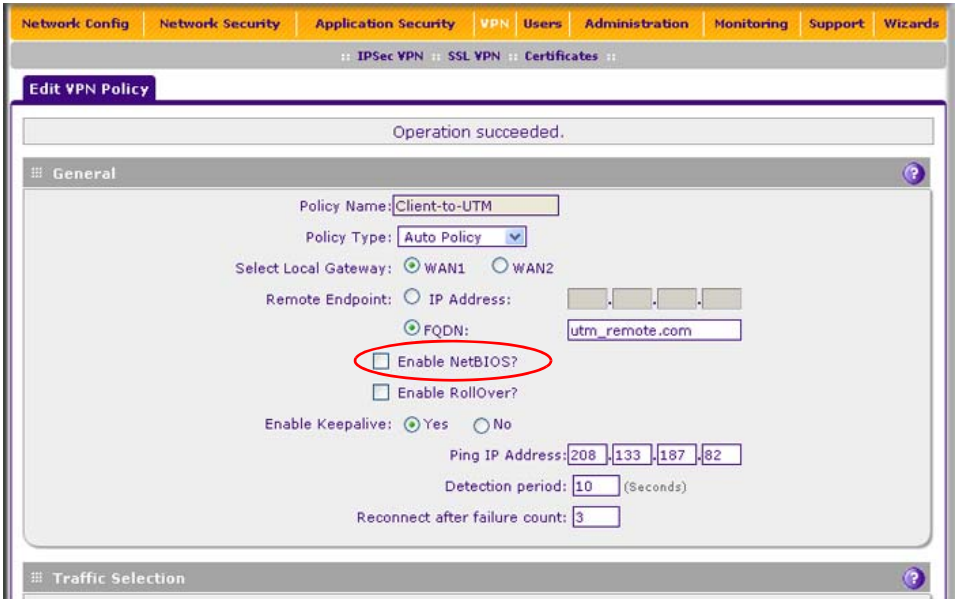


Figure 7-33

4. Select the **Enable NetBIOS** checkbox.
5. Click **Apply** to save your settings.

Chapter 8
Virtual Private Networking Using SSL Connections

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 pre-installed 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 is completed, the server and client can establish an encrypted connection. With support for up to 13 dedicated SSL VPN tunnels, users can easily access the remote network for a customizable, secure, user portal experience from virtually any available platform.

This chapter contains the following sections:

Understanding the 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 installs 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 connection 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.

Using 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. To edit policies or to manually configure policies, see "Manually Configuring and Editing SSL Connections" on page 8-17."

To start the SSL VPN Wizard:

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

Figure 8-1

2. Select the **SSLS 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 Configuring and Editing SSL Connections" on page 8-17 or in other chapters; each section below provides a specific link to a section in "Manually Configuring and Editing SSL Connections" on page 8-17 or to a section in another chapter.

SSL VPN Wizard Step 1 of 6: Portal Settings

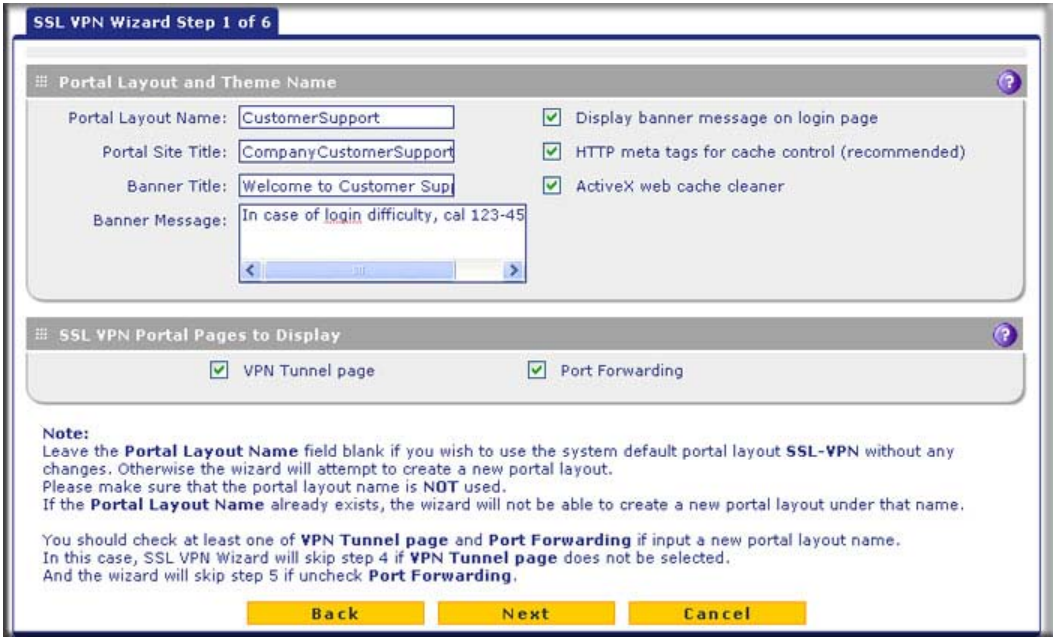


Figure 8-2

Note that Figure 8-2 contains some examples. Enter the settings as explained in Table 8-1 on page 8-4, 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 SSL-VPN. You must enter a name other than SSL VPN in the Portal Layout Name field so the SSL VPN Wizard can create a new portal layout. Do not enter an existing portal layout name in the in the Portal Layout Name field, otherwise the SSL VPN Wizard will fail (although the UTM will not reboot in this situation).

Note: 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 "Creating the Portal Layout" on page 8-18.

Table 8-1. SSL VPN Wizard Step 1: Portal Settings

Item	Description (or Subfield and 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 sub-site 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 non-alphanumeric character. **Note**: Unlike most other URLs, this name is case-sensitive.
Portal Site Title	The title that appears 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 Java script tags. The maximum length of the login page message is 4096 characters.
Display banner message on login page	Select this checkbox to show the banner title and banner message text on the login screen as shown in Figure 8-8 on page 8-15.

Table 8-1. SSL VPN Wizard Step 1: Portal Settings (continued)

Item	Description (or Subfield and Description)
HTTP meta tags for cache control (recommended)	Select this checkbox 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 checkbox 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	Select this checkbox to provide full network connectivity.
Port Forwarding	Select this checkbox to provides access to specific defined network services. **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.

SSL VPN Wizard Step 2 of 6: Domain Settings

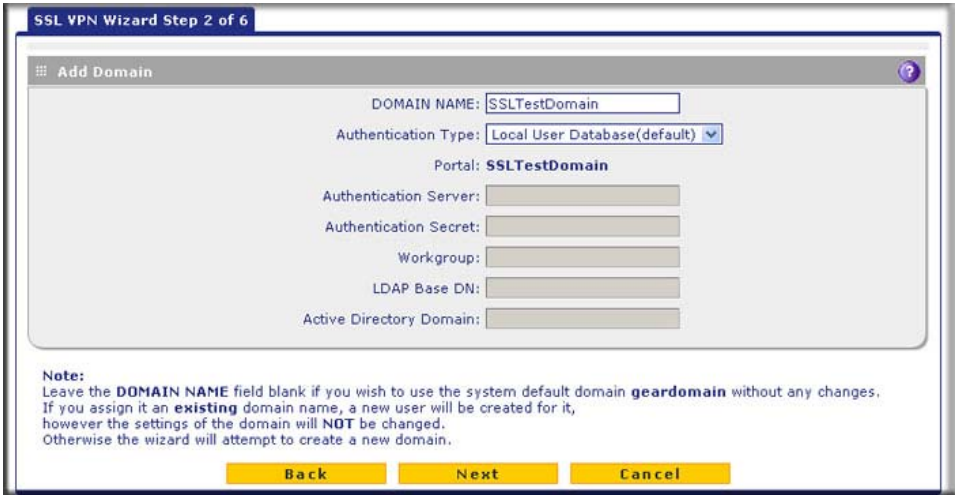


Figure 8-3

Note that Figure 8-3 contains some examples. Enter the settings as explained in Table 8-2, 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 must enter a name other than geardomain in the Domain Name field so the SSL VPN Wizard can create a new domain. Do not enter an existing domain name in the in the Domain Name field, otherwise the SSL VPN Wizard will fail and the UTM will reboot to recover its configuration.

Note: 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 "Configuring Domains" on page 9-2.

Table 8-2. SSL VPN Wizard Step 2: Domain Settings

Setting	Description (or Subfield and 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 7-40). Authentication Type (continued)	From the pull-down menu, 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 Authentication Server and Authentication Secret fields. • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the Authentication Server and Authentication Secret fields. • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the Authentication Server and Authentication Secret fields. • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the Authentication Server and Authentication Secret fields. • **WIKID-PAP**. WIKID Systems PAP. Complete the Authentication Server and Authentication Secret fields. • **WIKID-CHAP**. WIKID Systems CHAP. Complete the Authentication Server and Authentication Secret fields. • **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the Authentication Server and Authentication Secret fields. • **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the Authentication Server and Authentication Secret fields. • **NT Domain**. Microsoft Windows NT Domain. Complete the Authentication Server and Workgroup fields. • **Active Directory**. Microsoft Active Directory. Complete the Authentication Server and Active Directory Domain fields. • **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the Authentication Server and LDAP Base DN fields.

Table 8-2. SSL VPN Wizard Step 2: Domain Settings (continued)

Setting	Description (or Subfield and 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.

SSL VPN Wizard Step 3 of 6: User Settings

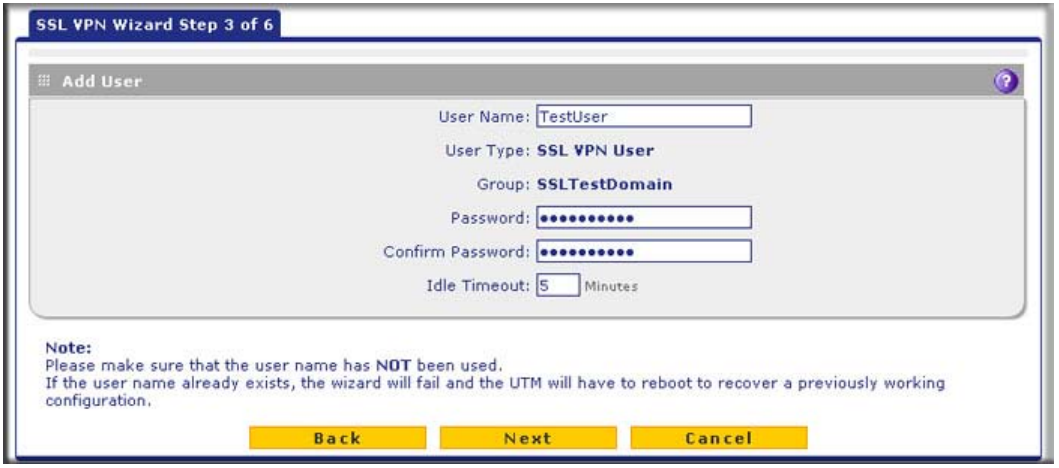


Figure 8-4

Note that Figure 8-4 contains some examples. Enter the settings as explained in Table 8-3 on page 8-8, then click **Next** to go the following screen.

Note: Do not enter an existing user name in the in the User Name field, otherwise the SSL VPN Wizard will fail and the UTM will reboot to recover its configuration.

Note: 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 "Configuring User Accounts" on page 9-9.

Table 8-3. SSL VPN Wizard Step 3: User Settings

Setting	Description (or Subfield and 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 always is 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 must belong to a group, and a group must belong to a domain.) You cannot change the group on this screen; the group is displayed for information only.
Password	The password that must be entered by the user to gain access to the UTM. The password must contain alphanumeric, '—' or '_' characters.
Confirm Password	This field must be identical to the Password field above.
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.

SSL VPN Wizard Step 4 of 6: Client IP Address Range and Routes

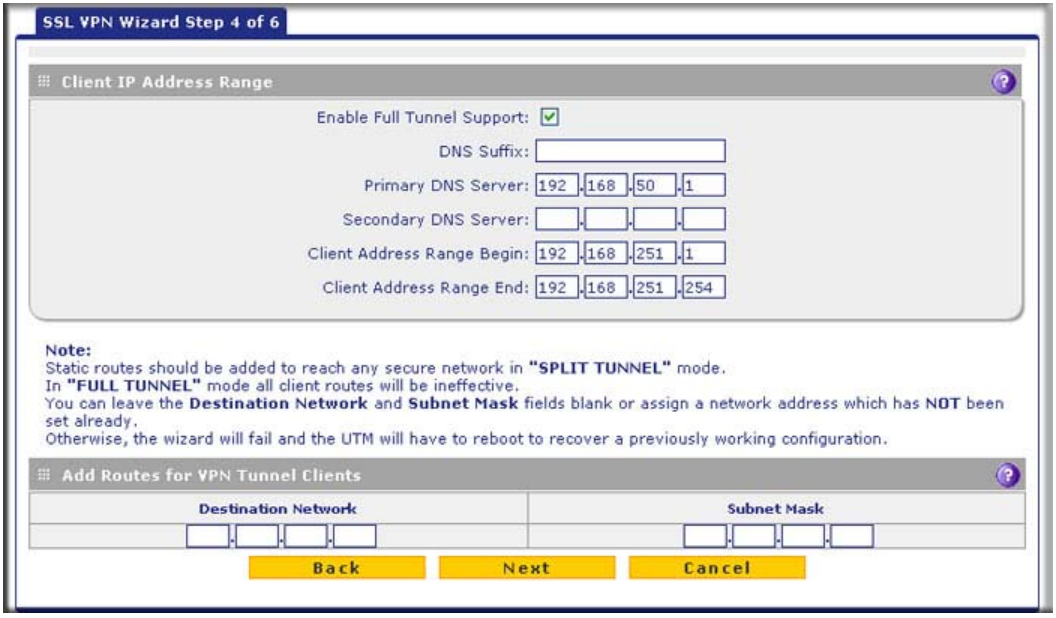


Figure 8-5

Note that Figure 8-5 contains some examples. Enter the settings as explained in Table 8-4 on page 8-10, 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.

	Note: 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 "Configuring the SSL VPN Client" on page 8-25.

Table 8-4. SSL VPN Wizard Step 4: Client IP Address Range and Routes Settings

Item	Description (or Subfield and Description)
Client IP Address Range	
Enable Full Tunnel Support	Select this checkbox to enable full tunnel support. If you leave this checkbox deselected (which is the default setting), split tunnel support is enabled, and you must 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 is an option.
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This is an option. **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 is an option.
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.

SSL VPN Wizard Step 5 of 6: Port Forwarding

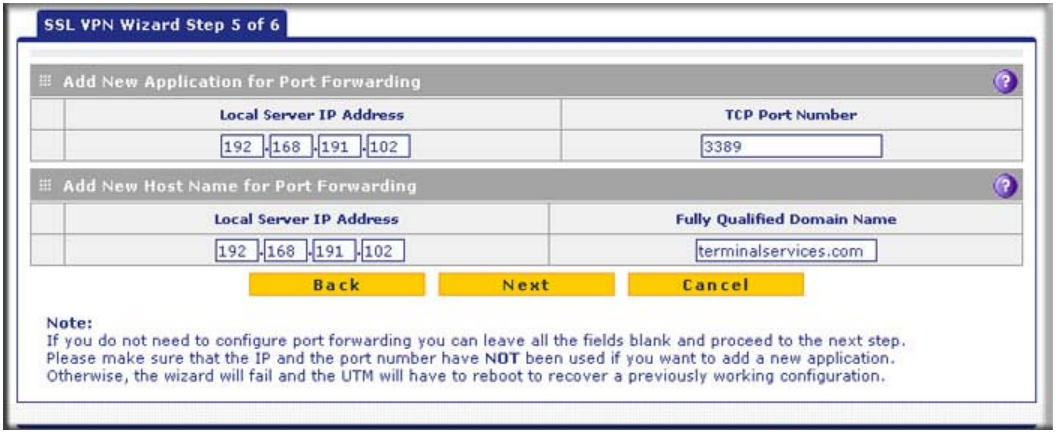


Figure 8-6

Note that Figure 8-6 contains some examples. Enter the settings as explained in Table 8-5, then click **Next** to go the following screen.

Note: Do not enter an IP address that is already in use in the first Local Server IP Address field or a port number that is already in use in the TCP Port NumberAction field, otherwise the SSL VPN Wizard will fail and the UTM will reboot to recover its configuration.

Note: 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 "Configuring Applications for Port Forwarding" on page 8-22.

Table 8-5. SSL VPN Wizard Step 5: Port Forwarding Settings

Item	Description (or Subfield and 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.

Table 8-5. SSL VPN Wizard Step 5: Port Forwarding Settings (continued)

Item	Description (or Subfield and Description)	
TCP Port NumberAction	The TCP port number of the application that is accessed through the SSL VPN tunnel. Below 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
	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 Local Server IP Address fields on this screen (that is, the one in the Add New Application for Port Forwarding section and the one in the Add New Host Name for Port Forwarding section) must contain the same IP address.	
Fully Qualified Domain NameAction	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.

SSL VPN Wizard Step 6 of 6: Verify and Save Your Settings

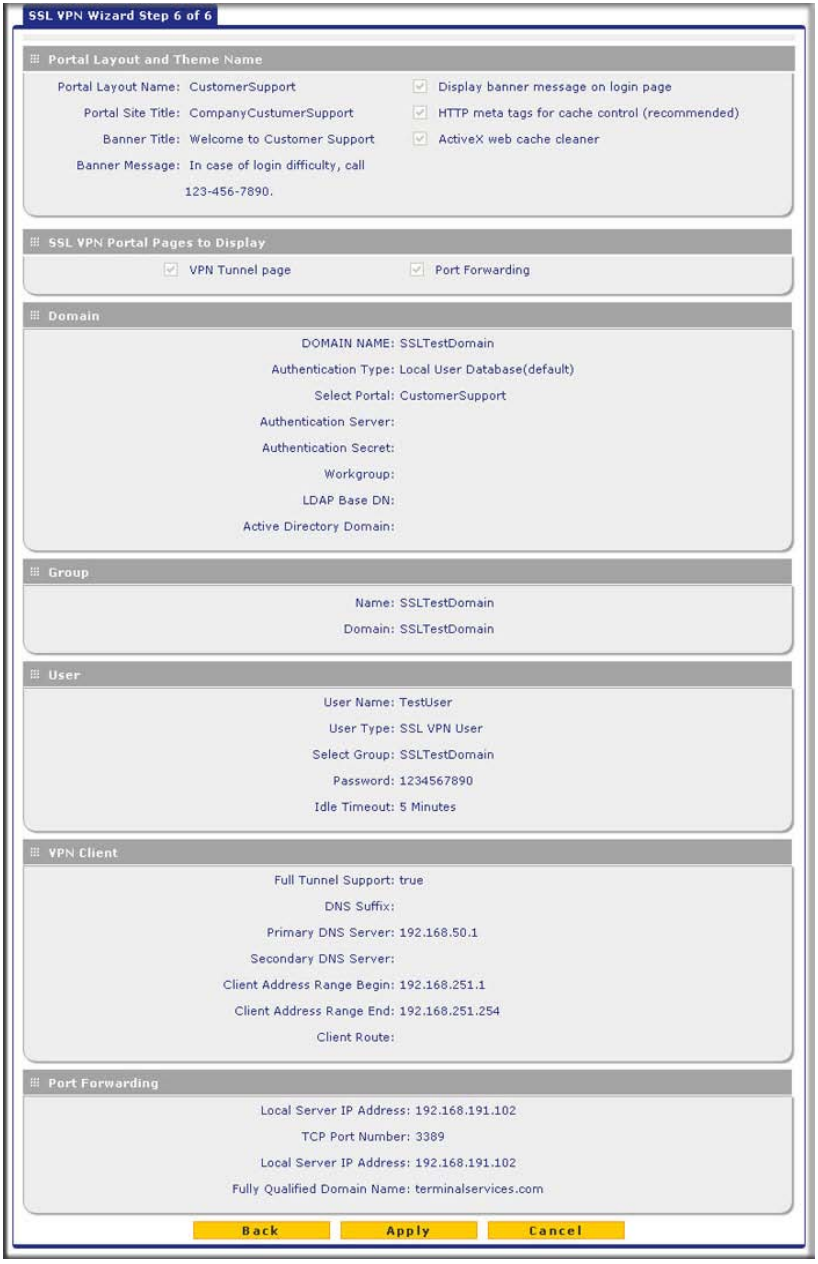
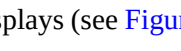


Figure 8-7

Verify your settings; if you need to make any changes, click the Back action button (if needed several times) to return to the screen on which you want to make changes.

Click **Apply** to save your settings. If the settings are accepted by the UTM, a message “Operation Succeeded” appears at the top of the screen, and the “Welcome to the Netgear Configuration Wizard” screen displays again (see Figure 8-1 on page 8-2).

Accessing the New SSL Portal Login Screen

All screens that you can access from the SSL VPN menu of the Web Management Interface display a user portal link at the right upper corner, above the menu bars (

).

When you click on the user portal link, the SSL VPN default portal opens (see Figure 8-9 on page 8-15.) 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** from the menu. The SSL VPN submenu tabs appear, with the Policies screen in view.
2. Click the **Portal Layouts** submenu tab. The Portal Layout screen displays (see Figure 8-12 on page 8-19).
3. In the Portal URL field of the List of Layouts table, click on 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 (see Figure 8-8 on page 8-15).

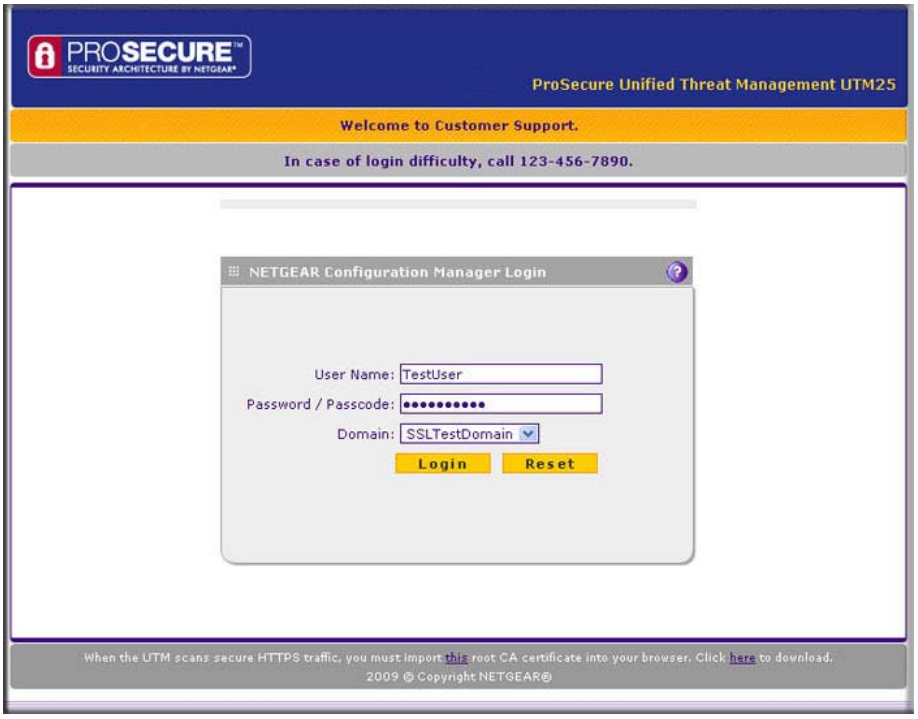


Figure 8-8

4. Enter the user name and password that you just created with the help of the SSL VPN Wizard
5. Click **Login**. The default User Portal screen displays.

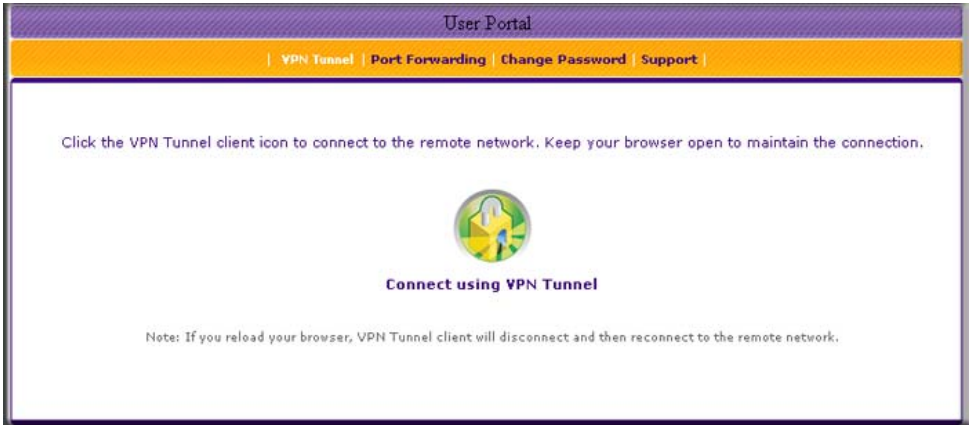


Figure 8-9

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 in "SSL VPN Wizard Step 5 of 6: Port Forwarding" on page 8-11.
- **Change Password**. Allows the user to change their password.
- **Support**. Provides access to the NETGEAR Web site.

Viewing the UTM SSL VPN Connection Status

To review the status of current SSL VPN tunnels:

1. Select **Monitoring > Active Users & VPNs** from the main menu. The Active Users & VPN submenu tabs appear, with the Active Users screen in views
2. Click the **SSL VPN Connection Status** submenu tab. The SSL VPN Connection Status screen displays.

Figure 8-10

The active user's user name, group, and IP address are listed in the table with a timestamp 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.

Viewing the UTM SSL VPN Log

To query the SSL VPN log:

1. Select **Monitoring** > **Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Logs Query** submenu tab. The Logs Query screen displays.

3. From the Log Type pull-down menu, select **SSL VPN**. The SSL VPN logs display.

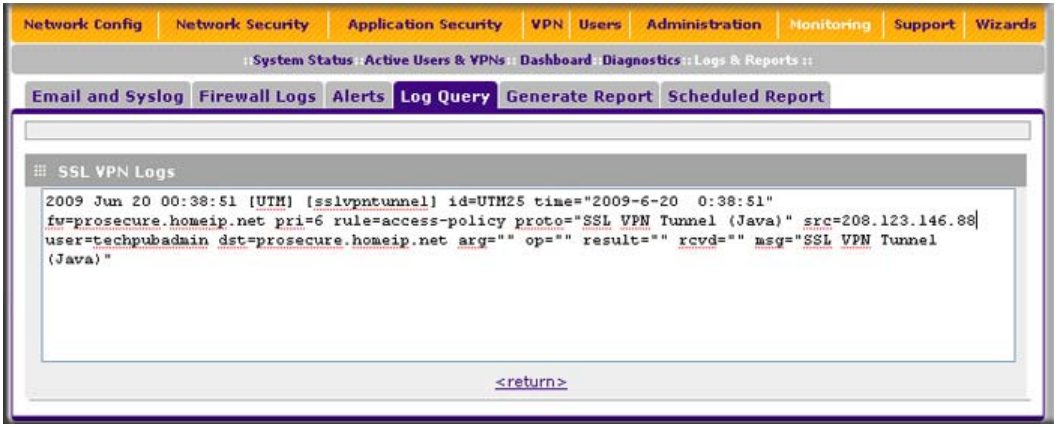


Figure 8-11

Manually Configuring and Editing 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 "Creating the Portal Layout" on page 8-18).

   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 "Configuring Domains, Groups, and Users" on page 8-22).)

   a. Create one or more authentication domains for authentication of SSL VPN users,

      When remote users log in to the UTM, they must 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 must 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 must 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 must 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 ("Configuring Applications for Port Forwarding" on page 8-22).

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 "Configuring the SSL VPN Client" on page 8-25).

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 "Using Network Resource Objects to Simplify Policies" on page 8-28).

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 "Configuring User, Group, and Global Policies" on page 8-31).

Policies determine access to network resources and addresses for individual users, groups, or everyone.

Creating the Portal Layout

The Portal Layouts screen that you can access from the SSL VPN menu allows you to create a custom page that remote users see when they log into 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 only permitted to access a few resources, the page that you create presents only the resources that are relevant to these users.

Portal layouts are applied 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 “Configuring Domains” on page 9-2). 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 may 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 SSL UTM by clicking the default button in the Action column of the List of Layouts, to the right of the desired portal layout.

To create a new SSL VPN portal layout:

1. Select **VPN** > **SSL VPN** from the menu. The SSL VPN submenu tabs appear, with the Policies screen in view.
2. Click the **Portal Layouts** submenu tab. The Portal Layout screen displays. (Figure 8-12 shows layouts in the List of Layouts table as an example.)

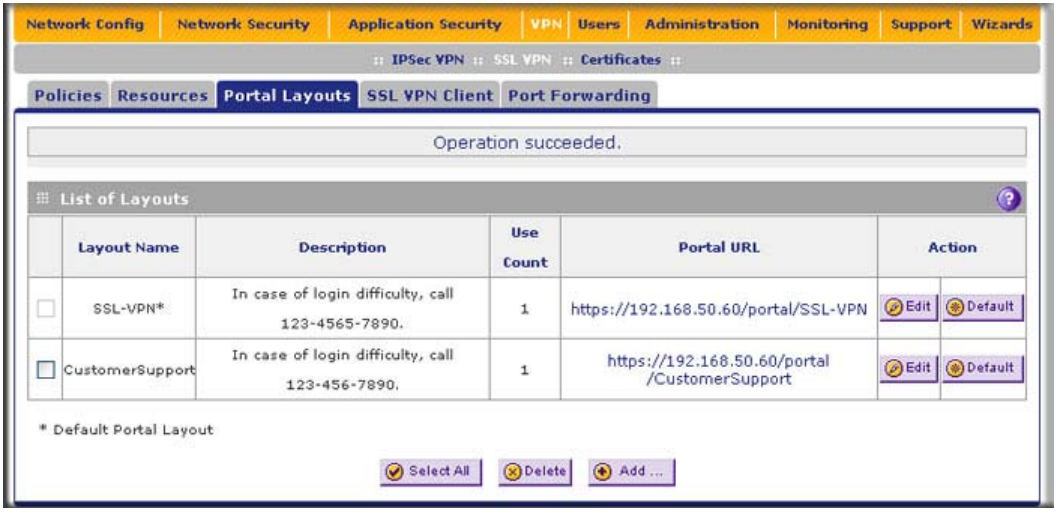


Figure 8-12

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 8-8 on page 8-15).
- **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 that allow you to edit or delete the portal layout.

3. Under the List of Layouts table, click the **Add** table button. The Add Portal Layout screen displays. (Figure 8-13 shows some examples.)

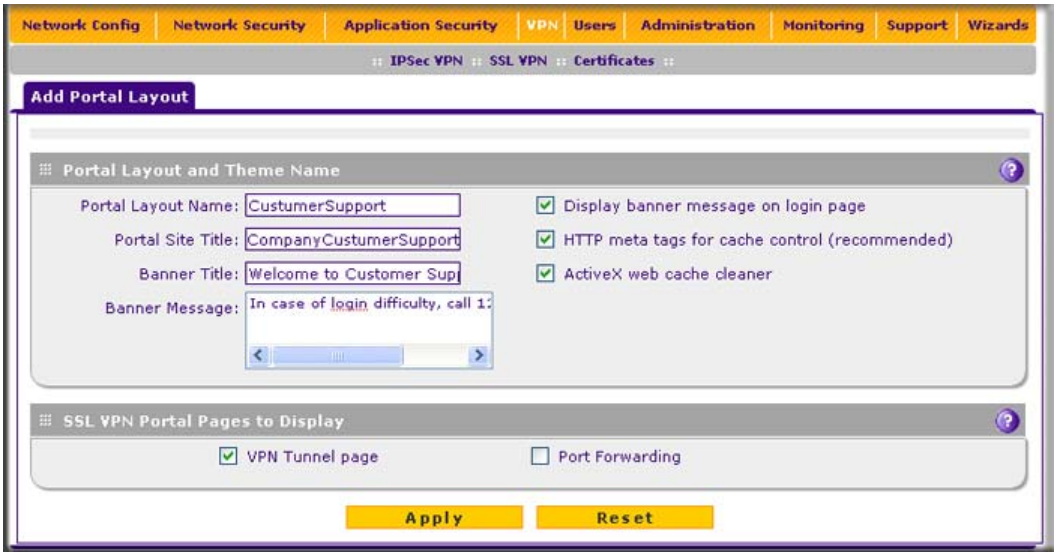


Figure 8-13

4. Complete the fields and select the checkboxes as explained Table 8-6.

Table 8-6. Add Portal Layout Settings

Item	Description (or Subfield and 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 sub-site 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 non-alphanumeric character. **Note**: Unlike most other URLs, this name is case-sensitive.
Portal Site Title	The title that appears 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.” **Note**: For an example, see Figure 8-8 on page 8-15. 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 Java script tags. The maximum length of the login page message is 4096 characters. **Note**: For an example, see Figure 8-8 on page 8-15. The banner message text is displayed in the grey header bar.
Display banner message on login page	Select this checkbox to show the banner title and banner message text on the login screen as shown in Figure 8-8 on page 8-15.

HTTP meta tags for cache control (recommended)	Select this checkbox 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.

Table 8-6. Add Portal Layout Settings (continued)

Item	Description (or Subfield and Description)
ActiveX web cache cleaner	Select this checkbox 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	Select this checkbox to provide full network connectivity.
Port Forwarding	Select this checkbox to provides access to specific defined network services **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.

5. Click **Apply** to save your settings. The new portal layout is added to the List of Layouts table. To display the new portal layout.

Configuring Domains, Groups, and Users

Remote users connecting to the UTM through an SSL VPN portal must be authenticated before they are being granted access to the network. The login window 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 must create name and password accounts for the SSL VPN users. When you create a user account, you must specify a group. Groups are used to simplify the application of access policies. When you create a group, you must specify a domain. Therefore, you should create any domains first, then groups, and then user accounts.

To configure domains, groups, and users, see “Configuring VPN Authentication Domains, Groups, and Users” on page 9-1.

Configuring Applications for Port Forwarding

Port forwarding provides access to specific defined network services. To define these services, you must 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.

Adding Servers and Port Numbers

To configure port forwarding, you must 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** from the menu. The SSL VPN s submenu tabs appear, with the Policies screen in view.
2. Click the **Port Forwarding** submenu tab. The Port Forwarding screen displays. (Figure 8-14 shows some examples.)

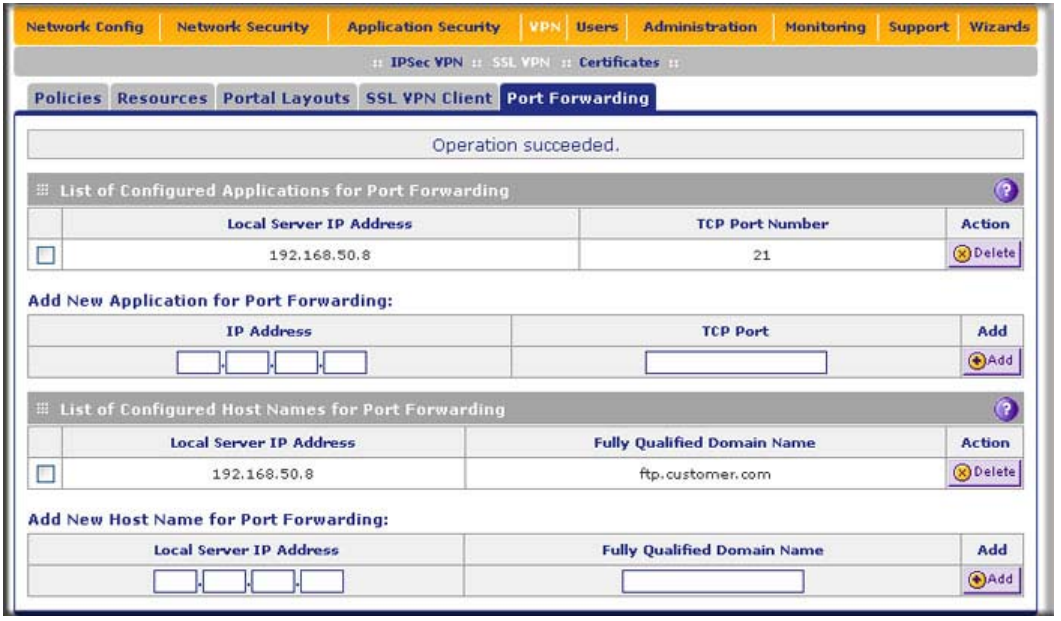


Figure 8-14

3. 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. Table 8-7 on page 8-24 lists some commonly used TCP applications and port numbers.

Table 8-7. 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.

4. 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 into the SSL VPN portal and launched port forwarding.

To delete an application from the List of Configured Applications for Port Forwarding table, select the checkbox to the left of the application that you want to delete, and then click the **Delete** table button in the Action column.

Adding 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** from the menu. The SSL VPN s submenu tabs appear, with the Policies screen in view.
2. Click the **Port Forwarding** submenu tab. The Port Forwarding screen displays (see Figure 8-14 on page 8-23).

3. 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 appear in the List of Configured Applications for Port Forwarding table, you must add it before you can rename it.

4. 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, select the checkbox to the left of the name that you want to delete, and then click the **Delete** table button in the Action column.

Configuring 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 than the subnet that is used by the local network, you must add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel.

Configuring the Client IP Address Range

First determine the address range to be assigned to VPN tunnel clients, then define the address range.

To define the client IP address range:

1. Select **VPN** > **SSL VPN** from the menu. The SSL VPN s submenu tabs appear, with the Policies screen in view.
2. Click the **SSL VPN Client** submenu tab. The SSL VPN Client screen displays.

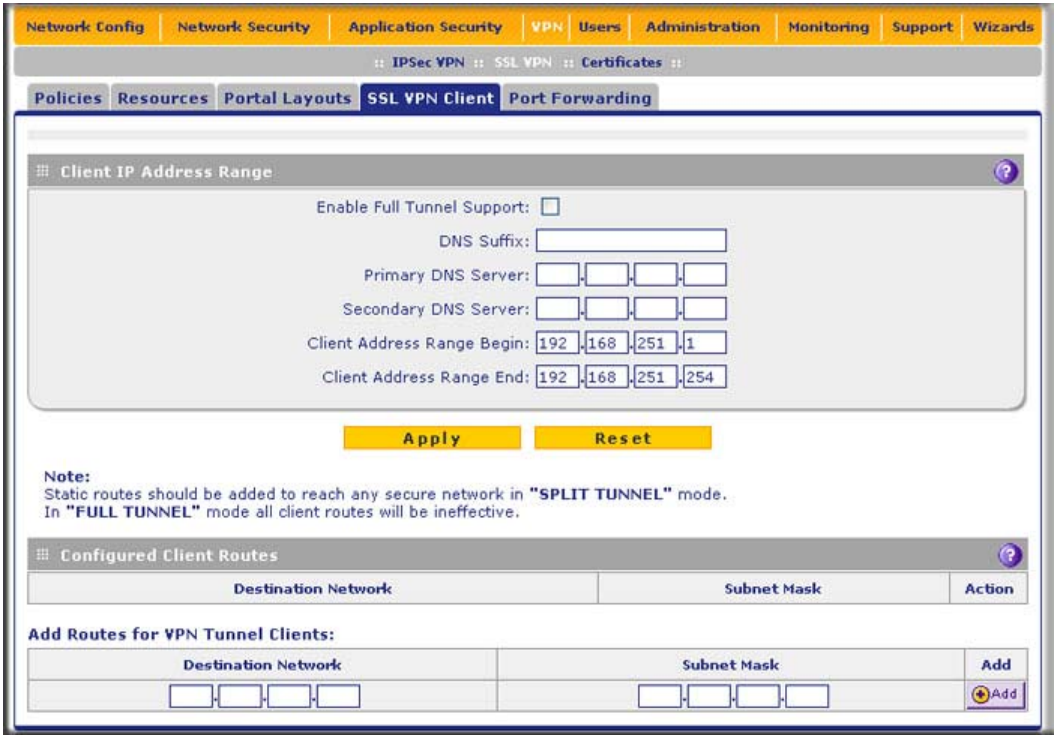


Figure 8-15

3. Select the checkbox and complete the fields as explained Table 8-8.

Table 8-8. Client IP Address Range Settings

Item	Description (or Subfield and Description)
Client IP Address Range	
Enable Full Tunnel Support	Select this checkbox to enable full tunnel support. If you leave this checkbox deselected (which is the default setting), split tunnel support is enabled, and you must add client routes (see "Adding Routes for VPN Tunnel Clients" on page 8-27). **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 is an option.
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This is an option. **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 is an option.
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.

4. 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.

Adding 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 than the local network, or if the local network has multiple subnets, or if you select split mode tunnel operation, you must define client routes.

To add an SSL VPN tunnel client route:

1. Select **VPN** > **SSL VPN** from the menu. The SSL VPN s submenu tabs appear, with the Policies screen in view.
2. Click the **SSL VPN Client** submenu tab. The SSL VPN Client screen displays (see Figure 8-15 on page 8-26).
3. 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.
4. Click the **Add** table button. The new client route is added to the Configured Client Routes table.

Restart the UTM if VPN tunnel clients are currently connected. 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.

Using 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.

Adding New Network Resources

To define a network resource:

1. Select **VPN** > **SSL VPN** from the menu. The SSL VPN s submenu tabs appear, with the Policies screen in view.
2. Click the **Resources** submenu tab. The Resources screen displays. (Figure 8-16 shows some resources in the List of Resource(s) table as an example.)

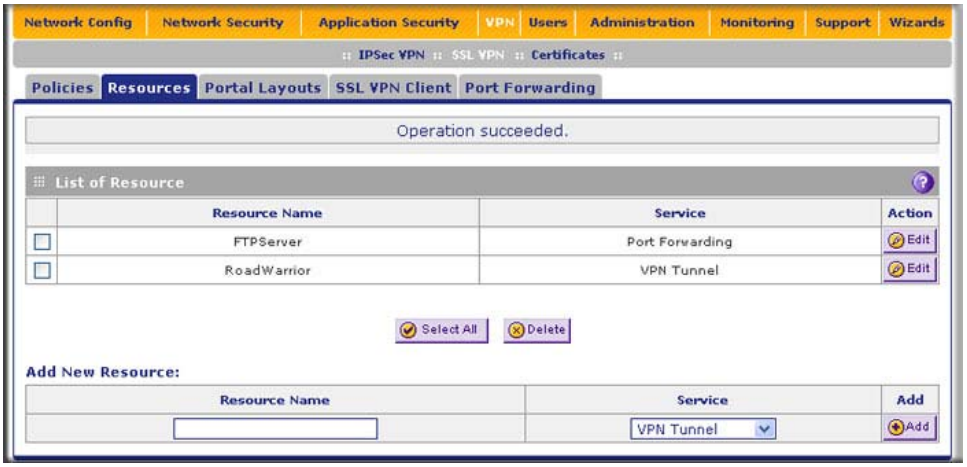


Figure 8-16

3. 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 pull-down menu, 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 a port forwarding.
     - **All**. The resource applies both to a VPN tunnel and to port forwarding.
4. 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 checkbox to the left of the network resource that you want to delete or click the **Select All** table button to select all VPN policies.
2. Click the **Delete** table button.

Editing Network Resources to Specify Addresses

1. Select **VPN** > **SSL VPN** from the menu. The SSL VPN s submenu tabs appear, with the Policies screen in view.
2. Click the **Resources** submenu tab. The Resources screen displays (see Figure 8-16 on page 8-29, which shows some examples).
3. 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. (Figure 8-17 shows some examples.)

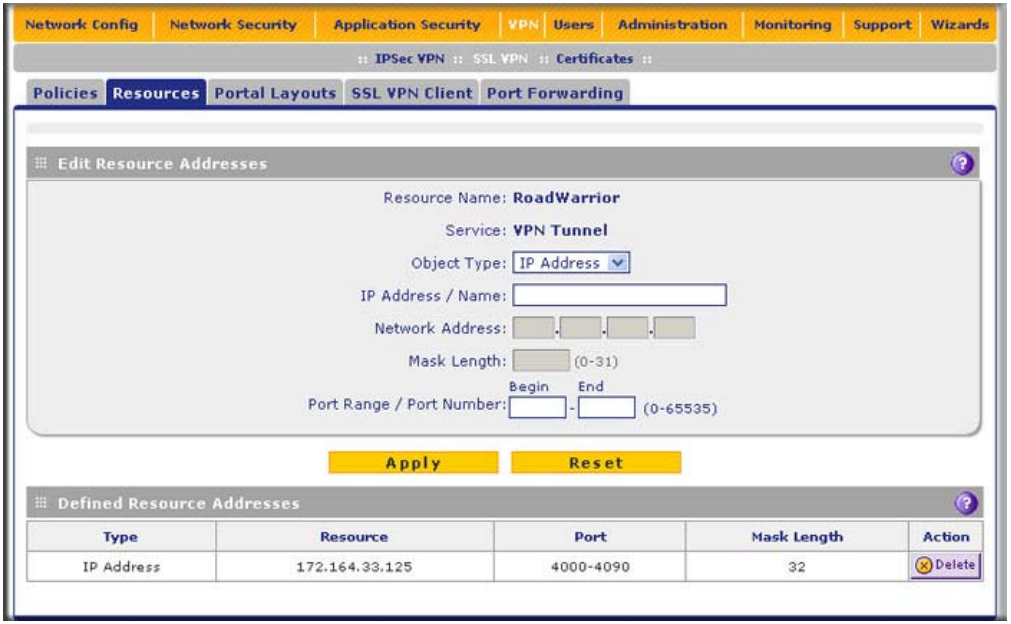


Figure 8-17

4. Complete the fields and make your selection from the pull-down menu as explained Table 8-8.

Table 8-9. Add Resource Addresses Settings

Item	Description (or Subfield and 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.
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.

Table 8-9. Add Resource Addresses Settings (continued)

Item	Description (or Subfield and Description)	
Object Type	From the pull-down menu, select one of the following options: • **IP Address**. The object is an IP address. You must enter the IP address or the FQDN in the IP Address / Name field. • **IP Network**. The object is an IP network, You must 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.
	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.	

5. 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.

Configuring 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:

1. User policies take precedence over all group policies.
2. Group policies take precedence over all global policies.
3. 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 would attempt to access:

- an FTP server at 10.0.0.1, the user would be blocked by Policy 1.
- an FTP server at 10.0.1.5, the user would be blocked by Policy 2.
- an FTP server at 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.
- an FTP server at 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.

Viewing Policies

To view the existing policies, follow these steps:

1. Select **VPN** > **SSL VPN** from the menu. The SSL VPN s submenu tabs appear, with the Policies screen in view. (Figure 8-18 on page 8-33 shows some examples.)

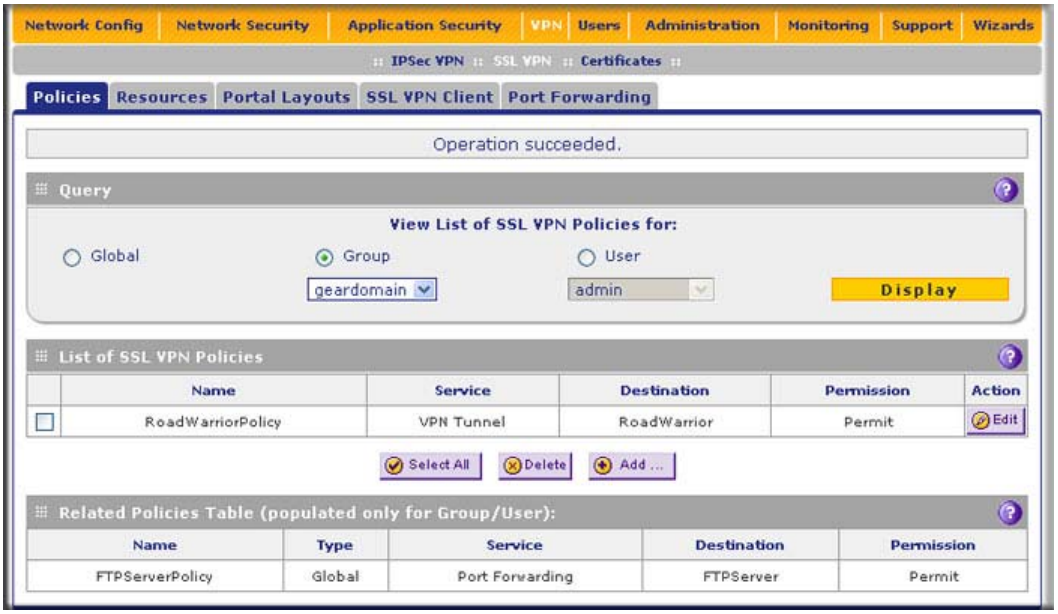


Figure 8-18

2. Make your selection from the following Query options:
   - Click **Global** to view all global policies.
   - Click **Group** to view group policies, and choose the relevant group's name from the pull-down menu.
   - Click **User** to view group policies, and choose the relevant user's name from the pull-down menu.
3. Click the **Display** action button. The List of SSL VPN Policies table displays the list for your selected Query option.

Adding a Policy

To add an SSL VPN policy:

1. Select **VPN** > **SSL VPN** from the menu. The SSL VPN s submenu tabs appear, with the Policies screen in view (see Figure 8-18, which shows some examples).
2. Under the List of SSL VPN Policies table, click the **Add** table button. The Add Policy screen displays (see Figure 8-19 on page 8-34).

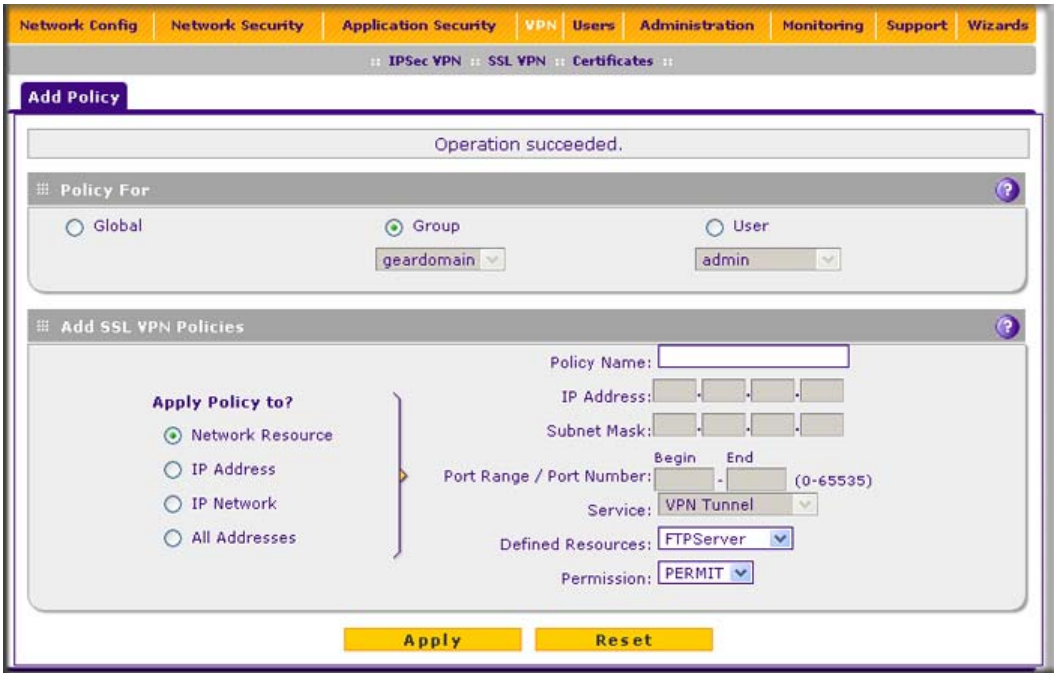


Figure 8-19

3. Select the radio buttons, complete the fields, and make your selection from the pull-down menus as explained Table 8-10.

Table 8-10. Add Policy Settings

Item	Description (or Subfield and 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 excludes all groups and users. • **Group**. The new policy must be limited to a single group. From the pull-down menu, select a group name. **Note**: For information about how to create groups, see "Configuring Groups for VPN Policies" on page 9-6. • **User**. The new policy must be limited to a single user. From the pull-down menu, select a user name. **Note**: For information about how to create user accounts, see "Configuring User Accounts" on page 9-9.	

Table 8-10. Add Policy Settings (continued)

Item	Description (or Subfield and Description)		
Add SSL VPN Policies			
Apply Policy For	Select one of the following radio buttons to specify how the policy is applied: • **Network Resource**. The policy is applied to a network resource that you have defined on the Resources screen (see "Using Network Resource Objects to Simplify Policies" on page 8-28). The screen adjust to unmask the fields that are shown in the Network Resource fields below. • **IP Address**. The policy is applied to a single IP address. The screen adjust to unmask the fields that are shown in the IP Address fields below. • **IP Network**. The policy is applied to a network address. The screen adjust to unmask the fields that are shown in the IP Network fields below. • **All Addresses**. The policy is applied to a all address. The screen adjust to unmask the fields that are shown in the All Addresses fields below.		
	Network Resource	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		Defined Resources	From the pull-down menu, select the network resource that you have defined on the Resources screen (see "Using Network Resource Objects to Simplify Policies" on page 8-28).
		Permission	From the pull-down menu, select whether the policy permits (PERMIT) or denies (DENY) 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 (enter in the Begin field) or a range of ports (enter 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 pull-down menu, 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 pull-down menu, select whether the policy permits (PERMIT) or denies (DENY) access.

Table 8-10. Add Policy Settings (continued)

Item	Description (or Subfield and Description)		
Apply Policy For (continued)	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 (enter in the Begin field) or a range of ports (enter 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 pull-down menu, 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 pull-down menu, select whether the policy permits (PERMIT) or denies (DENY) access.
	All Addresses	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		Port Range / Port Number	A port (enter in the Begin field) or a range of ports (enter 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 pull-down menu, 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 pull-down menu, select whether the policy permits (PERMIT) or denies (DENY) 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: In addition to configuring SSL VPN user policies, ensure that HTTPS remote management is enabled (see "Configuring Remote Management Access" on page 10-12). If it not enabled, all SSL VPN user connections are disabled.

Chapter 9
Managing Users, Authentication, and Certificates

This chapter describes how to manage users, authentication, and security certificates for IPsec VPN and SSL VPN. This chapter contains the following sections:

Configuring VPN Authentication Domains, Groups, and Users

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.

You must create name and password accounts for all users who must be able connect to the UTM. This includes administrators 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 must be authenticated before being allowed to access the UTM or the VPN-protected network. The login window 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 must specify a group. When you create a group, you must specify a domain. Therefore, you should first create any domains, then groups, then user accounts.

Configuring 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.

Table 9-1 summarizes the authentication protocols and methods that the UTM supports.

Table 9-1.Authentication Protocols and Methods

Authentication Protocol or Method	Description (or Subfield and 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 or CHAP 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 pass code with a short expiration period. The client logs in with the pass code. See Appendix D, "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. **Note**: A Microsoft Active Directory database uses an LDAP organization schema.

Table 9-1.Authentication Protocols and Methods

Authentication Protocol or Method	Description (or Subfield and 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.

To create a domain:

1. Select **Users** > **Domains** from the menu. The Domains screen displays. Figure 9-1 shows the UTM's default domain—geardomain—and, as an example, another domain in the List of Domains table.

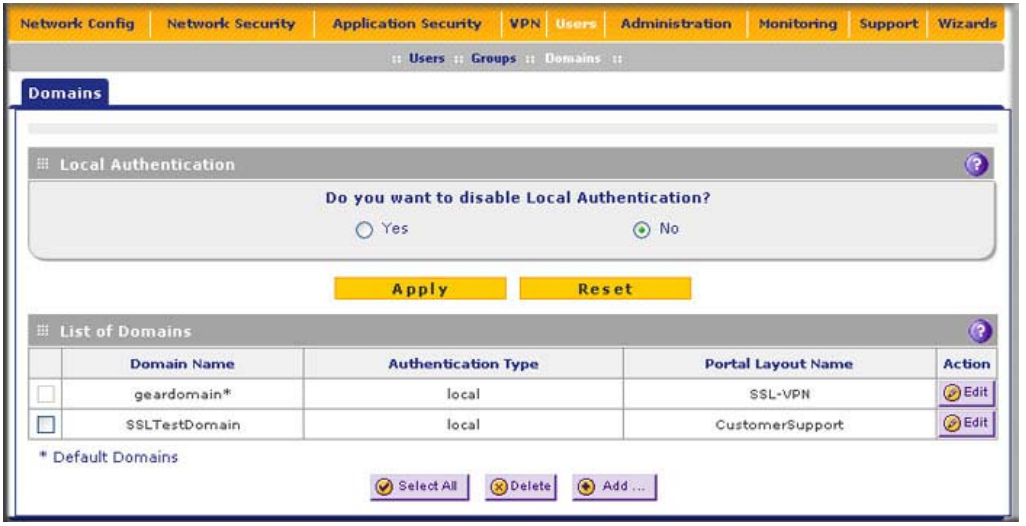


Figure 9-1

The List of Domains table displays the domains with the following fields:

- **Checkbox**. 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 that provides access to the Edit Domain screen.

2. Under the List of Domains table, click the **Add** table button. The Add Domain screen displays.

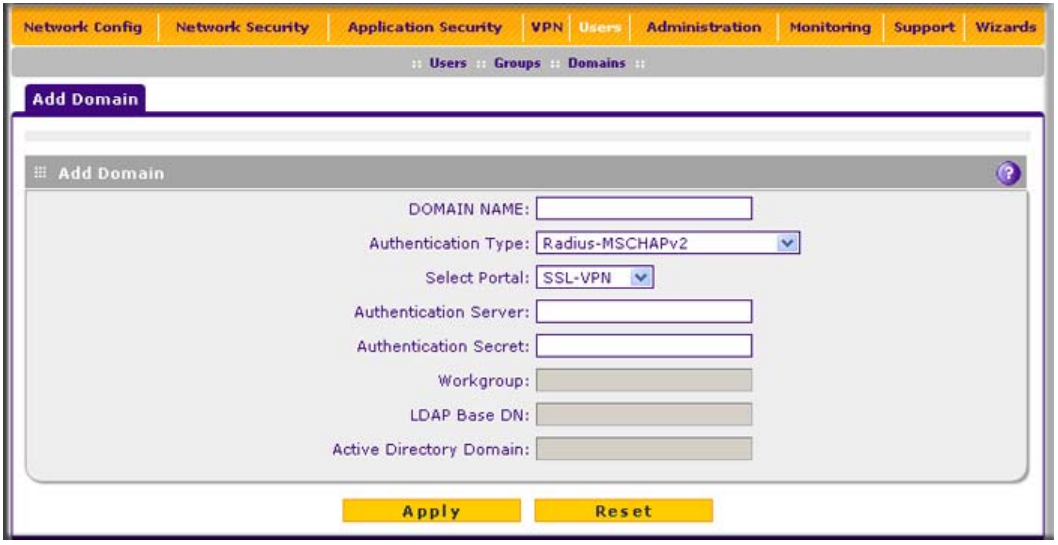


Figure 9-2

3. Enter the settings as explained in Table 9-2.

Table 9-2. Add Domain Settings

Setting	Description (or Subfield and 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 7-40).	From the pull-down menu, 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 Authentication Server and Authentication Secret fields. • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the Authentication Server and Authentication Secret fields. • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the Authentication Server and Authentication Secret fields. • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the Authentication Server and Authentication Secret fields. • **WIKID-PAP**. WIKID Systems PAP. Complete the Authentication Server and Authentication Secret fields.

Table 9-2. Add Domain Settings (continued)

Setting	Description (or Subfield and Description)
Authentication Type (continued)(	• **WIKID-CHAP**. WIKID Systems CHAP. Complete the Authentication Server and Authentication Secret fields. • **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the Authentication Server and Authentication Secret fields. • **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the Authentication Server and Authentication Secret fields. • **NT Domain**. Microsoft Windows NT Domain. Complete the Authentication Server and Workgroup fields. • **Active Directory**. Microsoft Active Directory. Complete the Authentication Server and Active Directory Domain fields. • **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the Authentication Server and LDAP Base DN fields.
Select Portal	The pull-down menu shows the SSL portals that are listed on the Portal Layout screen. From the pull-down menu, select the SSL portal with which the domain is associated. For information about how to configure SSL portals, see "Creating the Portal Layout" on page 8-18.
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.

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: select the **No** radio button in the Local Authentication section of the Domain screen (see Figure 9-1 on page 9-3).

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 checkbox to the left of the 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.

Configuring Groups for VPN Policies

The use of groups simplifies the configuration of VPN policies when different sets of users have different restrictions and access controls. 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 group. In addition, when you create a new domain on the second SSL VPN Wizard screen (see "SSL VPN Wizard Step 2 of 6: Domain Settings" on page 8-5), a default group with the same name as the domain is automatically created.

Note: IPsec VPN users always belong to the default domain (geardomain) and are not assigned to groups.

Note: Groups that are defined in the User menu 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 "Managing Groups and Hosts (LAN Groups)" on page 4-12.

Creating and Deleting Groups

To create a VPN group:

1. Select **Users** > **Groups** from the menu. The Groups screen displays. Figure 9-3 shows the UTM's default group—geardomain—and, as an example, several other groups in the List of Groups table.

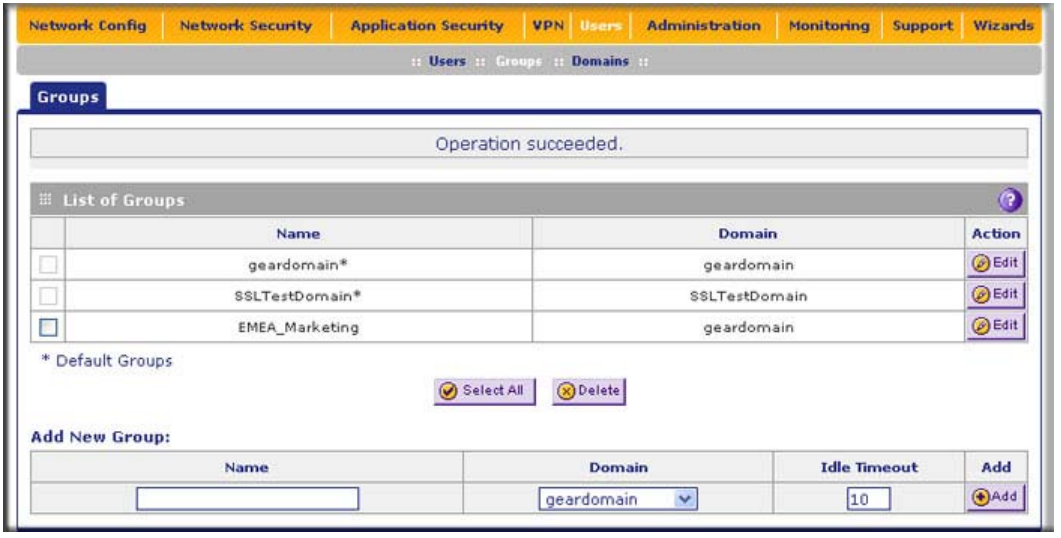


Figure 9-3

The List of Groups table displays the VPN groups with the following fields:

- **Checkbox**. 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 only delete 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 that provides access to the Edit Group screen.

2. In the Add New Group section of the screen, enter the settings as explained in Table 9-3 on page 9-8.

Table 9-3. (VPN) Group Settings

Setting	Description (or Subfield and Description)
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.
Domain	The pull-down menu shows the domains that are listed on the Domain screen. From the pull-down menu, select the domain with which the group is associated. For information about how to configure domains, see "Configuring Domains" on page 9-2.
Idle Timeout	The period after which an idle user is automatically logged out of the UTM's Web management interface. De default idle timeout period is 10 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 checkbox to the left of the group that you want to delete or click the **Select All** table button to select all groups. You cannot delete a default group; you can only delete the domain with the identical name as the default group (see "Configuring Domains" on page 9-2), which causes the default group to be deleted.
2. Click the **Delete** table button.

Note: You cannot delete a default group that was automatically created when you created a new domain on the second SSL VPN Wizard screen (see "SSL VPN Wizard Step 2 of 6: Domain Settings" on page 8-5). You can only delete such a default group by deleting the domain for which the group was created (see "Configuring Domains" on page 9-2).

Editing Groups

To edit a VPN group:

1. Select **Users** > **Groups** from the menu. The Groups screen displays (see Figure 9-3 on page 9-7).
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 (see Figure 9-4 on page 9-9).

   With the exception of groups that are associated with domains that use the LDAP authentication method, you can only modify the idle timeout settings.

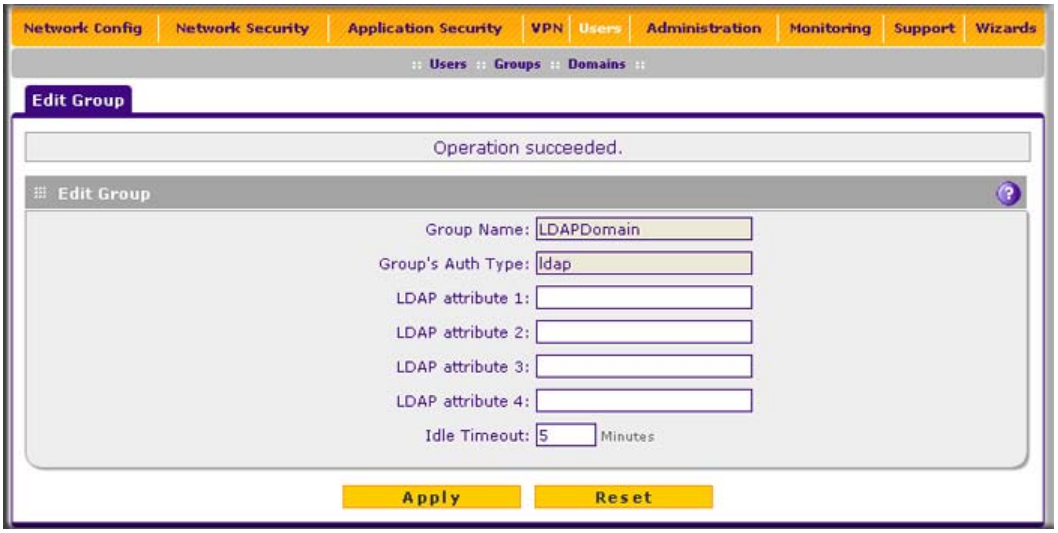


Figure 9-4

3. Modify the idle timeout 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.

Configuring User Accounts

When you create a user account, you must assign the user to a user group. When you create a group, you must assign the group to a domain that specifies the authentication method. Therefore, you should first create any domains, then groups, 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 only log in to the SSL VPN portal.
- **IPSEC VPN User**. A user who can only make an IPsec VPN connection via a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see “Configuring Extended Authentication (XAUTH)” on page 7-38).
- **Guest user**. A user who can only view the UTM configuration (that is, read-only access).

To create an individual user account:

1. Select **Users** > **Users** from the menu. The Users screen displays. Figure 9-5 shows the UTM's default users—admin and guest—and, as an example, several other users in the List of Users table.

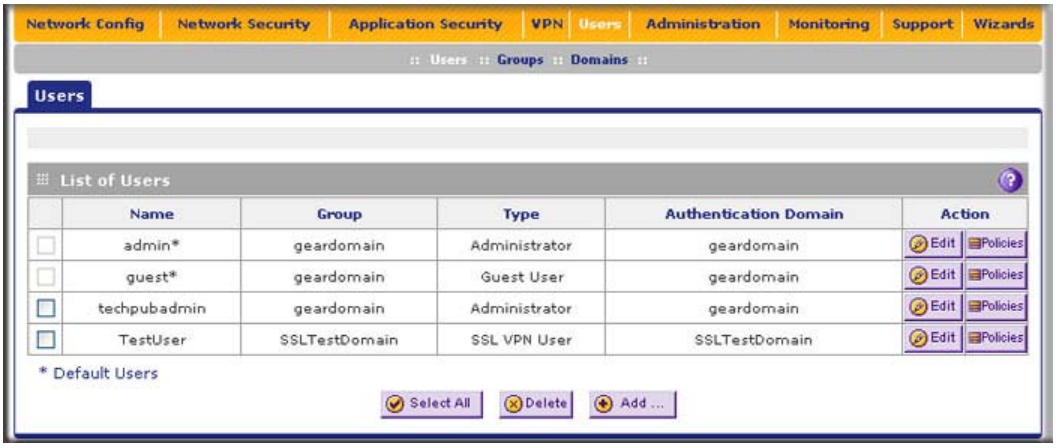


Figure 9-5

The List of Users table displays the users with the following fields:

- **Checkbox**. 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 pre-configured 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 that provides access to the Edit User screen; the policies table button that provides access to the policy screens.

2. Click the **Add** table button. The Add User screen displays (see Figure 9-6 on page 9-11).

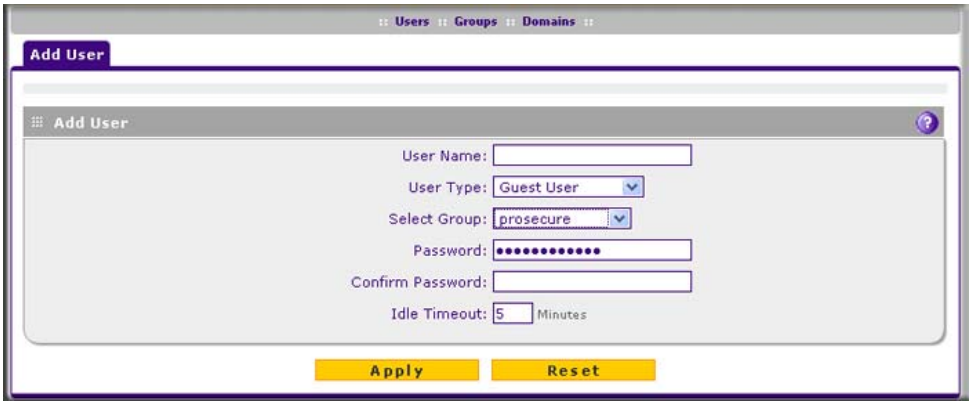


Figure 9-6

3. Enter the settings as explained in Table 9-4.

Table 9-4. Add User Settings

Setting	Description (or Subfield and Description)
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	From the pull-down menu, select one of the pre-defined 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 only log in to the SSL VPN portal. • **IPSEC VPN User**. User who can only make an IPsec VPN connection via a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see "Configuring Extended Authentication (XAUTH)" on page 7-38). • **Guest User**. User who can only view the UTM configuration (that is, read-only access).
Select Group	The pull-down menu shows the groups that are listed on the Group screen. From the pull-down menu, select the group to which the user is assigned. For information about how to configure groups, see "Configuring Groups for VPN Policies" on page 9-6. **Note**: The user is assigned to the domain that is associated with the selected group.
Password	The password that the user must enter to gain access to the UTM. The password must contain alphanumeric, '—' or '_' characters.
Confirm Password	This field must be identical to the Password field above.
Idle Timeout	The period after which an idle user is automatically logged out of the Web management interface. De default idle timeout period is 10 minutes.

4. Click **Apply** to save your settings. The user is added to the List of Users table.

To delete one or more users:

1. In the List of Users table, select the checkbox to the left of the user that you want to delete or click the **Select All** table button to select all users. You cannot delete a default user.
2. Click the **Delete** table button.

Setting User Login Policies

You can restrict the ability of defined users to log into the UTM's Web management interface. You can also require or prohibit logging in from certain IP addresses or from particular browsers.

Configuring Login Policies

To configure user login policies:

1. Select **Users** > **Users** from the menu. The Users screen displays (see Figure 9-5 on page 9-10).
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 appear, with the Login Policies screen in view.

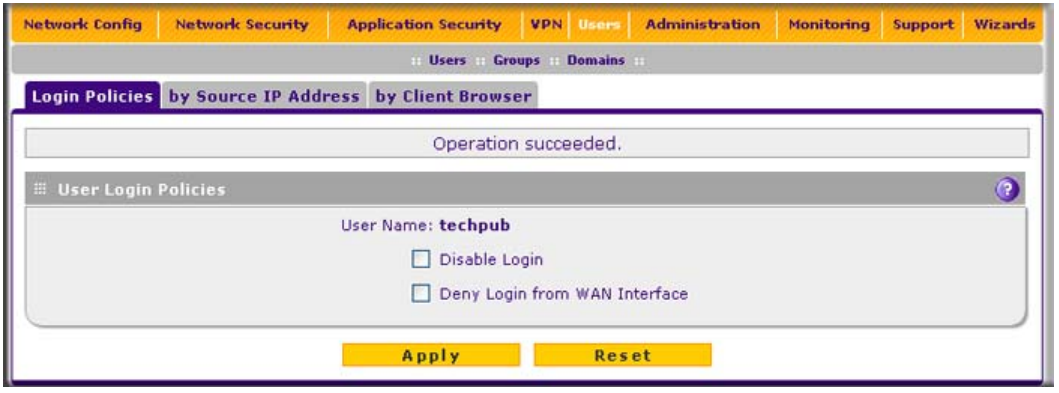


Figure 9-7

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** checkbox.
   - To prohibit this user from logging in from the WAN interface, select the **Deny Login from WAN Interface** checkbox. In this case, the user can log in only from the LAN interface.

Note: For security reasons, the Deny Login from WAN Interface checkbox is selected by default for guests and administrators. The Disable Login checkbox is disabled (masked out) for administrators.

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

Configuring Login Restrictions Based on IP Address

To restrict logging in based on IP address:

1. Select **Users** > **Users** from the menu. The Users screen displays (see Figure 9-5 on page 9-10).
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 appear, with the Login Policies screen in view.
3. Click the **by Source IP Address** submenu tab. The by Source IP Address screen displays. Figure 9-8 shows an IP address in the Defined Addresses table as an example.

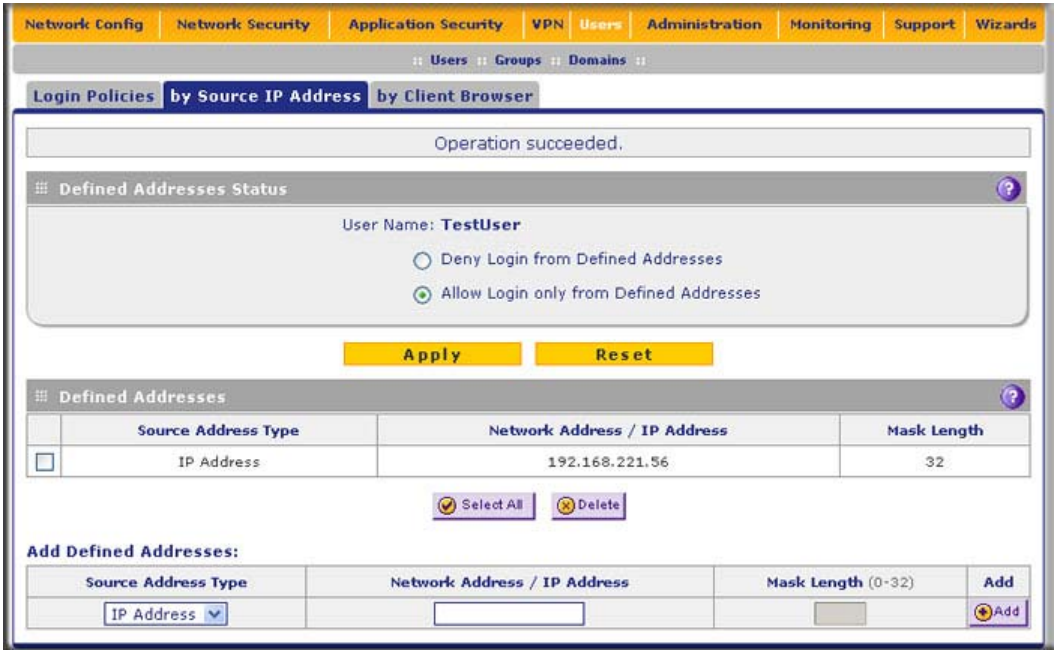


Figure 9-8

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 Table 9-5.

Table 9-5. Add Defined Addresses Settings

Setting	Description (or Subfield and Description)
Source Address Type	Select the type of address from the pull-down menu: • **IP Address**. A single IP address. • **IP Network**. A subnet of IP Addresses. You must enter a netmask length in the Mask Length field.
Network Address / IP Address	Depending on your selection of the **Source Address Type** pull-down menu, 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 checkbox to the left of the address that you want to delete or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Configuring Login Restrictions Based on Web Browser

To restrict logging in based on the user's browser:

1. Select **Users** > **Users** from the menu. The Users screen displays (see Figure 9-5 on page 9-10).
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 appear, with the Login Policies screen in view.

3. Click the **by Client Browser** submenu tab. The by Client Browser screen displays. Figure 9-9 shows a browser in the Defined Browsers table as an example.

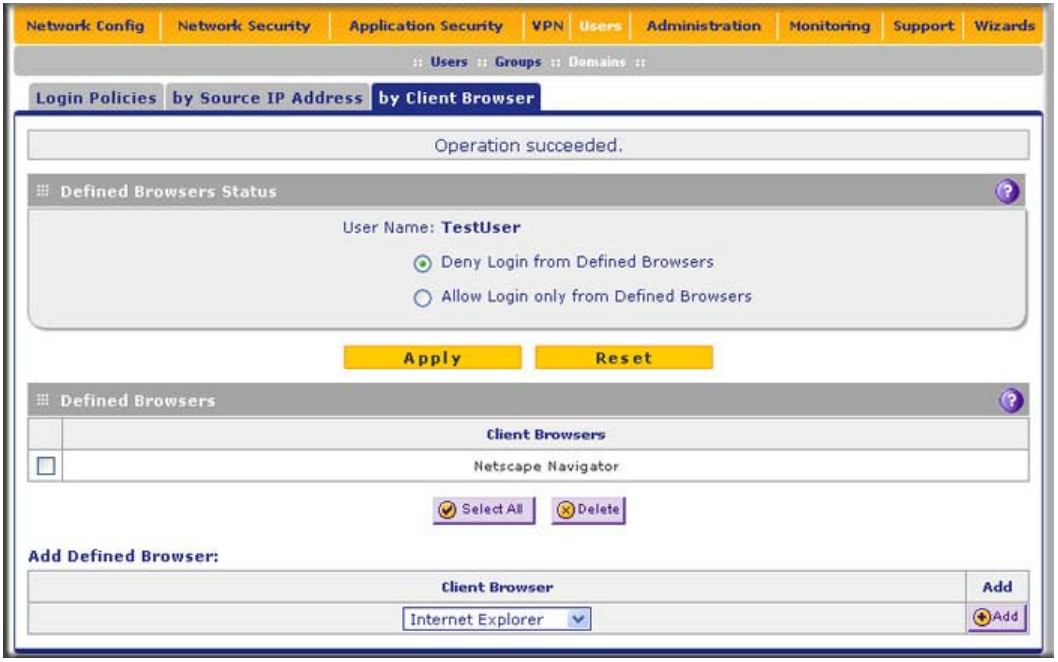


Figure 9-9

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 pull-down menu:
   - **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 checkbox to the left of the browser that you want to delete or click the **Select All** table button to select all browsers.
2. Click the **Delete** table button.

Changing Passwords and Other User Settings

For any user, you can change the password, user type, and idle timeout settings. Only administrators have read/write access. All other users have read-only access.

Note: The default password for the administrator and for a guest to access the UTM's Web management interface is **password**.

To modify user settings:

1. Select **Users** > **Users** from the menu. The Users screen displays (see Figure 9-5 on page 9-10).
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.

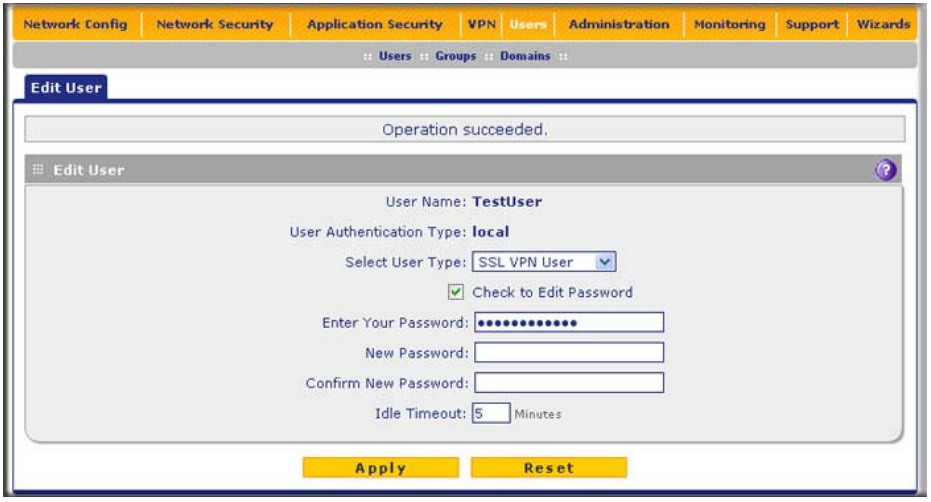


Figure 9-10

3. Enter the settings as explained in Table 9-6.

Table 9-6. Edit User Settings

Setting	Description (or Subfield and Description)	
User Type	From the pull-down menu, select one of the pre-defined 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 only log in to the SSL VPN portal. • **IPSEC VPN User**. User who can only make an IPsec VPN connection via a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see "Configuring Extended Authentication (XAUTH)" on page 7-38). • **Guest User**. User who can only view the UTM configuration (that is, read-only access).	
Check to Edit Password	Select this checkbox 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	Re-enter the new password for confirmation.
Idle Timeout	The period after which an idle user is automatically logged out of the Web management interface. De default idle timeout period is 10 minutes.	

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

Managing Digital Certificates

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 can be either self-signed or can be issued by certification authorities (CAs) such as an internal Windows server or an external organizations such as Verisign or Thawte.

However, if the digital certificates contain the extKeyUsage extension, the certificate must 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 must 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 certificate 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 digital certificate triggers a warning from most browsers because it provides no protection against identity theft of the server.

The UTM contains a self-signed digital 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.

To display the Certificates screen, select **VPN** > **Certificates** from the menu. 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 9-11 on page 9-19, Figure 9-13 on page 9-22, and Figure 9-15 on page 9-26).

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 digital certificates. Each CA issues its own CA identity digital certificate to validate communication with the CA and to verify the validity of digital certificates that are signed by the CA.
- Self digital 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 digital certificates that were issued by CAs and that you uploaded (see "Managing CA Certificates" on this page).
- **Active Self Certificates table**. Contains the digital self certificates that were issued by CAs and that you uploaded (see "Managing Self Certificates" on page 9-20).
- **Self Certificate Requests table**. Contains the self certificate requests that you generated. These request may or may not have been submitted to CAs, and CAs may or may not have issued digital certificates for these requests. Only the digital self certificates in the Active Self Certificates table are active on the UTM (see "Managing Self Certificates" on page 9-20).
- **Certificate Revocation Lists (CRL) table**. Contains the lists with digital 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 "Managing the Certificate Revocation List" on page 9-25).

Managing CA Certificates

To view and upload trusted certificates:

Select **VPN** > **Certificates** from the menu. The Certificates screen displays. Figure 9-11 shows the top section of the screen with the trusted certificate information and some example certificates in the Trusted Certificates (CA Certificates) table.

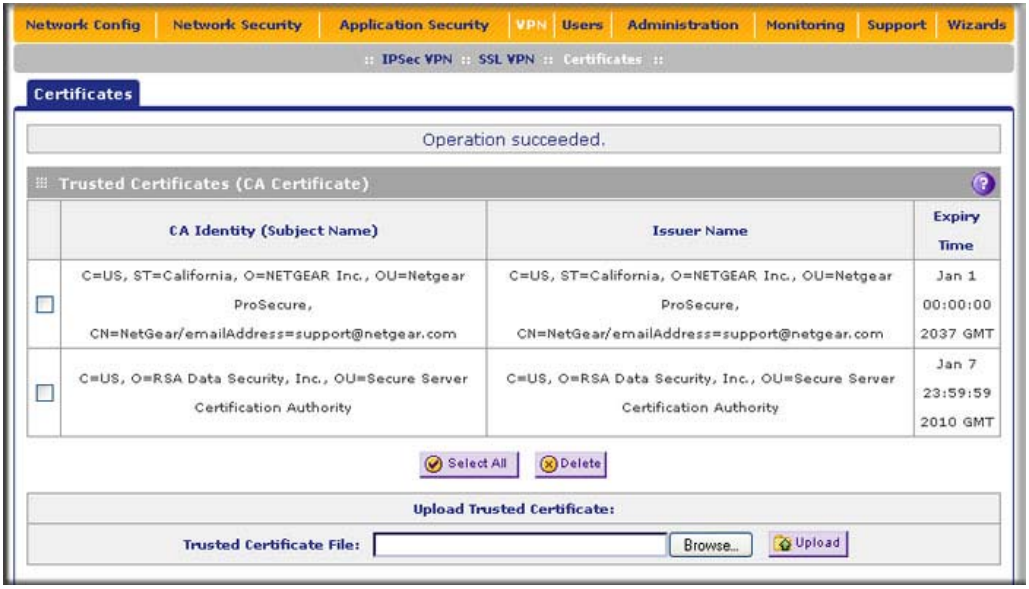


Figure 9-11 [Certificates, screen 1 of 3]

The Trusted Certificates (CA Certificates) 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 **Browse** 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 Certificates) table, select the checkbox to the left of the 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.

Managing Self Certificates

Instead of obtaining a digital certificate from a CA, you can generate and sign your own digital certificate. However, a self-signed digital certificate triggers a warning from most browsers because it provides no protection against identity theft of the server. Figure 9-12 on page 9-21 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 9-12

Generating a CSR and Obtaining a Self Certificate from a CA

To use a self certificate, you must first request the digital certificate from a CA, and then download and activate the digital certificate on the UTM. To request a self certificate from a CA, you must 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 must 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** from the menu. The Certificates screen displays. Figure 9-13 on page 9-22 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.)

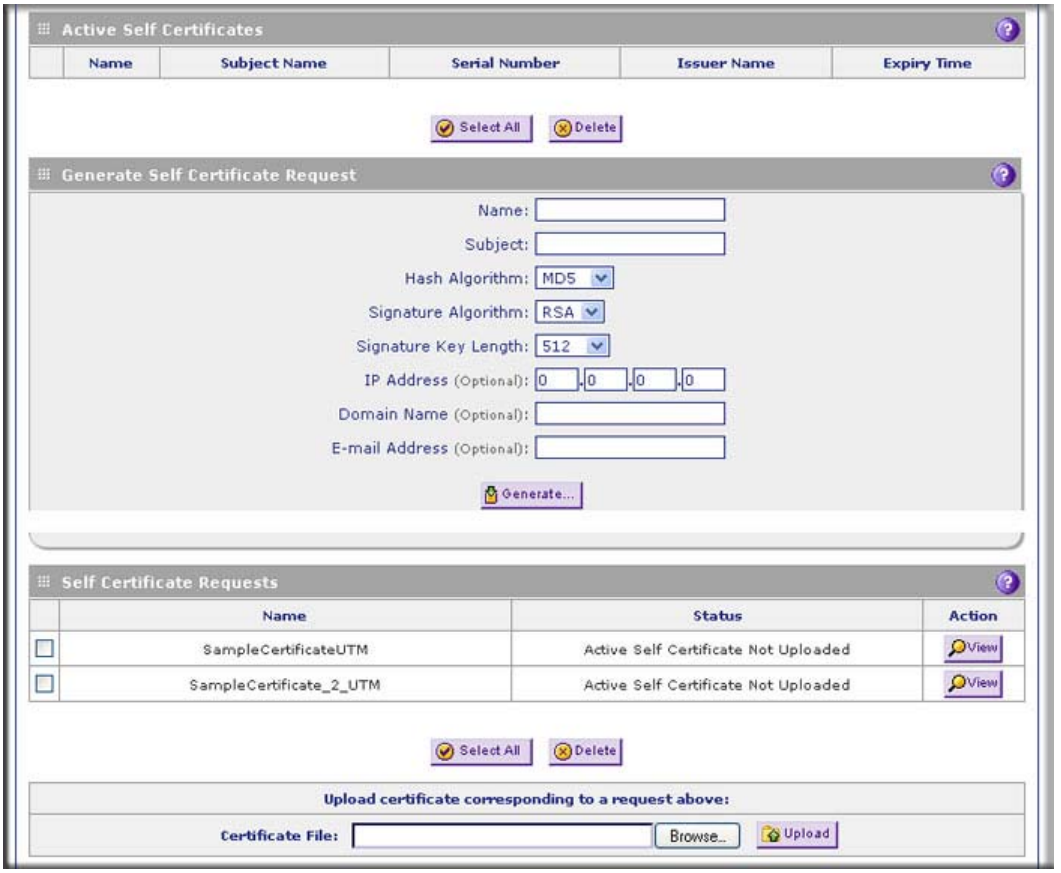


Figure 9-13 [Certificates, screen 2 of 3]

2. In the Generate Self Certificate Request section of the screen, enter the settings as explained in Table 9-7.

Table 9-7. Generate Self Certificate Request Settings

Setting	Description (or Subfield and 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.

Table 9-7. Generate Self Certificate Request Settings (continued)

Setting	Description (or Subfield and Description)	
Hash Algorithm	From the pull-down menu, 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 pull-down menu, the only possible selection is RSA. In other words, RSA is the default to generate a CSR.	
Signature Key Length	From the pull-down menu, 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 e-mail 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 (see Figure 9-14 on page 9-24).

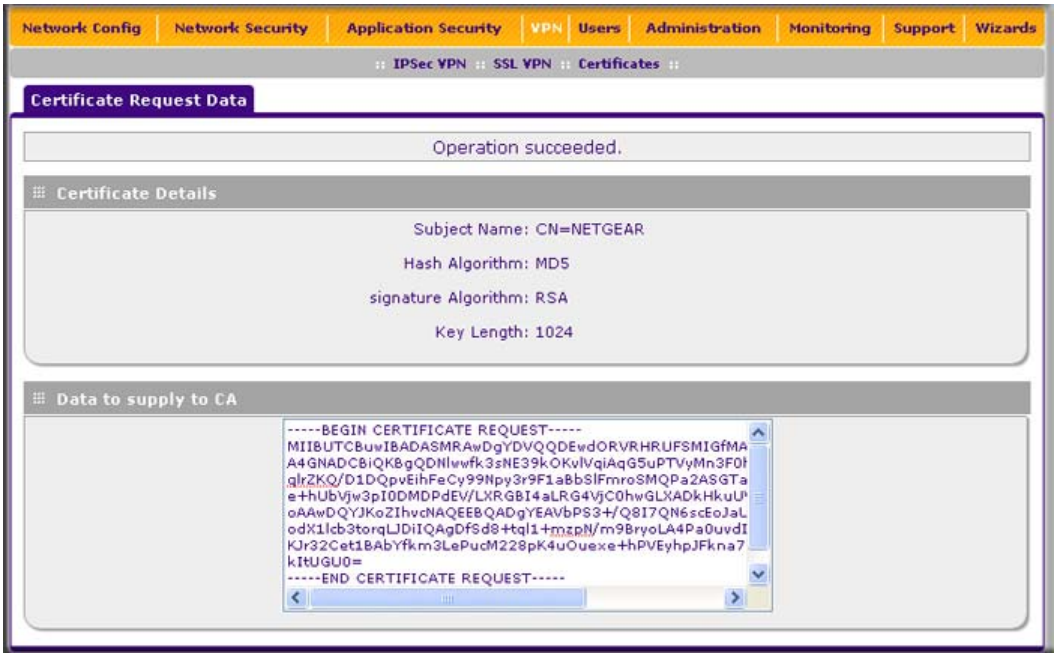


Figure 9-14

5. Copy the contents of the Data to supply to CA text box 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 9-13 on page 9-22) and locate the Self Certificate Requests section.
9. Select the checkbox next to the self certificate request.

10. Click **Browse** 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 checkbox to the left of the SCR that you want to delete or click the **Select All** table button to select all SCRs.
2. Click the **Delete** table button.

Viewing and Managing Self Certificates

The Active Self Certificates table on the Certificates screen (see Figure 9-13 on page 9-22) shows the digital certificates issued to you by a CA and available for use. For each self certificate, the table lists the following information:

- **Name**. The name that you used to identify this digital 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 digital certificate with in the CA.
- **Issuer Name**. The name of the CA that issued the digital certificate.
- **Expiry Time**. The date on which the digital certificate expires. You should renew the digital certificate before it expires.

To delete one or more self certificates:

1. In the Active Self Certificates table, select the checkbox to the left of the self certificate that you want to delete or click the **Select All** table button to select all self certificates.
2. Click the **Delete** table button.

Managing 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 their 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** from the menu. The Certificates screen displays. Figure 9-15 shows the bottom section of the screen with Certificate Revocation Lists (CRL) table. There are no examples in the table (that is, the table is empty).

Figure 9-15[Certificates, screen 3 of 3]

The Certificate Revocation Lists (CRL) table lists the active CAs and their critical release dates:

- **CA Identify**. 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 **Browse** 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 checkbox to the left of the CRL that you want to delete or click the **Select All** table button to select all CRLs.
2. Click the **Delete** table button.

Chapter 10
Network and System Management

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

Performance management consists of controlling the traffic through the UTM so that the necessary traffic gets through when there is a bottleneck and either reducing unnecessary traffic or rescheduling 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 dual-WAN port models):
  2000 Mbps (two LAN ports at 1000 Mbps each)
- WAN side:
  - Load balancing mode (dual-WAN port models only): 2000 Mbps (two WAN ports at 1000 Mbps each)
  - Auto-rollover mode (dual-WAN port models only): 1000 Mbps (one active WAN port at 1000 Mbps)
  - Single-WAN port mode (single-WAN port models and dual-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 (dual-WAN port models only): 3 Mbps (two WAN ports at 1.5 Mbps each)

- Auto-rollover mode (dual-WAN port models only): 1.5 Mbps (one active WAN port at 1.5 Mbps)
- Single-WAN port mode (single-WAN port models and dual-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 to throughput for most installations.

Using the dual 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 fail. When such as 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 only! Incorrect configuration might cause serious problems.

Each rule lets you specify the desired action for the connections that re covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise allow
- ALLOW always

- ALLOW by schedule, otherwise block

The section below 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 5-4. For detailed procedures on how to configure outbound rules, see "Setting LAN WAN Rules" on page 5-12 and "Setting DMZ WAN Rules" on page 5-15.

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 to be covered by an outbound rule. If the desired service or application does not appear in the list, you must define it using the Services screen (see "Services-Based Rules" on page 5-3 and "Adding Customized Services" on page 5-32).
- **LAN Users**. You can specify which computers on your network are affected by an outbound rule. There are several options:
  - **Any**. All PCs and devices on your LAN.
  - **Single address**. The rule is applied to the address of a particular PC.
  - **Address range**. The rule is applied 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 "Managing the Network Database" on page 4-13. PCs and network devices are entered into the Network Database by various methods that are described in "Managing Groups and Hosts (LAN Groups)" on page 4-12.
- **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 is applied to a range of Internet IP addresses.
- **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 "Setting a Schedule to Block or Allow Specific Traffic" on page 5-41.

- **QoS Profile**. You can define QoS profiles and then apply them to outbound rules to regulate the priority of traffic. To define QoS profiles, see "Creating Quality of Service (QoS) Profiles" on page 5-35.
- **Bandwidth Profile**. You can define bandwidth profiles and then apply them to outbound rules to limit traffic. To define bandwidth profiles, see "Creating Bandwidth Profiles" on page 5-38.

Content Filtering

If you want to reduce traffic by preventing undesired e-mails 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 Web site is allowed with the exception of Web content categories that are mentioned in "Default E-mail and Web Scan Settings" on page 6-2.

- **E-mail Content Filtering**. To reduce incoming e-mail traffic, you can block e-mails with large attachments, reject e-mails based on keywords, file extensions, or file names, and set spam protection rules. There are several ways you can reduce undesired e-mail traffic:
  - **Setting the size of e-mail files to be scanned**. Scanning large e-mail files requires network resources and might slow down traffic. You can specify the maximum file or message size that is scanned, and if files that exceed the maximum size are skipped (which might compromise security) or blocked. For more information, see "Customizing E-mail Anti-Virus and Notification Settings" on page 6-5.
  - **Keyword, file extension, and file name blocking**. You can reject e-mails based on keywords in the subject line, file type of the attachment, and file name of the attachment. For more information, see "E-mail Content Filtering" on page 6-8.
  - **Protecting against spam**. Set up spam protection to prevent spam from using up valuable bandwidth. For more information, see "Protecting Against E-mail Spam" on page 6-11.
- **Web Content Filtering**. The UTM provides extensive methods to filtering 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 "Configuring Web Content Filtering" on page 6-23.
  - **Keyword and file extension blocking**. You can specify words that, should they appear in the Web site name (URL), file extension, or newsgroup name, cause that site, file, or newsgroup to be blocked by the UTM. For more information, see "Configuring Web Content Filtering" on page 6-23.

- **URL blocking**. You can specify up to 200 URLs that are blocked by the UTM. For more information, see "Configuring Web URL Filtering" on page 6-30.
- **Web services blocking**. You can block Web services such as instant messaging and peer-to-peer services. For more information, see "Customizing Web Protocol Scan Settings and Services" on page 6-19.
- **Web object blocking**. You can block the following Web component types: embedded objects (ActiveX, Java, Flash), proxies, and cookies, and you can disable Java scripts. For more information, see "Configuring Web Content Filtering" on page 6-23.
- **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 file size that is scanned, and if files that exceed the maximum size are skipped (which might compromise security) or blocked. For more information, see "Configuring Web Malware Scans" on page 6-21.

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 "Configuring Web Content Filtering" on page 6-23) and configure exceptions for groups (see "Setting Web Access Exception Rules" on page 6-41).

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 "Enabling Source MAC Filtering" on page 5-42 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 only! 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 section below 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 5-6. For detailed procedures on how to configure inbound rules, see “Setting LAN WAN Rules” on page 5-12 and “Setting DMZ WAN Rules” on page 5-15.

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 to be covered by an inbound rule. If the desired service or application does not appear in the list, you must define it using the Services screen (see “Services-Based Rules” on page 5-3 and “Adding Customized Services” on page 5-32).
- **WAN Destination IP Address**. For the dual-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 (that is WAN1 or WAN2 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**. All PCs and devices on your LAN.
  - **Single address**. The rule is applied to the address of a particular PC.

  - **Address range**. The rule is applied 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 "Managing the Network Database" on page 4-13. PCs and network devices are entered into the Network Database by various methods that are described in "Managing Groups and Hosts (LAN Groups)" on page 4-12.

- **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 is applied to a range of Internet IP addresses.
- **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 "Setting a Schedule to Block or Allow Specific Traffic" on page 5-41.
- **QoS Profile**. You can define QoS profiles and then apply them to inbound rules to regulate the priority of traffic. To define QoS profiles, see "Creating Quality of Service (QoS) Profiles" on page 5-35.
- **Bandwidth Profile**. You can define bandwidth profiles and then apply them to inbound rules to limit traffic. To define bandwidth profiles, see "Creating Bandwidth Profiles" on page 5-38.

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 this 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 requests 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 "Configuring Port Triggering" on page 5-46.

Configuring the DMZ Port

The De-Militarized 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

e-mail server) and provide public access to them. The fourth LAN port on the UTM (the rightmost LAN port) can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN. 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 the information on how to enable the DMZ port, see "Configuring and Enabling the DMZ Port" on page 4-18. For the procedures on how to configure DMZ traffic rules, see "Setting DMZ WAN Rules" on page 5-15.

Configuring 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 on how to set up an exposed host, see "LAN WAN or DMZ WAN Inbound Rule: Specifying an Exposed Host" on page 5-25.

Configuring VPN Tunnels

The UTM supports up to 25 site-to-site IPsec VPN tunnels and up to 13 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."

Using QoS and Bandwidth Assignment 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.

Assigning 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 “Creating Quality of Service (QoS) Profiles” on page 5-35.

Assigning Bandwidth Profiles

By applying 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 “Creating Bandwidth Profiles” on page 5-38.

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 “Monitoring System Access and Performance” on page 11-1 for a description of these tools.

System Management

System management tasks are described in the following sections:

Changing Passwords and Administrator Settings

The default administrator and default guest passwords for the Web Management Interface are both **password**. NETGEAR recommends that you change these passwords to more secure passwords. You can also configure a separate password for the guest account.

To modify the administrator user account settings, including the password:

1. Select **Users** > **Users** from the menu. The Users screen displays. Figure 10-1 shows the UTM's default users—admin and guest—and, as an example, several other users in the List of Users table.

Figure 10-1

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.

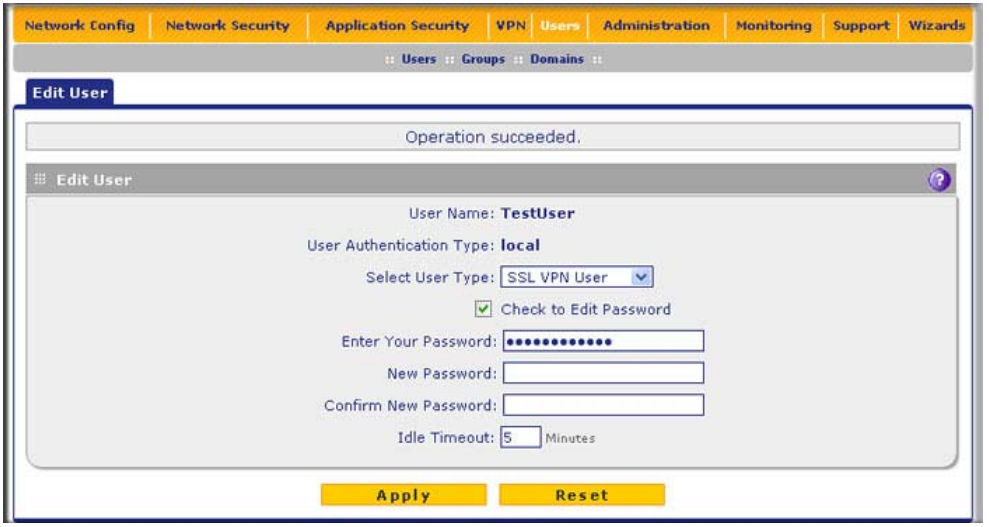


Figure 10-2

3. Select the **Check to Edit Password** checkbox. The password fields become active.
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 upper and lower case), numbers, and symbols. Your password can be up to 30 characters.

5. As an option, you can change the idle timeout 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 default reset, the password and timeout 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 “Setting User Login Policies” on page 9-12.

Configuring Remote Management Access

An administrator can configure, upgrade, and check the status of the UTM over the Internet via a Secure Sockets Layer (SSL) VPN connection.

Note: When remote management is enabled and administrative access through a WAN interface is granted (see "Configuring Login Policies" on page 9-12), 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 "Changing Passwords and Administrator Settings" on page 10-9).

To configure the UTM for remote management:

1. Select **Administration** > **Remote Management** from the menu The Remote Management screen displays.

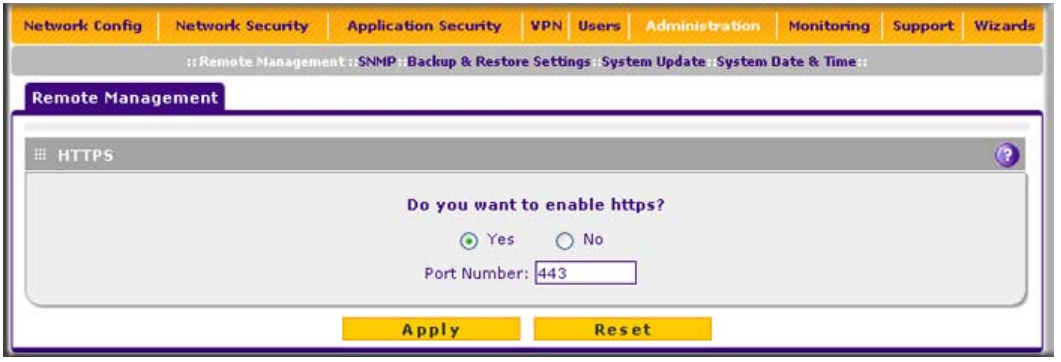


Figure 10-3

2. Select one of the following radio buttons:
   - **Yes**. Enable HTTPS remote management. This is the default setting.
   - **No**. Disable HTTPS remote management.

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 must use an SSL connection to access the UTM from the Internet. You must 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 172.16.0.123, type the following in your browser: **https://172.16.0.123**.

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 "Setting User Login Policies" on page 9-12 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 via 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 higher, 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 "Configuring Login Policies" on page 9-12).

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.

Using an SNMP 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** from the menu. The SNMP screen displays.

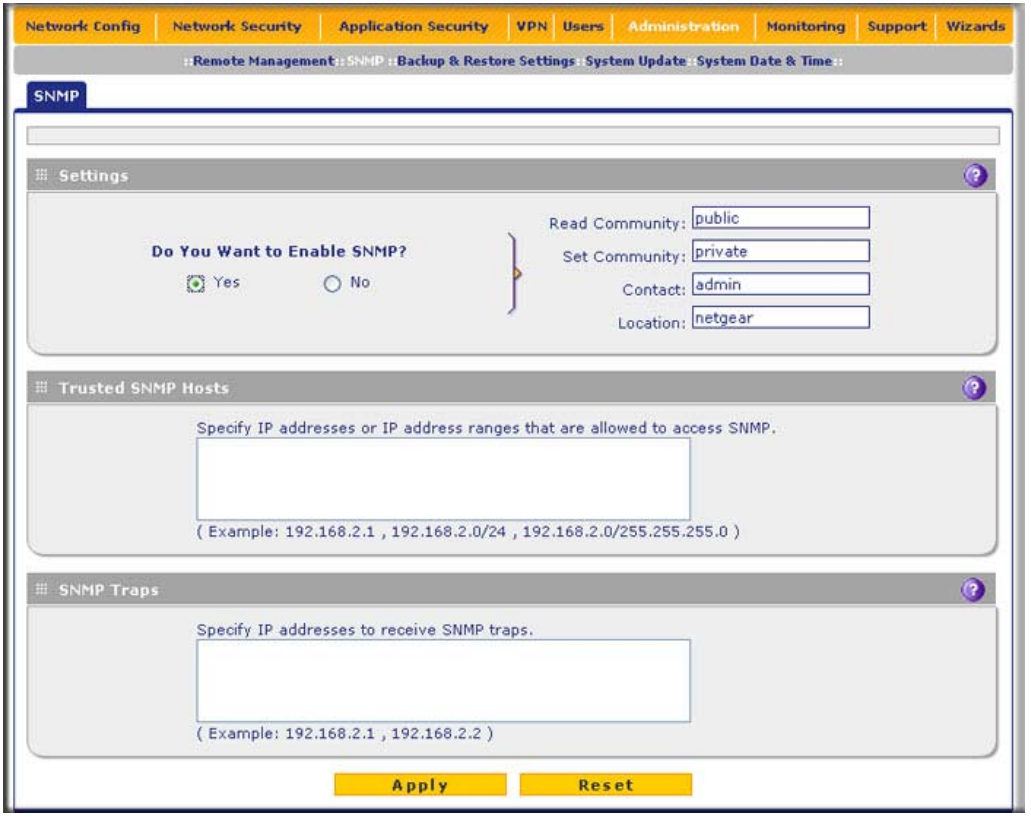


Figure 10-4

2. Enter the settings as explained in Table 10-1.

Table 10-1. SNMP Settings

Setting	Description (or Subfield and 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.
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.

Managing 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 properly, make a back-up 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** from the menu.

Figure 10-5

Backup 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.
- **Anti-spam setting**s. 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 backup settings:

1. On the Backup & Restore Settings screen (see Figure 10-5), next to Save a copy of current settings, click the **backup** button to save a copy of your current settings. A dialog screen appears, showing the file name of the backup file (backup.gpg).

2. Select **Save file**, and then click **OK**.
3. Open the folder where 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 you have your browser 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 Figure 10-5 on page 10-16), next to Restore save settings from file, click **Browse**.
2. Locate and select the previously saved backup file (by default, backup.pkg).
3. When you have located the file, click the **restore** button. A warning screen might appear, 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.

Reverting to Factory Default Settings

To reset the UTM to the original factory default settings, you can use one of the following two methods:

- Using a sharp object, press and hold the Reset button on the rear panel of the UTM (see "Rear Panel" on page 1-12) for about eight seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Reset button method.
- On the Backup & Restore Settings screen (see Figure 10-5 on page 10-16), next to Revert to factory default 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 push the hardware 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**.

Updating the Firmware

The UTM can automatically detect any new firmware version from NETGEAR. The firmware upgrade process for the UTM consists of the following stages that are explained in detail in the sections below:

1. Querying the available firmware versions.
2. Selecting a firmware version to download directly to the UTM (that is, not first to a computer and then to the UTM).
3. Installing the downloaded firmware version.
4. Rebooting the UTM with the new firmware version.

Viewing 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** from the menu. The System Update submenu tabs appear, with the Signatures & Engine screen in view.
2. Click the **Firmware** submenu tab. The Firmware screen displays.

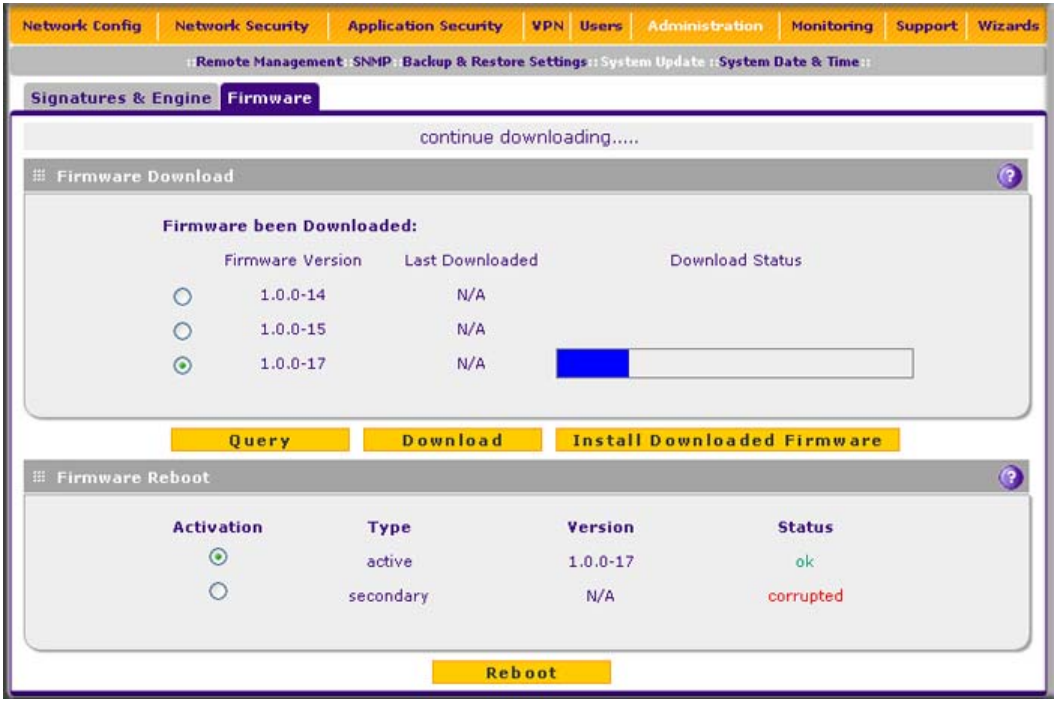


Figure 10-6

The Firmware Reboot section shows the following information fields for both the active and secondary (that is, non-active) firmware:

- **Type**. Active or secondary firmware.
- **Version**. The firmware version.
- **Status**. The status of the firmware (“ok” or “corrupted”).

3. 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.

Upgrading the Firmware and Rebooting the UTM

To upgrade the UTM's firmware and reboot the UTM:

1. In the Firmware Download section of the Firmware screen (see Figure 10-6 on page 10-19), 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.
4. When the firmware download process has completed, click **Install Downloaded Firmware**.
5. After the firmware installation process is complete, the newly installed firmware should be the secondary firmware and not the active firmware. Select the **Activation** radio button for he secondary firmware, that is, the newly installed firmware.
6. Click the **Reboot** button.

   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.

Warning: Once you start 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. After the UTM has rebooted, check the firmware version in Firmware Reboot section of the Firmware screen to verify that the UTM now has the new firmware installed: the newly loaded firmware should be shown as the active firmware and the Activation radio button should be automatically selected. The previously loaded firmware should be shown as the secondary firmware and the Activation radio button should be automatically deselected.

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.

Rebooting Without Changing the Firmware

To reboot the UTM without changing the firmware:

1. In the Firmware Reboot section of the Firmware screen (see Figure 10-6 on page 10-19), select the active firmware version by clicking the **Activation** radio button for the firmware that states “active” in the Type column.
2. Select the radio button that corresponds to the firmware version that you want to download onto the UTM.
3. 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.

Updating 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 as current as possible. 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** from the menu. The System Update submenu tabs appear, with the Signatures & Engine screen in view (see Figure 10-7 on page 10-22).

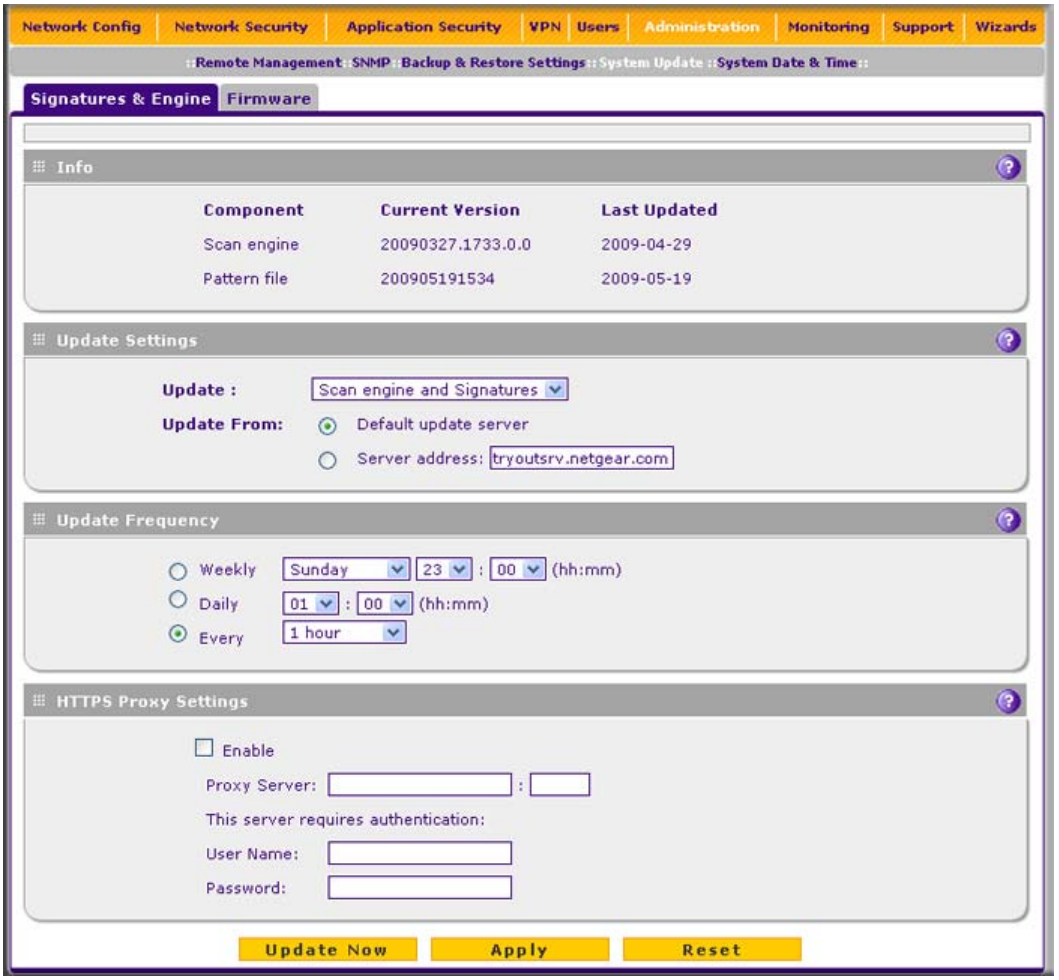


Figure 10-7

The Info section 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 **Update Now** at the bottom of the screen.

Configuring 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 section on the Signatures & Engine screen (see Figure 10-7 on page 10-22).
2. Enter the settings as explained in Table 10-2.

Table 10-2. Signatures & Scan Engine Settings

Setting	Description (or Subfield and Description)	
Update Settings		
Update	From the pull-down menu, 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 Update Frequency settings below.	
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.	
Update Frequency		
Specify the frequency with which the UTM checks for file updates: • **Weekly**. From the pull-down menus, select the weekday, hour, and minutes that the updates occur. • **Daily**. From the pull-down menus, select the hour, and minutes that the updates occur. • **Every**. From the pull-down menu, 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 via a proxy server, select the **Enable** checkbox to specify and enable a proxy server and 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.

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

Configuring 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** from the menu. The System Date & Time screen displays.

Figure 10-8

The bottom of the screen displays the current weekday, date, time, time zone, and year (in the example in Figure 10-8: Current Time: Thu May 21 01:37:18 GMT 2009).

2. Enter the settings as explained in Table 10-2.

Table 10-3. System Date & Time Settings

Setting	Description (or Subfield and Description)
Date/Time	From the pull-down menu, select the local time zone in which the UTM operates. The proper time zone is required in order for scheduling to work correctly. The UTM includes a real-time clock (RTC), which it uses for scheduling.

Table 10-3. System Date & Time Settings (continued)

Setting	Description (or Subfield and Description)	
Automatically Adjust for Daylight Savings Time	If daylight savings time is supported in your region, select the **Automatically Adjust for Daylight Savings Time** checkbox.	
NTP Server (default or custom)	From the pull-down menu, 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 must specify in the fields that become available with this menu 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://ntp.isc.org/bin/view/Servers/WebHome*.	
	Server 1 Name / IP Address	Enter the IP address or host name the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name 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. You must configure a DNS server address in the Network menu before the UTM can perform this lookup.

Chapter 11
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.

Note: All log and report functions that are part of the Logs & Reports configuration menu and some of the functions that are part of the Diagnostics configuration menu require that you configure the e-mail notification server—see "Configuring the E-mail Notification Server" on page 11-5.

This chapter contains the following sections:

Enabling 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 both WAN ports.

To monitor traffic limits on each of the WAN ports:

1. Select **Network Config** > **WAN Metering** from the menu. On the dual-WAN port models, the WAN Metering tabs appear, with the WAN1 Traffic Meter screen in view (see Figure 11-1 on page 11-2). On the 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 via the WAN port. If you have not enabled the traffic meter, these statistics are not available.

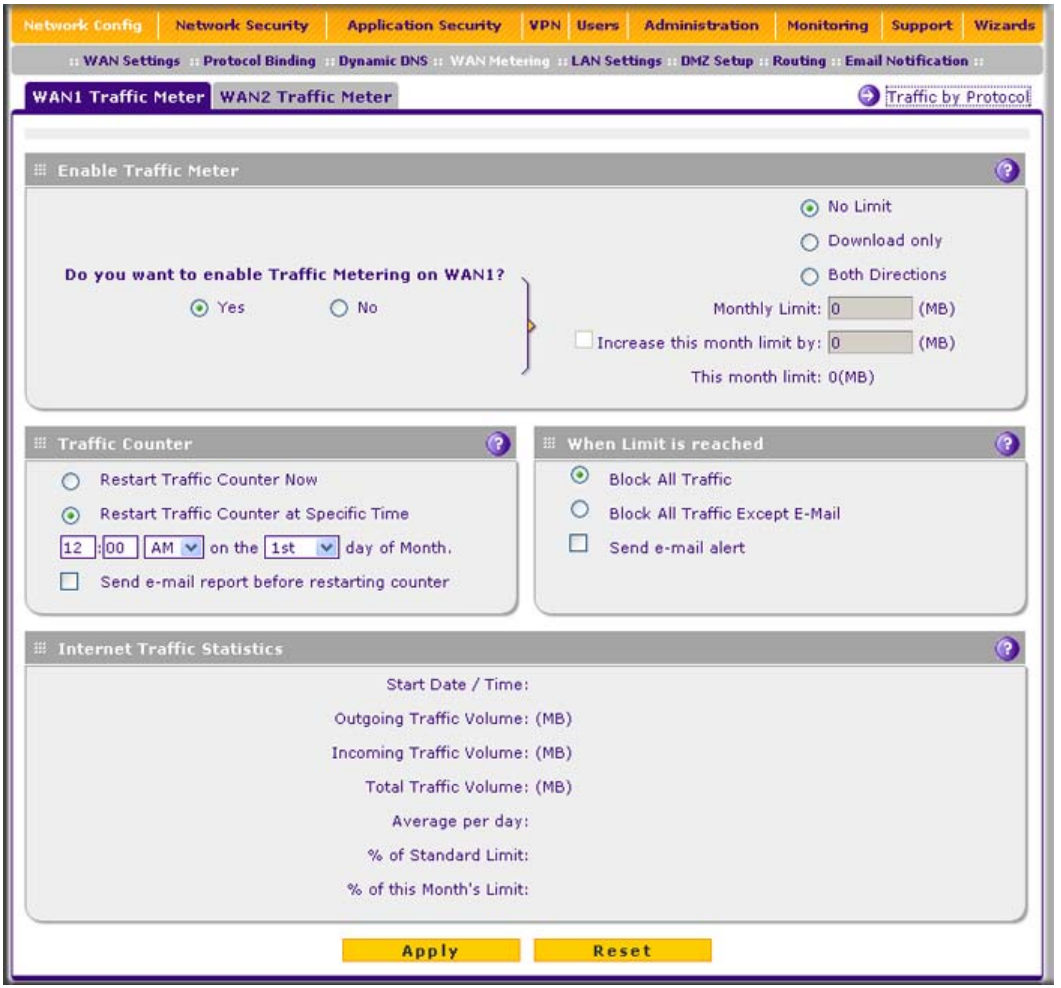


Figure 11-1

2. Enter the settings as explained in Table 11-1 on page 11-3.

Table 11-1. WAN Traffic Meter Settings

Setting	Description (or Subfield and Description)	
Enable Traffic Meter		
Do you want to enable Traffic Metering on WAN1? (dual-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 (dual-WAN port models) or WAN interface (single-WAN port models). Complete the fields below (on the screen, these fields are presented on the right). • **No**. Traffic metering is disabled. This is the default setting.	
	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. Complete the monthly limit field below. • **Both Directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached. Complete the monthly limit field below.	
	Monthly Limit	Enter the monthly traffic volume limit in MB. The default setting is 0 MB.
	Increase this month limit by	Select this checkbox 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 non-configurable 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.
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 choose AM or PM and the day of the month from the pull-down menus.	
Send e-mail report before restarting counter	An e-mail report is sent immediately before restarting the counter. Ensure that e-mailing of logs is enabled on the Email and Syslog screen (see “Configuring Logging, Alerts, and Event Notifications” on page 11-5).	

Table 11-1. WAN Traffic Meter Settings (continued)

Setting	Description (or Subfield and Description)
When Limit is reached	
Block traffic	Select one of the following radio buttons to specify what action the UTM performs when the traffic limit has been reached: • **Block All Traffic**. All incoming and outgoing Internet and e-mail traffic is blocked. • **Block All Traffic Except E-Mail**. All incoming and outgoing Internet traffic is blocked but incoming and outgoing e-mail traffic is still allowed.
Send e-mail alert	An e-mail alert is sent when traffic is blocked. Ensure that e-mailing of logs is enabled on the Email and Syslog screen (see "Configuring and Activating System, E-mail, and Syslog Logs" on page 11-6).

3. Click **Apply** to save your settings.
4. For the dual-WAN port models only, click the **WAN2 Traffic Meter** submenu tab. The WAN2 Traffic Meter screen displays. This screen is identical to the WAN1 Traffic Meter screen (see Figure 11-1 on page 11-2).
5. For the dual-WAN port models only, repeat step 2 and step 3 for the WAN2 interface.

To display a report of the Internet traffic by type, click the **Traffic by Protocol** option arrow at the top right of the WAN1 Traffic Meter or WAN2 Traffic Meter screen (dual-WAN port models), or at the top right of the WAN Traffic Meter screen (single-WAN port models). The Traffic by Protocol screen appears in a popup window. The incoming and outgoing volume of traffic for each protocol and the total volume of traffic is displayed. Traffic counters are updated in MBs; the counter starts only when traffic passed is at least 1 MB. In addition, the popup screen displays the traffic meter's start end dates.

Figure 11-2

Configuring 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 e-mail content, spam attempts, and many other types of events. You can configure the UTM to e-mail logs and alerts to a specified e-mail address.

To receive the logs in an e-mail message, the UTM's e-mail notification server must be configured and e-mail notification must be enabled. If the e-mail notification server is not configured or e-mail 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.

For more information about logs, see "Querying Logs and Generating Reports" on page 11-32.

Configuring the E-mail Notification Server

The UTM can automatically send information such as notifications and reports to the administrator. You must configure the necessary information for sending e mail, such as the administrator's e-mail address, the e-mail server, user name, and password.

To configure the e-mail notification server:

1. Select **Network Config** > **Email Notification** from the menu. The Email Notification screen displays (Figure 11-3 shows some examples).

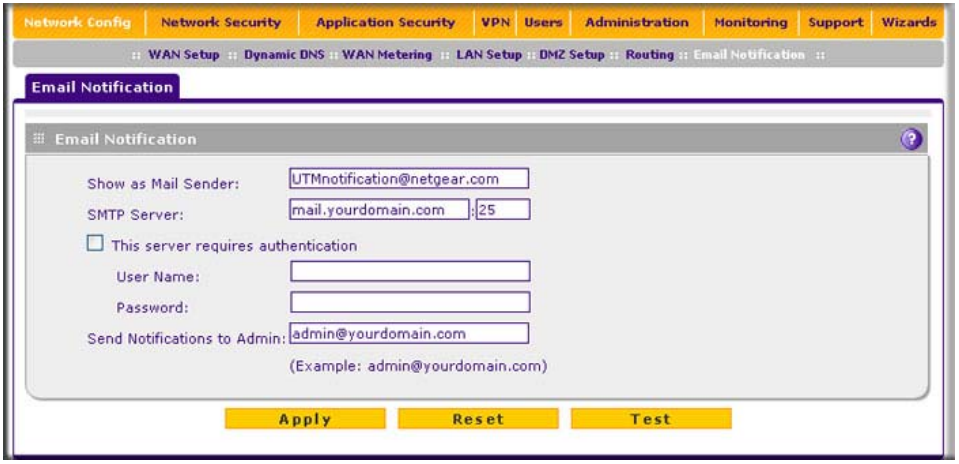


Figure 11-3

2. Enter the settings as explained in Table 11-2.

Table 11-2. E-mail Notification Settings

Setting	Description (or Subfield and Description)	
Show as mail sender	A descriptive name of the sender for e-mail 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 e-mail SMTP server. The default port number is 25. **Note**: If you leave this field blank, the UTM cannot send e-mail notifications.	
This server requires authentication	If the SMTP server requires authentication, select the **This server requires authentication** checkbox and enter the following settings:	
	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 e-mail address of the administrator.	

3. Click **Test** to ensure that the connection to the server and e-mail address succeeds.
4. Click **Apply** to save your settings.

Configuring and Activating System, E-mail, 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** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view (see Figure 11-4 on page 11-7).

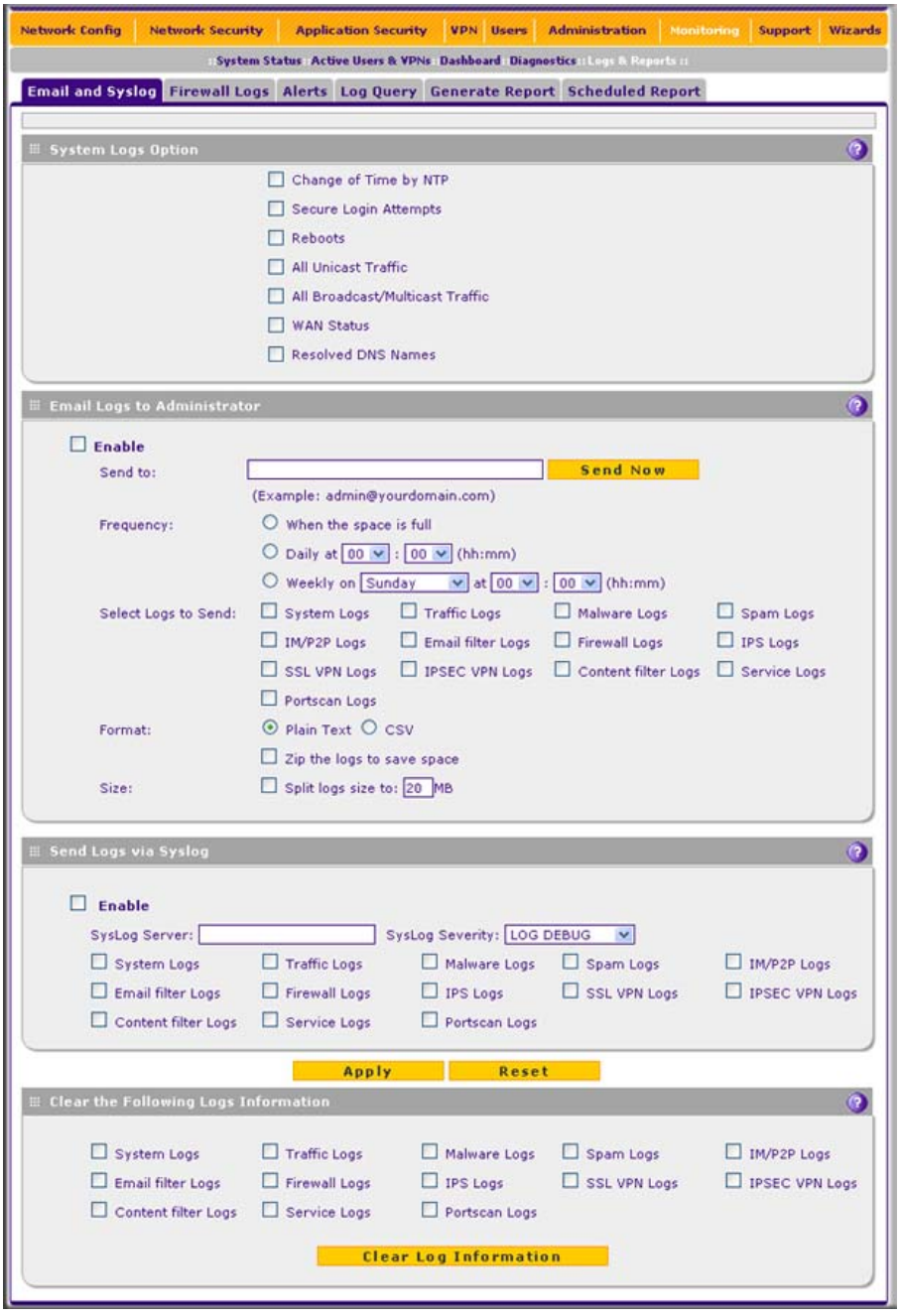

Network Config
Network Security
Application Security
VPN
Users
Administration
Monitoring
Support
Wizards
System Status
Active Users & VPNs
Dashboard
Diagnostics
Logs & Reports
Email and Syslog
Firewall Logs
Alerts
Log Query
Generate Report
Scheduled Report
System Logs Option
Change of Time by NTP
Secure Login Attempts
Reboots
All Unicast Traffic
All Broadcast/Multicast Traffic
WAN Status
Resolved DNS Names
Email Logs to Administrator
Enable
Send to:
Send Now
(Example: admin@yourdomain.com)
Frequency:
When the space is full
Daily at 00 : 00 (hh:mm)
Weekly on Sunday at 00 : 00 (hh:mm)
Select Logs to Send:
System Logs
Traffic Logs
Malware Logs
Spam Logs
IM/P2P Logs
Email filter Logs
Firewall Logs
IPS Logs
SSL VPN Logs
IPSEC VPN Logs
Content filter Logs
Service Logs
Portscan Logs
Format:
Plain Text
CSV
Zip the logs to save space
Size:
Split logs size to: 20 MB
Send Logs via Syslog
Enable
SysLog Server:
SysLog Severity: LOG DEBUG
System Logs
Traffic Logs
Malware Logs
Spam Logs
IM/P2P Logs
Email filter Logs
Firewall Logs
IPS Logs
SSL VPN Logs
IPSEC VPN Logs
Content filter Logs
Service Logs
Portscan Logs
Apply
Reset
Clear the Following Logs Information
System Logs
Traffic Logs
Malware Logs
Spam Logs
IM/P2P Logs
Email filter Logs
Firewall Logs
IPS Logs
SSL VPN Logs
IPSEC VPN Logs
Content filter Logs
Service Logs
Portscan Logs
Clear Log Information

Figure 11-4

2. Enter the settings as explained in Table 11-2.

Table 11-3. E-mail and Syslog Settings

Setting	Description (or Subfield and Description)	
System Logs Option		
Select the checkboxes 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 Reset button has been pushed to reboot the UTM.) • **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		
Enable	Select this checkbox to enable the UTM to send a log file to an e-mail address.	
	Send to	The e-mail address of the recipient of the log file. Click **Send Now** to immediately send the logs that you first must have specified below.
	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. • **Daily**. Logs are sent daily at the time that you specify from the pull-down menus (hours and minutes). • **Weekly**. Logs are sent weekly at the day and time that you specify from the pull-down menus (weekday, hours, and minutes).
	Select Logs to Send	Select the checkboxes to specify which logs are sent via e-mail: • **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. • **IM/P2P Logs**. All instant messaging and peer-to-peer access violations. • **Email filter Logs**. All e-mails 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 "Configuring and Activating Firewall Logs" on page 11-13).

Table 11-3. E-mail and Syslog Settings (continued)

Setting	Description (or Subfield and 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 Web sites and URLs. • **Service Logs**. All events that are related to the status of scanning and filtering services that are part of 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** checkbox to enable the UTM to compress the log file.
	Size	Select the **Split logs size to** checkbox 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 checkbox to enable the UTM to send a log file to a syslog server.	
	SysLog Server	The IP address or name of the syslog server.
Enable (continued)	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: • **LOG EMERG**. The UTM is unusable. • **LOG ALERT**. An action must 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 checkboxes to specify which logs are sent via the syslog server. The “Select Logs to Send” part of the “Email Logs to Administrator” section of the screen (see above) lists the same checkboxes as the “Send Logs via Syslog” section of the screen.

Table 11-3. E-mail and Syslog Settings (continued)

Setting	Description (or Subfield and Description)
Clear the Following Logs Information	
Select the checkboxes to specify which logs are cleared. The “Select Logs to Send” part of the “Email Logs to Administrator” section of the screen (see above) lists the same checkboxes as the “Clear the Following Logs Information” section of the screen.	

3. Click **Apply** to save your settings or click **Clear Log Information** to clear the selected logs.

Configuring and Activating Update Failure and Attack Alerts

You can configure the UTM to send an e-mail alert when a failure, malware (outbreak) attack, or Intrusion Prevention System (IPS) (outbreak) attack occurs. Five types of alerts 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.
- **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 e-mail alerts:

1. Select **Monitoring** > **Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Alerts** submenu tab. The Alerts screen displays (Figure 11-5 on page 11-11).

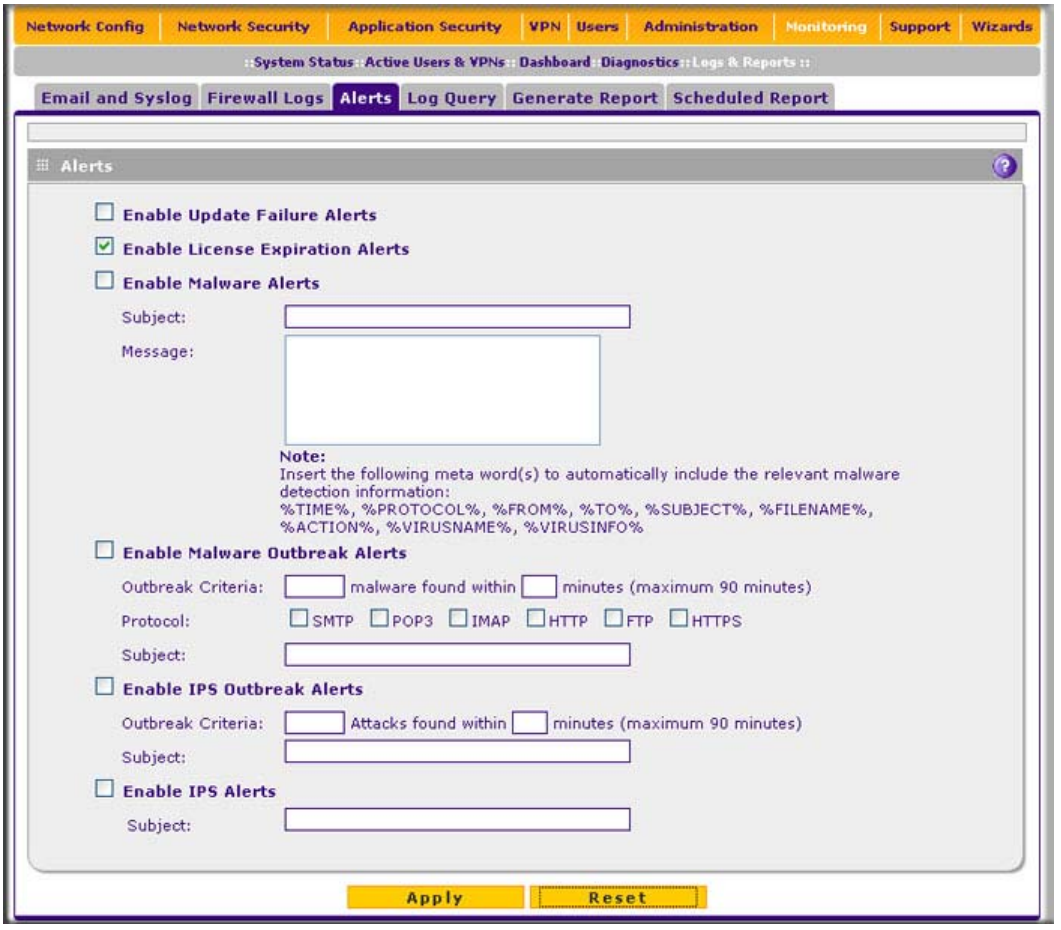


Figure 11-5

3. Enter the settings as explained in Table 11-4.

Table 11-4. Alerts Settings

Setting	Description (or Subfield and Description)
Enable Update Failure Alerts	Select this checkbox to enable update failure alerts.
Enable License Expiration Alerts	Select this checkbox to enable license expiration alerts. This checkbox is enabled by default.
Enable Malware Alerts	Select this checkbox to enable malware alerts, and configure the Subject and Message fields.

Table 11-4. Alerts Settings (continued)

Setting	Description (or Subfield and Description)	
Enable Malware Alerts (continued)	Subject	Enter the subject line for the e-mail alert. The default text is “[Malware alert]”.
	Message	Enter the content for the e-mail alert. **Note**: Make sure that you keep the %VIRUSINFO% and %TIME% meta words in a message to enable the UTM to insert the proper malware name and time information. In addition to these meta word, you can insert the following meta words in your customized message: %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.
Enable Malware Outbreak Alerts	Select this checkbox to enable malware outbreak alerts, and configure the Outbreak Criteria, Protocol, and Subject fields.	
	Outbreak Criteria	To define a malware outbreak, specify 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 checkbox or checkboxes to specify the protocols (**SMTP**, **POP3**, **IMAP**, **HTTP**, **FTP**, and **HTTPS**) for which malware threats are detected.
	Subject	Enter the subject line for the e-mail alert. The default text is “[Outbreak alert]”.
Enable IPS Outbreak Alerts	Select this checkbox to enable malware outbreak alerts, and configure the Outbreak Criteria and Subject fields.	
	Outbreak Criteria	To define an IPS outbreak, specify 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 e-mail alert. The default text is “[Outbreak alert]”.
Enable IPS Alerts	Select this checkbox to enable IPS alerts, and configure the Subject field.	
	Subject	Enter the subject line for the e-mail alert. The default text is “[IPS alert]”.

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

Configuring and Activating 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 “Enabling Source MAC Filtering” on page 5-42), and packets that are dropped because the session limit (see “Setting Session Limits” on page 5-30), bandwidth limit (see “Creating Bandwidth Profiles” on page 5-38), 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** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Firewall Logs** submenu tab. The Firewall Logs screen displays (see Figure 11-6).

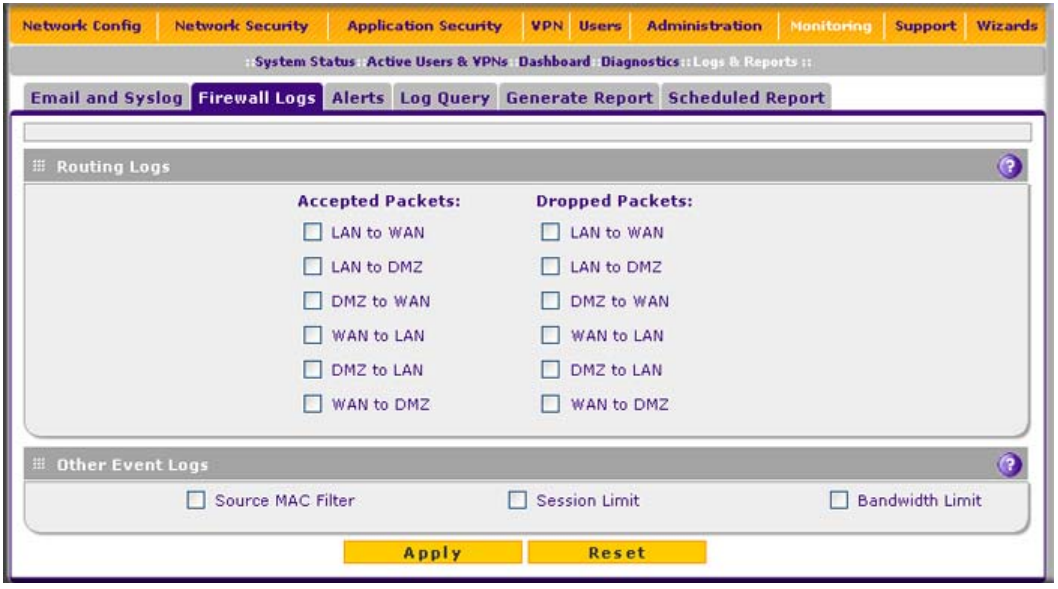


Figure 11-6

3. Enter the settings as explained in Table 11-5 on page 11-14.

Table 11-5. Firewall Logs Settings

Setting	Description (or Subfield and Description)
Routing Logs	
From the Accepted Packets and Dropped Packets columns, select checkboxes to specify which traffic is logged: • **LAN to WAN**. • **LAN to DMZ**. • **DMZ to WAN**. • **WAN to LAN**. • **DMZ to LAN**. • **WAN to DMZ**.	
Other Event Logs	
Source MAC Filter	Select this checkbox to log packets from MAC addresses that match the source MAC address filter settings.
Session Limit	Select this checkbox to log packets that are dropped because the session limit has been exceeded.
Bandwidth Limit	Select this checkbox to log packets that are dropped because the bandwidth limit has been exceeded.

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

Monitoring Real-Time Traffic, Security, and Statistics

When you start up the UTM, the default screen that displays is the Dashboard screen, which 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, instant messaging/peer-to-peer applications blocked, Web categories blocked, and spam e-mails blocked.

To display the Dashboard screen, select **Monitoring** > **Dashboard** from the menu. Because of the size of the Dashboard screen, it is divided and presented in this manual in three figures (Figure 11-7 on page 11-15, Figure 11-8 on page 11-17, and Figure 11-9 on page 11-19), 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 must be made on other screens.

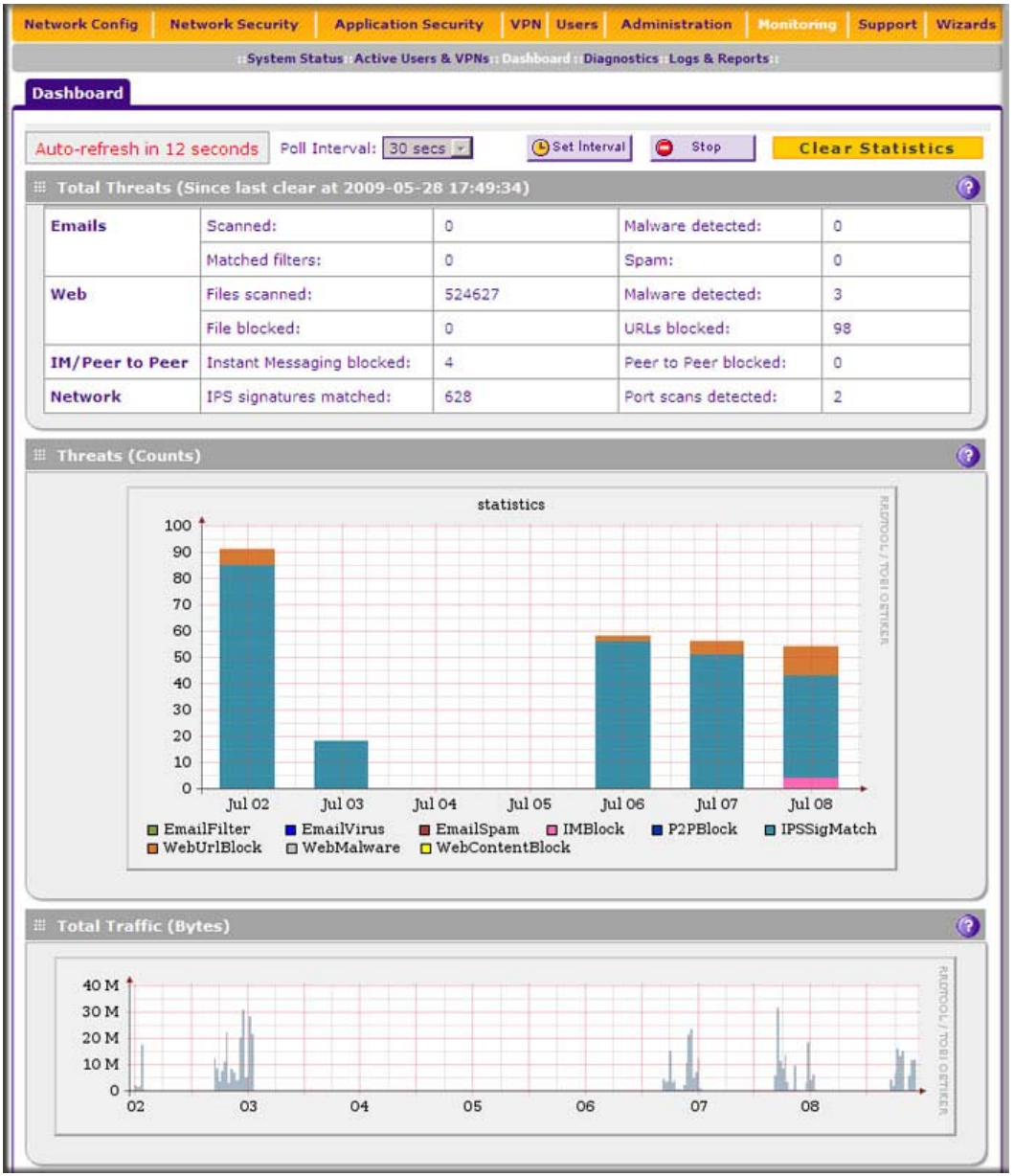


Figure 11-7 [Dashboard, screen 1 of 3]

To clear the statistics, click **Clear Statistics**.

To set the poll interval:

1. Click the **Stop** button.
2. From the Poll Interval pull-down menu, select a new interval (the minimum is 5 seconds, the maximum is 5 minutes).
3. Click the **Set Interval** button.

Table 11-6 explains the fields of the Total Threats, Threats (Counts), and Total Traffic (Bytes) sections of the Dashboard screen.

Table 11-6. Dashboard: Total Threats, Threats (Counts), and Total Traffic (Bytes) Information

Item	Description (or Subfield and Description)
Total Threats	
Emails	Displays the total number of: • Scanned e-mails. • Viruses detected (to configure, see "Customizing E-mail Anti-Virus and Notification Settings" on page 6-5). • E-mails that matched filters (to configure, see "E-mail Content Filtering" on page 6-8). • Spam (to configure, see "Protecting Against E-mail Spam" on page 6-11).
Web	Displays the total number of: • Files scanned. • Malware detected (to configure, see "Configuring Web Malware Scans" on page 6-21). • Files blocked (to configure, see "Configuring Web Content Filtering" on page 6-23). • URLs blocked (to configure, see "Configuring Web URL Filtering" on page 6-30).
IM/Peer to Peer	Displays the total number of: • Instant Messaging blocked (to configure, see "Customizing Web Protocol Scan Settings and Services" on page 6-19). • Peer to Peer blocked (to configure, see "Customizing Web Protocol Scan Settings and Services" on page 6-19).
Network	Displays the total number of: • IPS attack signatures matched (to configure, see "Using the Intrusion Prevention System" on page 5-49). • Port scans detected (to configure, see "Using the Intrusion Prevention System" on page 5-49).

Table 11-6. Dashboard: Total Threats, Threats (Counts), and Total Traffic (Bytes) Information (continued)

Item	Description (or Subfield and Description)
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 applications. **Note**: IMBlock stands for instant messaging applications blocked; P2PBlock stands for peer-to-peer applications blocked; IPSSisMatch stands for IPS signatures matched.	
Total Traffic (Bytes)	
This is a graphic that shows the relative number of traffic in bytes over the last week.	

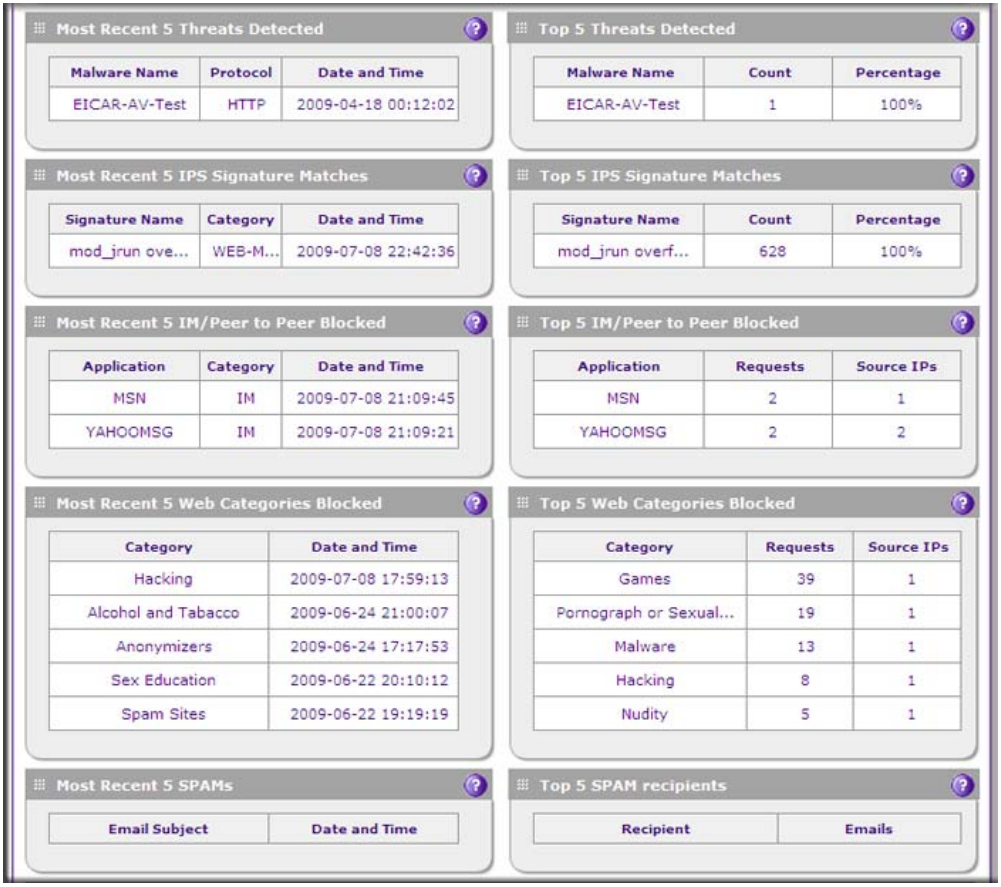


Figure 11-8 [Dashboard, screen 2 of 3]

Table 11-7 explains the fields of the Most Recent 5 and Top 5 sections of the Dashboard screen.

Table 11-7. Dashboard: Most Recent 5 and Top 5 Information

Category	Most Recent 5 Description	Top 5 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. **Note**: For more information about categories, see "Using the Intrusion Prevention System" on page 5-49. • **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.
IM/Peer to Peer	• **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. **Note**: For more information about Web categories, see "Configuring Web Content Filtering" on page 6-23. • **Date and Time**. The date and time that the Web request was blocked.	• **Category**. The Web category that was blocked. **Note**: For more information about Web categories, see "Configuring Web Content Filtering" on page 6-23. • **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 e-mail 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.

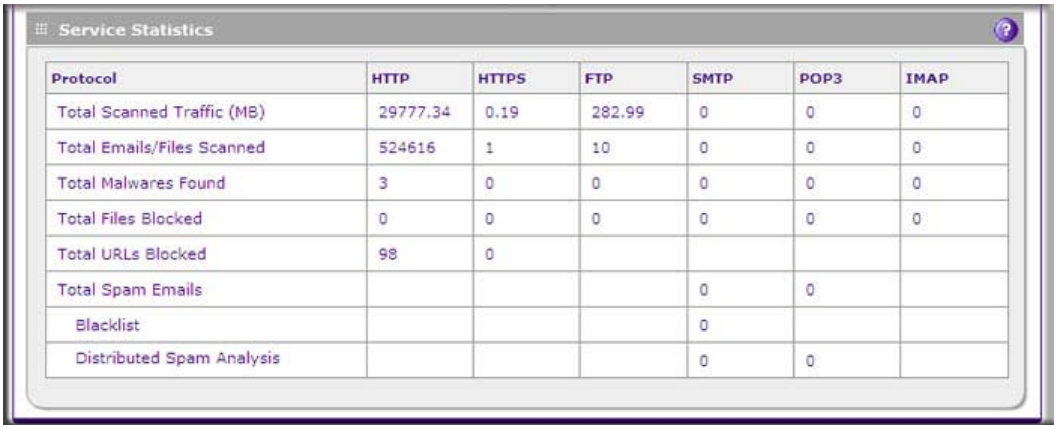


Figure 11-9 [Dashboard, screen 3 of 3]

Table 11-8 explains the fields of the Service Statistics section of the Dashboard screen.

Table 11-8. Dashboard: Service Statistics Information

Item	Description (or Subfield and 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 e-mails.
Total Malwares Found	The total number of detected viruses and attacks.
Total Files Blocked	The total number of downloaded files that were blocked.
Total URLs Blocked	The total number of URL requests that were blocked. These statistics are applicable only to HTTP and HTTPS.
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 e-mails that were detected from sources on the spam blacklist and Real-time blacklist (see “Setting Up the Whitelist and Blacklist” on page 6-12 and “Configuring the Real-time Blacklist” on page 6-14). These statistics are applicable only to SMTP.
Distributed Spam Analysis	The total number of spam messages that were detected through Distributed Spam Analysis (see “Configuring Distributed Spam Analysis” on page 6-16). These statistics are applicable only to SMTP and POP3.

Viewing Status Screens

The UTM provides real-time information in a variety of status screens that are described in the following sections:

Viewing System Status

The System Status screen provides real-time information about the following important components of the UTM:

- CPU, memory, and hard disk status, and the number of active connections per protocol.
- 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.

To view the System Status screen, click **Monitoring** > **System Status**. Because of the size of the System Status screen, it is divided and presented in this manual in three figures (Figure 11-10 on page 11-21, Figure 11-11 on page 11-22, and Figure 11-12 on page 11-23, all of which show examples for the dual-WAN port models), each with its own table that explains the fields. For the dual-WAN port models, the System Status screen shows information for both the WAN1 and WAN2 port. For the single-WAN port models, the System Status screen shows information for the single WAN port.

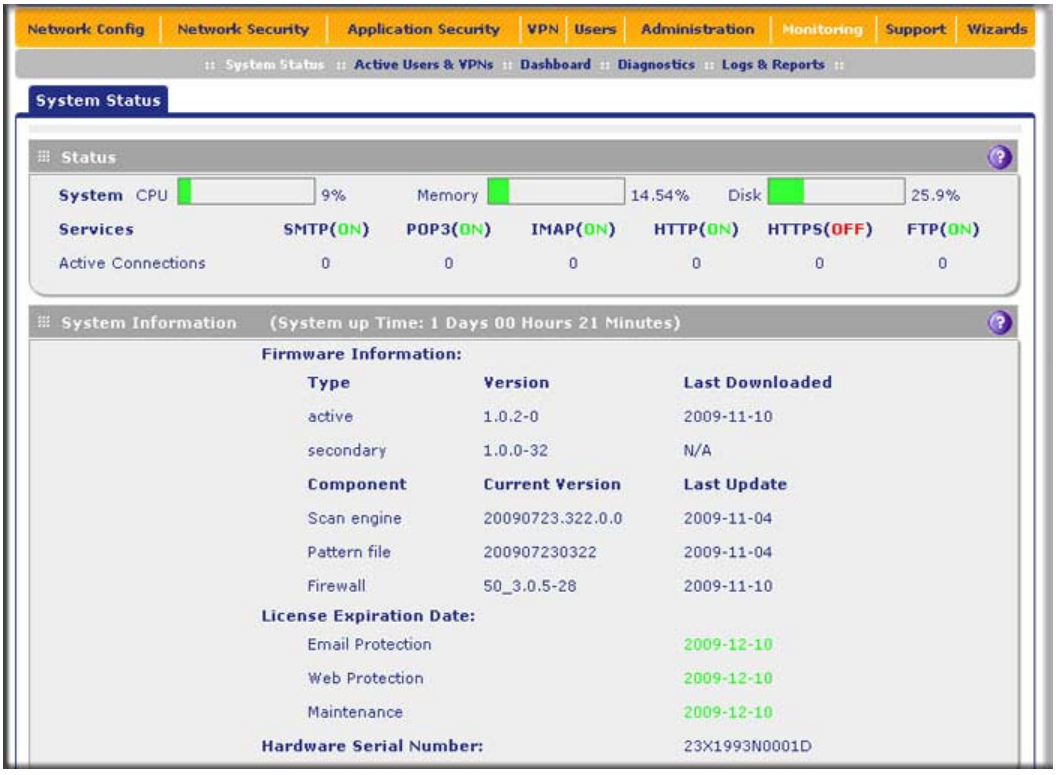


Figure 11-10 [System Status, screen 1 of 3]

Table 11-9 explains the fields of the Status and System Information sections of the System Status screen.

Table 11-9. System Status: Status and System Information

Setting	Description (or Subfield and Description)
Status	
System	The current CPU, memory, and hard disk usage. When usage is within safe limits, the status bars show green.
Services	The protocols that are being scanned for malware threats (ON or OFF stated next to the protocol) and the number of active connections for each protocol.

Table 11-9. System Status: Status and System Information (continued)

Setting	Description (or Subfield and Description)
System Information States system up time since last reboot.	
Firmware Information	The firmware version and most recent download for the active and secondary firmware of the UTM and for the scan engine, pattern file, and firewall.
License Expiration Date	The license expiration dates for the e-mail 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.

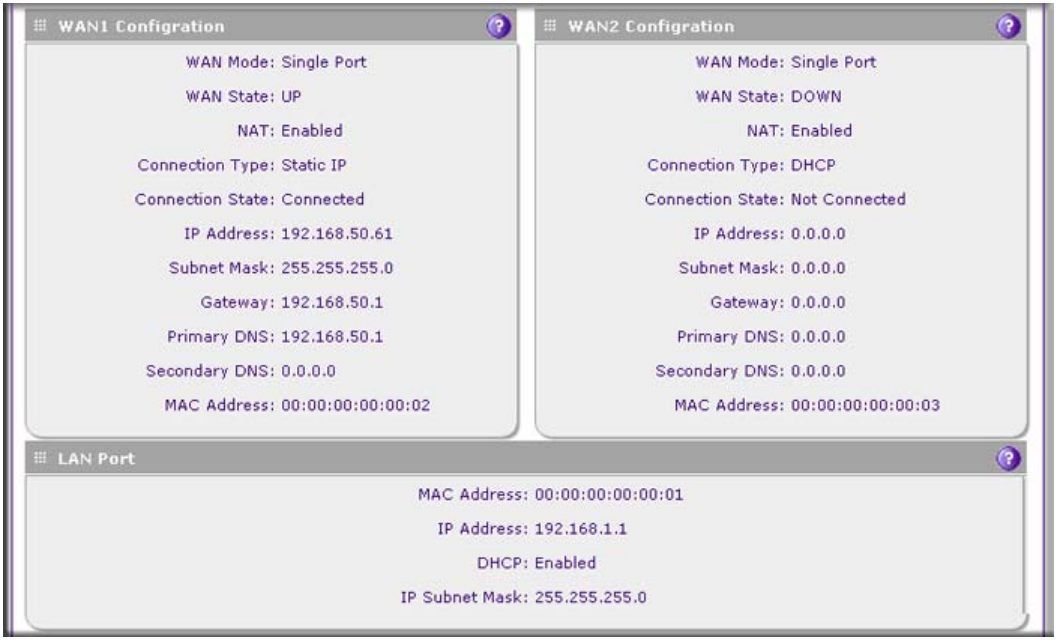


Figure 11-11 [System Status, screen 2 of 3]

Table 11-10 on page 11-23 explains the fields of the System Status screen of a dual-WAN port model with the WAN1 Configuration, WAN2 Configuration, and LAN Port sections. On the System Status screen for single-WAN port models, there is only a WAN Configuration and LAN Port section.

Table 11-10. System Status: WAN Configuration and LAN Port Information

Setting	Description (or Subfield and Description)
WAN1 Configuration/WAN2 Configuration (Dual-WAN Port Models) or WAN Configuration (Single-WAN Port Models)	
WAN Mode	Single Port, Load Balancing, or Auto Rollover.
WAN State	UP or DOWN.
NAT	Enabled or Disabled.
Connection Type	Static IP, DHCP, PPPoE, or PPTP.
Connection State	Connected or Not Connected.
IP Address	These fields are self-explanatory.
Subnet Mask	
Gateway	
Primary DNS	
Secondary DNS	
MAC Address	
LAN Port	
MAC Address	These fields are self-explanatory.
IP Address	
DHCP	DHCP or None.
IP Subnet Mask	This field is self-explanatory.

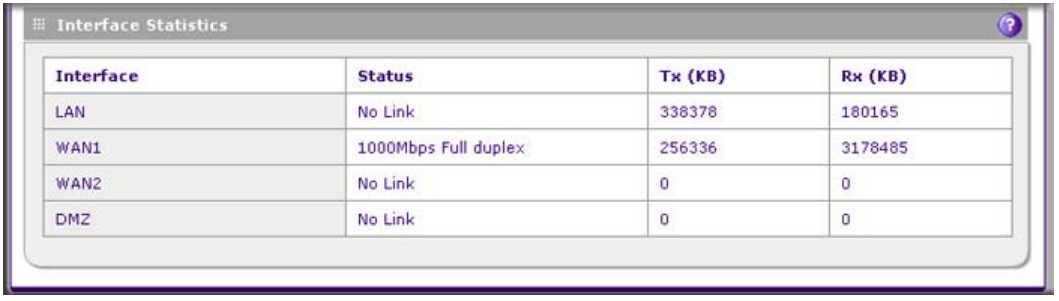


Figure 11-12 [System Status, screen 3 of 3]

Table 11-11 on page 11-24 explains the Interface Statistics section of the System Status screen.

Table 11-11. System Status: Interface Statistics

Setting	Description (or Subfield and Description)
For each interface (LAN, WAN1, WAN2, and DMZ for the dual-WAN port models; LAN, WAN, and DMZ for the single-WAN port models), the following statistics are displayed:	
Status	10BaseT Half duplex, 10BaseT Full duplex, 100BaseT Half duplex, 100BaseT Full duplex, or No Link.
Tx (KB)	The number of transmitted packets in KB.
Rx (KB)	The number of received packets in KB.

Viewing Active VPN Users

The Active Users screen displays a list of administrators, IPsec VPN, and SSL VPN users that are currently logged into the UTM.

To display the list of active VPN users:

Select **Monitoring > Active Users & VPNs** from the main menu. The Active Users & VPN submenu tabs appear, with the Active Users screen in views.

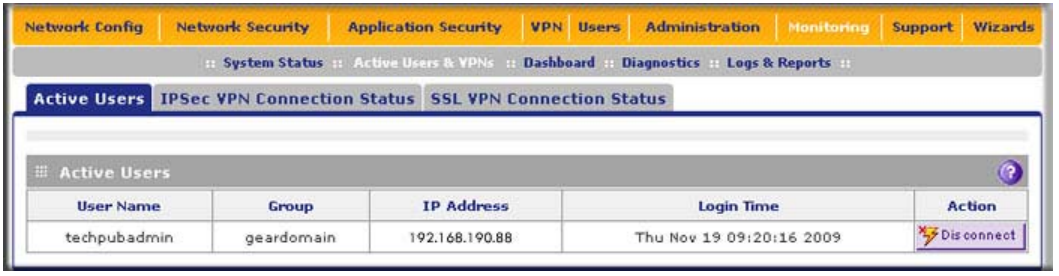


Figure 11-13

The active user's user name, group, and IP address are listed in the table with a timestamp 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.

Viewing VPN Tunnel Connection Status

To review the status of current IPsec VPN tunnels:

1. Select **Monitoring > Active Users & VPNs** from the main menu. The Active Users & VPN submenu tabs appear, with the Active Users screen in views

2. Click the **IPSec VPN Connection Status** submenu tab. The IPSec VPN Connection Status screen displays.

Figure 11-14

The Active IPsec SAs table lists each active connection with the information that is described in Table 11-12. 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 11-12. IPsec VPN Connection Status Information

Item	Description (or Subfield and 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 statu 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:

1. Select **Monitoring > Active Users & VPNs** from the main menu. The Active Users & VPN submenu tabs appear, with the Active Users screen in views

2. Click the **SSL VPN Connection Status** submenu tab. The SSL VPN Connection Status screen displays.

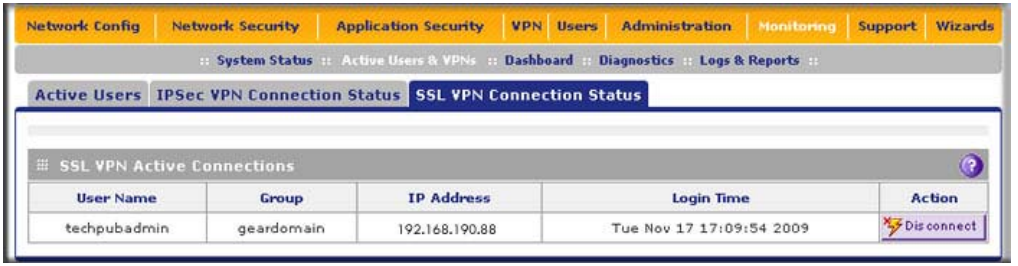


Figure 11-15

The active user's user name, group, and IP address are listed in the table with a timestamp 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.

Viewing Port Triggering Status

To view the status of the Port Triggering feature:

1. Select **Network Security** > **Port Triggering** from the menu. The Port Triggering screen displays (Figure 11-16 shows one rule in the Port Triggering Rules table as an example).

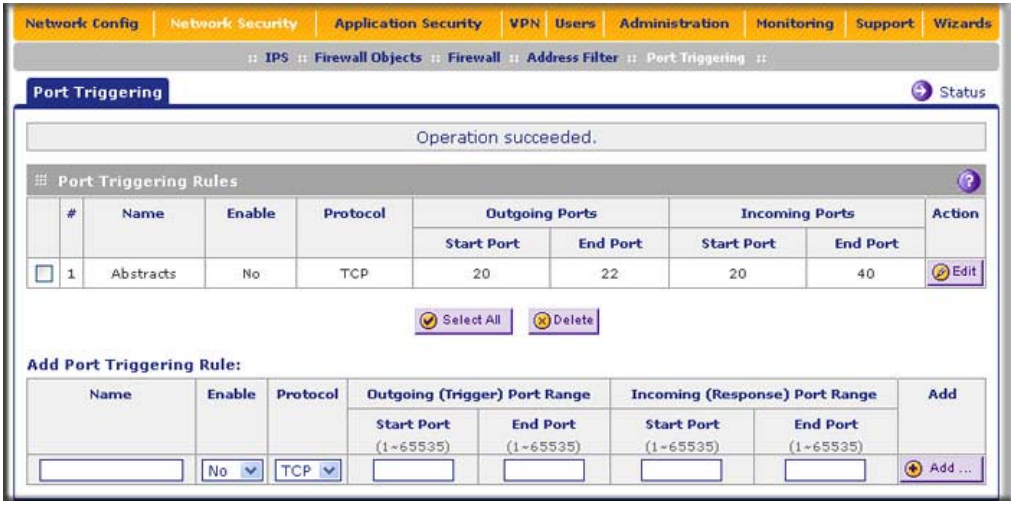


Figure 11-16

2. Click the **Status** option arrow at the top right of the Port Triggering screen.The Port Triggering Status screen appears in a popup window.

Figure 11-17

The Port Triggering Status screen displays the information that is described in Table 11-13.

Table 11-13. Port Triggering Status Information

Item	Description (or Subfield and 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.

Viewing 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 (dual-WAN port models) or WAN port (single-WAN port models):

1. Select **Network Config** > **WAN Settings** from the menu. On the dual-WAN port models, the WAN Settings submenu tabs appear, with the WAN1 ISP Settings screen in view (see Figure 11-18 on page 11-28). On the single-WAN port models, the WAN ISP Settings screen displays.

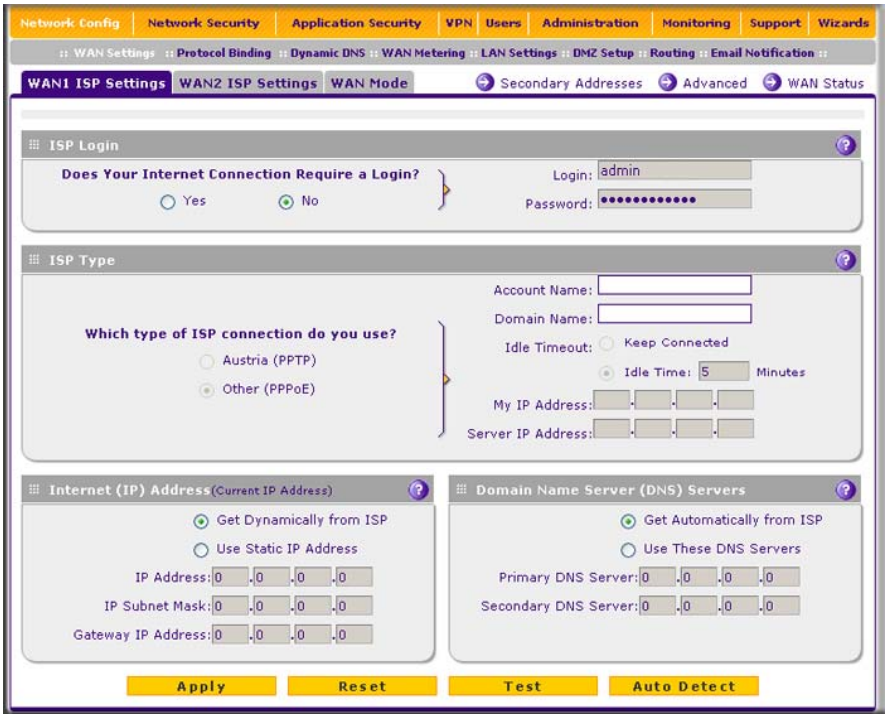


Figure 11-18

2. Click the **WAN Status** option arrow at the top right of the WAN1 ISP Settings screen (dual-WAN port models) or WAN1 ISP Settings screen (single-WAN port models). The Connection Status screen appears in a popup window.

Figure 11-19

The Connection Status screen displays the information that is described in Table 11-14.

Table 11-14. WAN1 (Dual-WAN Port Models) or WAN (Single WAN-Port Models) Port Status Informations

Item	Description (or Subfield and Description)
Connection Time	The period that the UTM has been connected through the WAN port.
Connection Type	DHCP or Static IP.
Connection Status	Connected or Disconnected.
IP Address	The addresses that were automatically detected (see "Automatically Detecting and Connecting" on page 3-2) or that you configured on the WAN1 ISP Settings screen (dual-WAN port models) or WAN ISP Settings screen (single-WAN port models) (see "Manually Configuring the Internet Connection" on page 3-5).
Subnet Mask	
Gateway	
DNS Server	
DHCP Server	The DHCP server that was automatically detected (see "Automatically Detecting and Connecting" on page 3-2) or that you configured for a VLAN profile on the Edit VLAN Profile screen (see "Configuring a VLAN Profile" on page 4-6).
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 may be displayed 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 dual-WAN port models only, the procedure to view the status of the WAN2 port is identical to the one for the WAN1 port with the exception that you must select the **WAN2 ISP Settings** submenu tab to display the WAN2 ISP Setting screen.

Viewing Attached Devices and the DHCP Log

The LAN Groups screen contains a table of all IP devices that the UTM has discovered on the local network. The LAN Setup screen lets you access the DHCP log.

Viewing Attached Devices

To view the attached devices in the LAN Groups screen:

1. Select **Network Config** > **LAN Settings** from the menu. The LAN Settings submenu tabs appear, with the LAN Setup screen in view (see Figure 11-20 on page 11-30, which contains some profiles in the VLAN Profiles table as an example).

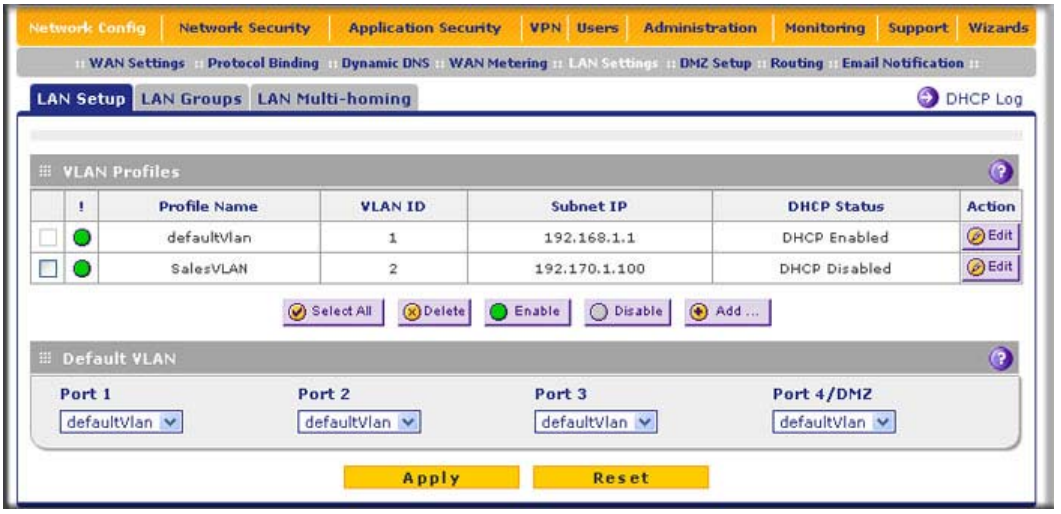


Figure 11-20

2. Click the **LAN Groups** submenu tab. The LAN Groups screen displays (Figure 11-21 shows some examples in the Known PCs and Devices table).

Figure 11-21

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:

- **Checkbox**. 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 pull-down menu in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen.
- **Action**. The Edit table button that 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.

Viewing the DHCP Log

To review the most recent entries in the DHCP log:

1. Select **Network Config** > **LAN Settings** from the menu. The LAN Settings submenu tabs appear, with the LAN Setup screen in view (see Figure 11-20 on page 11-30).
2. Click the **DHCP Log** option arrow at the top right of the LAN Setup screen. The DHCP Log appears in a popup window (see Figure 11-22 on page 11-32).

   To view the most recent entries, click **refresh**. To delete all the existing log entries, click **clear log**.

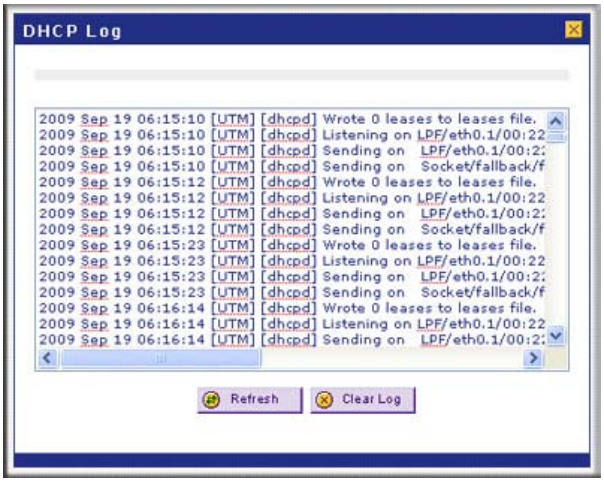


Figure 11-22

Querying Logs and Generating Reports

The extensive logging and 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:

- Querying and downloading logs
- Generating and downloading e-mail, Web, and system reports
- Scheduling automatic e-mail, Web, and system reports, and e-mailing these reports to specified recipients.

For information about e-mailing logs and sending logs to a syslog server, see “Configuring and Activating System, E-mail, and Syslog Logs” on page 11-6.

Querying 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).

The UTM provides 13 types of logs:

- **Traffic Logs**. All scanned incoming and outgoing traffic.
- **Spam Logs**. All intercepted spam.

- **System Logs**. The system event logs that you have specified on the Email and Syslog screen (see "Configuring and Activating System, E-mail, and Syslog Logs" on page 11-6). However, by default, many more types of events are logged in the system logs.
- **Service Logs**. All events that are related to the status of scanning and filtering services that are part of the Application Security main navigation menu. These events include update success messages, update failed messages, network connection errors, and so on.
- **Malware Logs**. All intercepted viruses, spyware, and other malware threats.
- **Email filter Logs**. All e-mails that are blocked because of file extension and keyword violations.
- **Content Filter Logs**. All attempts to access blocked Web sites and URLs.
- **IPS Logs**. All IPS events.
- **Portscan Logs**. All port scan events.
- **Instant Messaging/Peer-to-Peer Logs**. All instant messaging and peer-to-peer access violations.
- **Firewall Logs**. The firewall logs that you have specified on the Firewall Logs screen (see "Configuring and Activating Firewall Logs" on page 11-13 on page 11-14).
- **IPSEC VPN Logs**. All IPsec VPN events.
- **SSL VPN Logs**. 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
- Client and server IP addresses
- Recipient e-mail address

To query and download logs:

1. Select **Monitoring** > **Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Logs Query** submenu tab. The Logs Query screen displays (see Figure 11-23 on page 11-34, which shows the Malware log information settings as an example).

   Depending on the selection that you make from the Log Type pull-down menu, the screen adjusts to display the settings for the selected type of log.

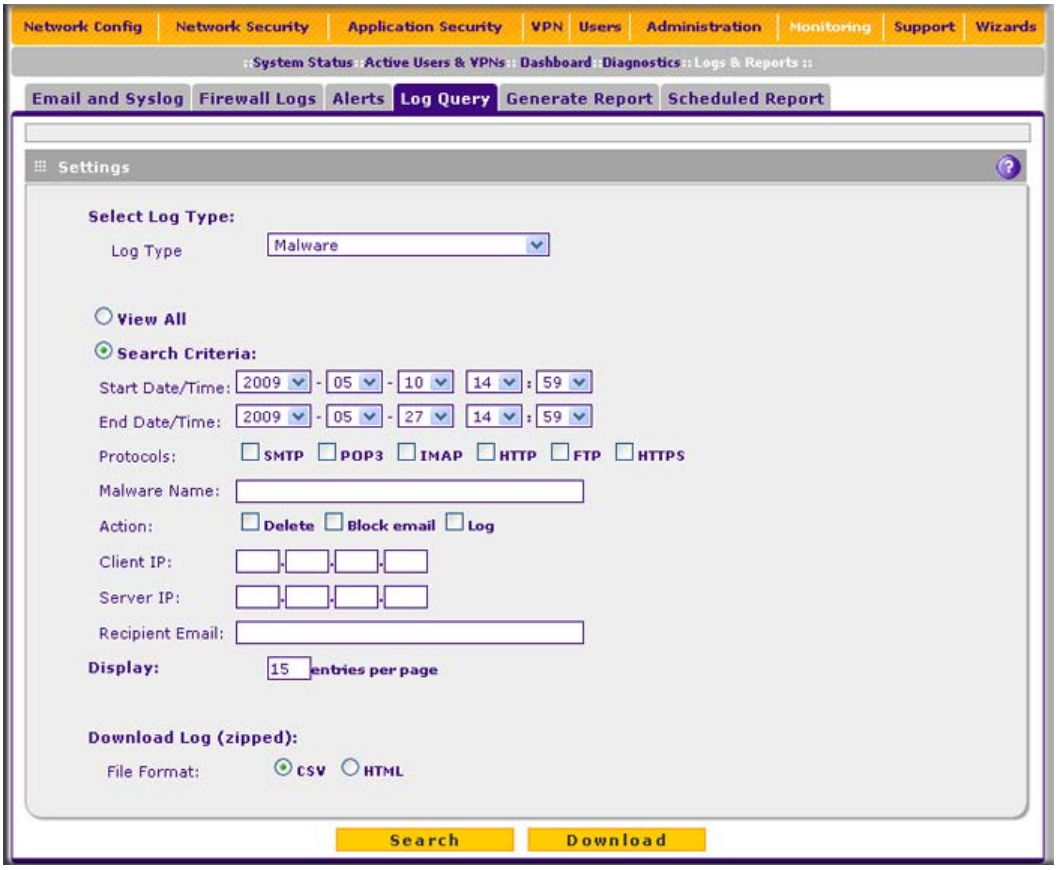


Figure 11-23

3. Enter the settings as explained in Table 11-15.

Table 11-15. Logs Query Settings

Setting	Description (or Subfield and Description)
Log Type	Select one of the following log types from the pull-down menu: • **Traffic**. All scanned incoming and outgoing traffic. • **Spam**. All intercepted spam. • **System**. 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.

Table 11-15. Logs Query Settings (continued)

Setting	Description (or Subfield and Description)	
Log Type (continued)	• **Service Logs**. All events that are related to the status of scanning and filtering services that are part of 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 e-mails that are blocked because of file extension and keyword violations. • **Content filters**. All attempts to access blocked Web sites and URLs. • **IPS**. All IPS events. • **Port Scan**. All port scan events. • **Instant Messaging/Peer to Peer**. All instant messaging and peer-to-peer access violations. • **Firewall**. The firewall logs that you have specified on the Firewall Logs screen (see "Configuring and Activating Firewall Logs" on page 11-13). • **IPSEC VPN**. All IPsec VPN events. • **SSL VPN**. All SSL VPN events.	
View All	Select one of the following radio buttons: • **View All**. Display or download the entire selected log. • **Search Criteria**. Query the selected log by configuring the search criteria that are available for the selected log.	
Search Criteria	Start Date/Time	From the pull-down menus, 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, Instant Messaging/Peer to Peer.
	End Date/Time	From the pull-down menus, 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, Instant Messaging/Peer to Peer.
	Protocols	Select one or more checkboxes 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.

Table 11-15. Logs Query Settings (continued)

Setting	Description (or Subfield and Description)	
Search Criteria (continued)	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, Instant Messaging/Peer to Peer.
	Server IP	The server IP address that is queried. **This field is available for the following logs**: Traffic, Malware, Content filters, Port Scan, IPS, Instant Messaging/Peer to Peer.
	Category	From the pull-down menu, select a category that is queried. **The following categories can be selected**: • For the IPS log: a threat, protocol, or application. • For the Instant Messaging/Peer to Peer log: an instant messaging or peer-to-peer application.
	Reason	Select one or more checkboxes to specify the reasons that are queried: **The following reasons can be selected**: • For the Email filters log: keyword, file type, file name, password, and size limit. • For the Content filters log: URL, file type, and size limit.
	Spam Found By	**This field is available only for the Spam log**. Select a checkbox to specify the method by which Spam is detected: Blacklist or Heuristic Scan. **Note**: Heuristic Scan refers to 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: block or tag. • For the Malware log: delete, block email, or log.
	Email Subject	The e-mail subject that is queried: **This field is available for the following logs**: Spam and Email filters.
	Sender Email	The sender's e-mail address that is queried. **This field is available only for the Traffic log**.
	Recipient Email	The recipient 's e-mail address that is queried. **This field is available for the following logs**: Traffic, Spam, Malware, and Email filters.

Table 11-15. Logs Query Settings (continued)

Setting	Description (or Subfield and Description)	
Search Criteria (continued)	Message	The e-mail message text that is queried. **This field is available for the following logs**: Port Scan, IPS, Instant Messaging/Peer to Peer.
	Subject	The e-mail subject line that is queried. **This field is available only for the Traffic log**.
	Size	The file's minimum and maximum size (in bytes) that are 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 for syslog server severity indications: 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.	

4. 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, on screen.
- **Download**. Query the log according to the search criteria that you specified and download the log to a computer.

Note: The system, firewall, IPsec VPN, and SSL VPN logs cannot be queried or downloaded. When you select any of these logs, you can view them through the Web Management Interface, that is, they appear on screen.

Example: Using 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:

1. On the Log Query screen (see Figure 11-23 on page 11-34), select **Traffic** as the log type.
2. Select the start date and time from the pull-down menus.
3. Select the end date and time from the pull-down menus.
4. Next to Protocols, select the **HTTP** checkbox.
5. Click **Search**. After a few minutes, the log appears on screen.
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 so 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% 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, non-traffic logs) are automatically backed up on the UTM every 15 minutes. However, if a power failure affects the UTM, logs that where created within this 15-minute period are lost.

To manually purge selected logs, see "Configuring and Activating System, E-mail, and Syslog Logs" on page 11-6.

Scheduling and Generating Reports

The UTM lets you schedule and generate three types of reports:

- **Email Reports**. For each protocol (SMTP, POP3, and IMAP), the report shows, the following information per day, both in tables and graphics:
  - Number of connections
  - Traffic amount in MB
  - Number of malware incidents
  - Number of files blocked
  - Number of blacklist violations (not applicable to POP3 and IMAP)
  - Number of e-mails captured by Distributed Spam Analysis (not applicable to IMAP).
- **Web Reports**. For each protocol (HTTP HTTPS, and FTP), the report shows the following information per day, both in tables and graphics:
  - Number of connections
  - Traffic amount in MB
  - Number of malware incidents
  - Number of files blocked
  - Number of URLs blocked (not applicable to FTP)
- **System Reports**. The report shows IPS, application, and malware incidents:
  - The following IPS incident are shown per day, both in tables and graphics:
    - Number of detected port scans and top 10 scanned destination IP addresses by count
    - Number of Web attacks
    - Number of mail attacks
    - Number of database attacks
    - Number of application attacks
    - Number of network protocol attacks
    - Number of malware attacks
    - Number of miscellaneous attacks
    - Top 10 attacking IPS rule names by count, top 10 attacking source IP addresses by count, and top 10 attacked destination IP addresses by count.

- The following application incident are shown per day, both in tables and graphics:
  - Number of instant messaging application violations, top 10 violating instant messaging applications by count, and top 10 violating instant messaging clients by count
  - Number of peer-to-peer application violations, top 10 violating peer-to-peer applications by count, and top 10 violating peer-to-peer clients by count
- The following malware incident are shown per day, both in tables and graphics:
  - The number of SMPT, POP3, and IMAP incidents, the top 10 e-mail malware threats by count, and the top 10 infected e-mail clients by count.
  - The number of HTTP, HTTPS, and FTP incidents, the top 10 Web malware threats by count, and the top 10 infected Web clients by count.

The reports that you select are generated as both Microsoft Office Comma Separated Values (CSV) and MHTML files. The CSV files do not contain headers for the tables nor graphics, but the MHTML files contain both. You can download the reports as zipped files.

Generating Reports

To generate a report:

1. Select **Monitoring** > **Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Generate Reports** submenu tab. The Generate Reports screen displays (see Table 11-24 on page 11-41).

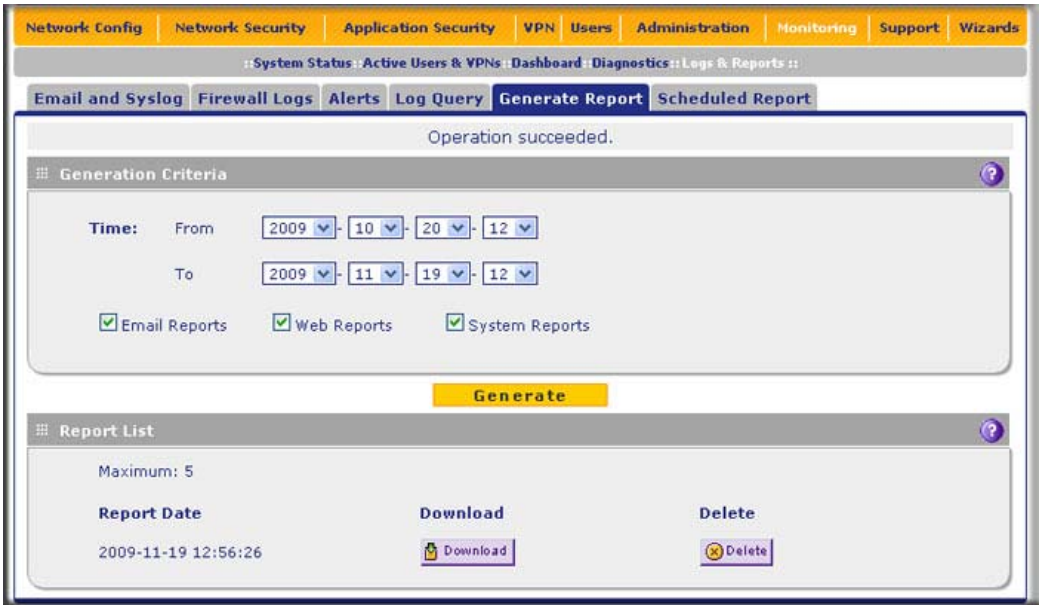


Figure 11-24

3. Enter the settings as explained in Table 11-16.

Table 11-16. Generate Report Settings

Setting	Description (or Subfield and Description)
Time From	From the pull-down menus, specify the start year, month, day, hour, and minutes for the report.
Time To	From the pull-down menus, specify the end year, month, day, hour, and minutes for the report. **Note**: The maximum report period is 31 days.
Reports	Select one or more checkboxes to specify the reports that are generated: • **Email Reports**. • **Web Reports**. • **System Reports**. **Note**: You can select all three checkboxes, but you might generate a very large report.

4. Click **Generate**. After a few minutes, the report is added to the Report List, which can contain a maximum of five saved reports. (To delete a a previously saved report, click its **Delete** table button.)

5. Select the new or a previously saved report for downloading by clicking its **Download** table button. The reports download as a zipped file that contains both CSV and HTML files.

Scheduling Reports

To schedule automatic generation and e-mailing of reports:

1. Select **Monitoring** > **Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Schedule Reports** submenu tab. The Schedule Reports screen displays.

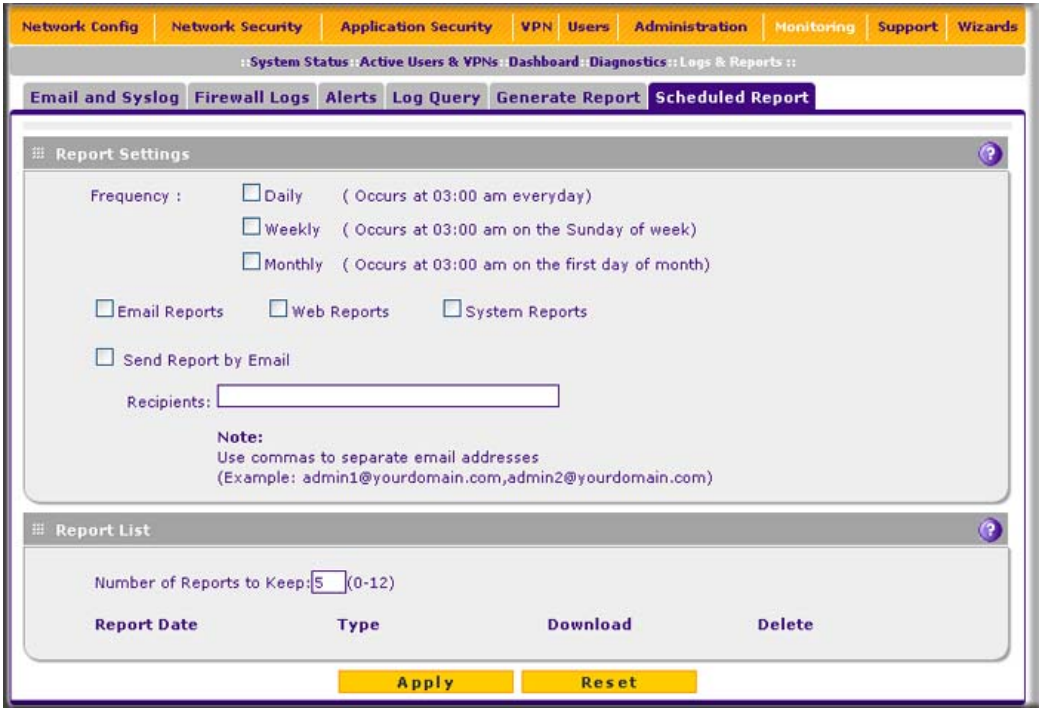


Figure 11-25

3. Enter the settings as explained in Table 11-17.

Table 11-17. Schedule Report Settings

Setting	Description (or Subfield and Description)
Report Settings	
Frequency	Select one of the following checkboxes to specify the frequency with which the reports are generated and e-mailed. • **Daily**. The report is generated daily at 3:00 am. • **Weekly**. The report is generated weekly on Sunday at 3:00 am. • **Monthly**. The report is generated monthly on first day of the month at 3:00 am.

Table 11-17. Schedule Report Settings (continued)

Setting	Description (or Subfield and Description)	
Reports	Select one or more checkboxes to specify the reports that are generated: • **Email Reports**. • **Web Reports**. • **System Reports**. **Note**: You can select all three checkboxes, but you might generate a very large report.	
Send Report by Email	Select this checkbox to enable the UTM to send the report to the recipients that you must specify below.	
	Recipients	The e-mail addresses of the report recipients. **Note**: Use commas to separate email addresses.
Report List		
Number of Reports to Keep	Enter the number of reports that the UTM saves. The maximum number is 12.	

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

Using 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.

To display the Diagnostics screen, select **Monitoring** > **Diagnostics** from the menu. To facilitate the explanation of the tools, the Diagnostics screen is divided and presented in this manual in three figures (Figure 11-26 on page 11-44, Figure 11-27 on page 11-46, and Figure 11-28 on page 11-47).

Using the Network Diagnostic Tools

This section discusses the Network Diagnostics section and the Perform a DNS Lookup section of the Diagnostics screen.

Figure 11-26 [Diagnostics, screen 1of 3]

Sending 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 Windows menu bar to return to the Diagnostics screen.

To send a ping:

1. Locate the Network Diagnostics section on the Diagnostics screen.
2. In the IP Address field, enter the IP address that you want to ping.
3. If the specified address is reached through a VPN tunnel, select the **Ping through VPN tunnel** checkbox.
4. 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 Windows menu bar.

Tracing 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.
2. In the IP Address field, enter the IP address for which you want trace the route.
3. 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 Windows menu bar.

Displaying the Routing Table

Displaying the internal routing table can assist NETGEAR Technical Support to diagnose routing problems.

To display the routing table:

1. Locate the Network Diagnostics section on the Diagnostics screen.
2. Next to Display the Routing Table, click the **Display** button. The routing table is displayed in the Route Display screen that appears as a popup window.

Looking up a DNS Address

A DNS (Domain Name Server) 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.
2. In the Domain Name field, enter a domain name.
3. 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 Windows menu bar.

Using the Realtime Traffic Diagnostics Tool

This section discusses the Realtime Traffic Diagnostics section and the Perform a DNS Lookup section of the Diagnostics screen.

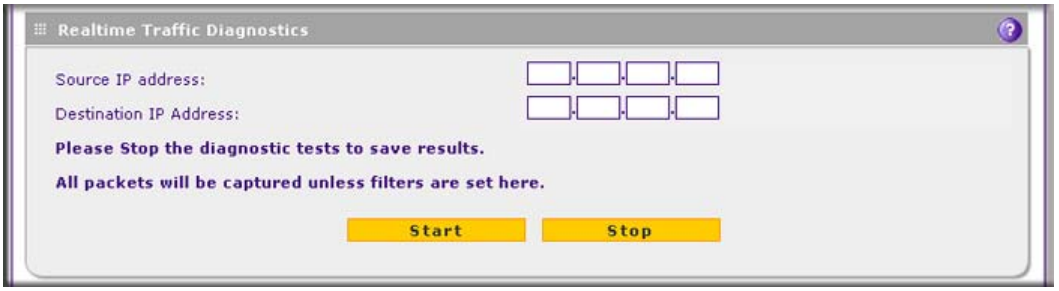


Figure 11-27 [Diagnostics, screen 2 of 3]

You can use the Realtime 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 most bandwidth, which users use most bandwidth, how long users are connected, and other information.

To use the Realtime Traffic Diagnostics tool:

1. Locate the Realtime Traffic Diagnostics section on the Diagnostics screen.
2. In the Source IP address field, enter the IP address of source of the traffic stream that you want to analyze.
3. In Destination IP address, enter the IP address of the destination of the traffic stream that you want to analyze.
4. 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.
5. When you want to stop capturing the traffic flow, click **Stop**.
6. Select a location to save the captured traffic flow. (The default file name is diagnostics.result.dat.) The file downloads to the location that you specify.
7. When the download is complete, browse to the download location you specified and verify that the file has been downloaded successfully.
8. Send the file to NETGEAR Technical Support for analysis.

Gathering Important Log Information and Generating a Network Statistics Report

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.

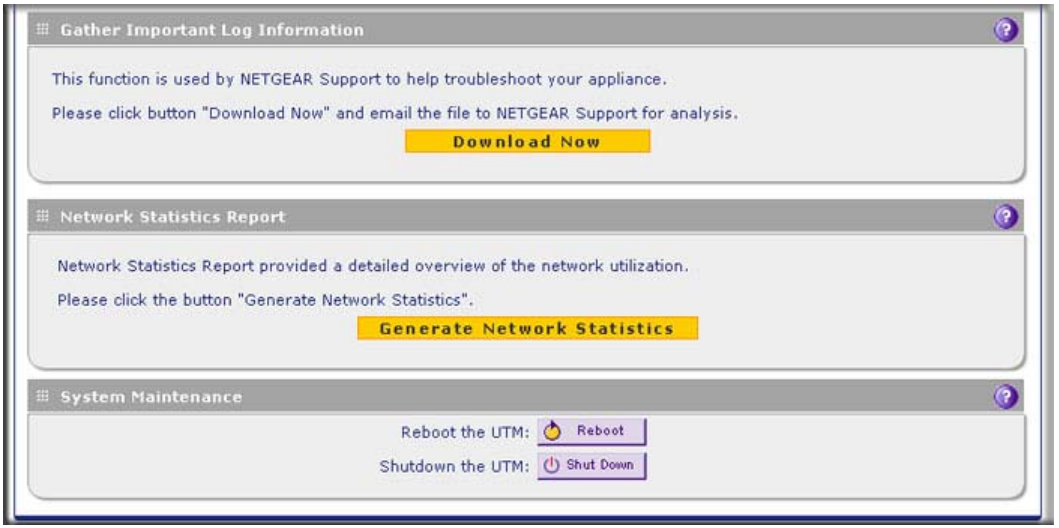


Figure 11-28 [Diagnostics, screen 3of 3]

Gathering Important Log Information

To gather log information about your UTM:

1. Locate the Gather Important Log Information section on the Diagnostics screen.
2. Click **Download Now**. You are prompted to save the downloaded log information file to your computer. The default file name is importantlog.gpg.
3. When the download is complete, browse to the download location you specified and verify that the file has been downloaded successfully.

Generating 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:

1. Locate the Network Statistics Report section on the Diagnostics screen.
2. Click **Generate Network Statistics**. The network statistics report is sent as an e-mail to the recipient that you specified on the Email Notification screen (see "Configuring the E-mail Notification Server" on page 11-5).

Rebooting and Shutting 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 re-established when possible.

To reboot the UTM:

1. Locate the Reboot the System section on the Diagnostics screen.
2. 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 "Rebooting Without Changing the Firmware" on page 10-21.

To shut down the UTM:

1. Locate the Reboot the System section on the Diagnostics screen.
2. Click the **Shutdown** button. The UTM shuts down.

Note: You can shut down the UTM using the Web Management Interface, but you cannot start up the UTM using the Web Management Interface.

Chapter 12
Troubleshooting and Using Online Support

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 12-2.
- Have I connected the UTM correctly?

  Go to "Basic Functioning" on page 12-2.
- I cannot access the UTM's Web Management Interface.

  Go to "Troubleshooting the Web Management Interface" on page 12-3.
- A time-out occurs.

  Go to "When You Enter a URL or IP Address a Time-out Error Occurs" on page 12-4.
- I cannot access the Internet or the LAN.

  "Troubleshooting the ISP Connection" on page 12-5.
- I have problems with the LAN connection.

  Go to "Troubleshooting a TCP/IP Network Using a Ping Utility" on page 12-7.
- I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 12-9.
- The date or time is not correct.

  Go to "Problems with Date and Time" on page 12-10.
- I need help from NETGEAR.

  Go to "Using Online Support" on page 12-10.

Note: The UTM's diagnostic tools are explained in "Using Diagnostics Utilities" on page 11-43.

Basic Functioning

After you turn on power to the UTM, the following sequence of events should occur:

1. When power is first applied, verify that the PWR LED is on.
2. After approximately two minutes, verify that:
   a. The Test LED is no longer lit.
   b. The LAN port Left LEDs are lit for any local ports that are connected.
   c. The WAN port Left 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 properly connected to your UTM and that the power supply adapter is properly 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:

- Turn the power off, and then turn it on again to see if the UTM recovers.
- Clear the UTM's configuration to factory defaults. Doing so sets the UTM's IP address to **192.168.1.1**. This procedure is explained in "Restoring the Default Configuration and Password" on page 12-9.

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 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 a standard straight-through Ethernet cables or an Ethernet crossover cables.

Troubleshooting the Web Management Interface

If you are unable to 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 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 MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated 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, clear the UTM's configuration to factory defaults. This sets the UTM's IP address to **192.168.1.1**. This procedure is explained in "Restoring the Default Configuration and Password" on page 12-9.

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 Configuration 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 properly. 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 WAN1 ISP Settings or WAN2 ISP Settings screen of the dual-WAN port models, or on the WAN ISP Settings screen of the single-WAN port models (see "Manually Configuring the Internet Connection" on page 3-5).

- 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 ("Troubleshooting the Web Management Interface" on page 12-3).
- If the UTM is configured correctly, check your Internet connection (for example, your modem or router) to make sure that it is working correctly.

Troubleshooting 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 Security** > **WAN Settings** from the menu. The WAN1 ISP Settings screen (dual-WAN port models) or WAN ISP Settings screen (single-WAN port models) displays. For dual-WAN port models only, to display the WAN2 ISP Settings screen, click **WAN2 ISP Settings**.
4. Click the **WAN Status** option arrow at the top right of the WAN1 ISP Settings or WAN2 ISP Settings screen of the dual-WAN port models, or at the top right of the WAN IPS Settings screen of the single-WAN port models .The Connection Status screen appears in a popup window. (For more information, see "Viewing the WAN Ports Status" on page 11-27.)
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 five 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.
  Enter the host name, system name, or account name that was assigned to you by your ISP in the Account Name field on the WAN1 ISP Settings or WAN2 ISP Settings screen of the dual-WAN port models, or on the WAN ISP Settings screen of the single-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 (see "Manually Configuring the Internet Connection" on page 3-5).
- 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:
  - Inform your ISP that you have bought a new network device, and ask them to use the UTM's MAC address; or
  - Configure your UTM to spoof your PC's MAC address. You can do this in the Router's MAC Address section of the WAN1 Advanced Options or WAN2 Advanced Options screen of the dual-WAN port models, or in the Router's MAC Address section of the WAN Advanced Options screen of the single-WAN port models (see "Configuring Advanced WAN Options" on page 3-22).

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 may 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.

Troubleshooting 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. Troubleshooting a TCP/IP network is made very easy by using the Ping utility in your PC or workstation.

Testing 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 choose **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 12-3.
     - 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.

Testing 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 menu, type:

PING -n 10 <*IP address*>

where <*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 WAN1 ISP Settings or WAN2 ISP Settings screen of the dual-WAN port models, or in the Account Name field on the WAN ISP Settings screen of the single-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 (see "Manually Configuring the Internet Connection" on page 3-5).
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic 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 must 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 of the WAN1 Advanced Options or WAN2 Advanced Options screen of the dual-WAN port models, or in the Router's MAC Address section of the WAN Advanced Options screen of the single-WAN port models (see "Configuring Advanced WAN Options" on page 3-22).

Restoring the Default Configuration and Password

To reset the UTM to the original factory default settings, you can use one of the following two methods:

- Push the Reset button on the rear panel of the UTM (see "Rear Panel" on page 1-12) and hold the Reset button for about eight seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Reset button method.
- On the Backup & Restore Settings screen (see Figure 12-1), next to Revert to factory default settings, click the **Default** button:

  a. To display the Backup & Restore Settings screen, select **Administration** > **Backup & Restore Settings** from the menu (see Figure 12-1 on page 12-9).

Figure 12-1

  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 push the hardware 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 “Configuring Date and Time Service” on page 10-24). 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 five minutes and check the date and time again.
- Time is off by one hour. Cause: The UTM does not automatically sense Daylight Savings Time. Go to the System Date & Time screen, and select or deselect the checkbox marked “Automatically Adjust for Daylight Savings Time”.

Using Online Support

The UTM includes online support tools that allow NETGEAR Technical Support to securely perform diagnostics of the UTM, and that lets you submit suspicious files for analysis by NETGEAR. You can also access the knowledge base and documentation online.

Enabling 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 is 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** from the menu The Online Support screen displays.

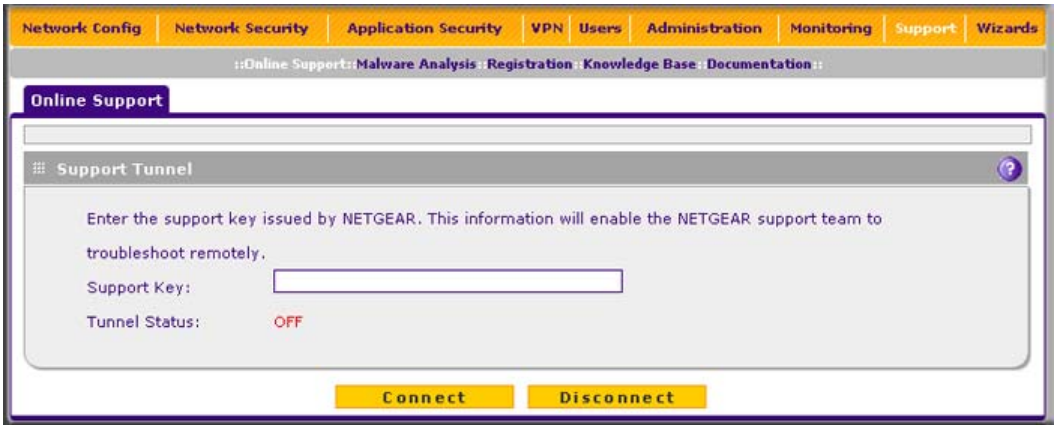


Figure 12-2

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 e-mail it to NETGEAR for analysis (see “Gathering Important Log Information” on page 11-47).

Sending Suspicious Files to NETGEAR for Analysis

You can report any undetected malware file or malicious e-mail 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** from the menu The Online Support screen displays.

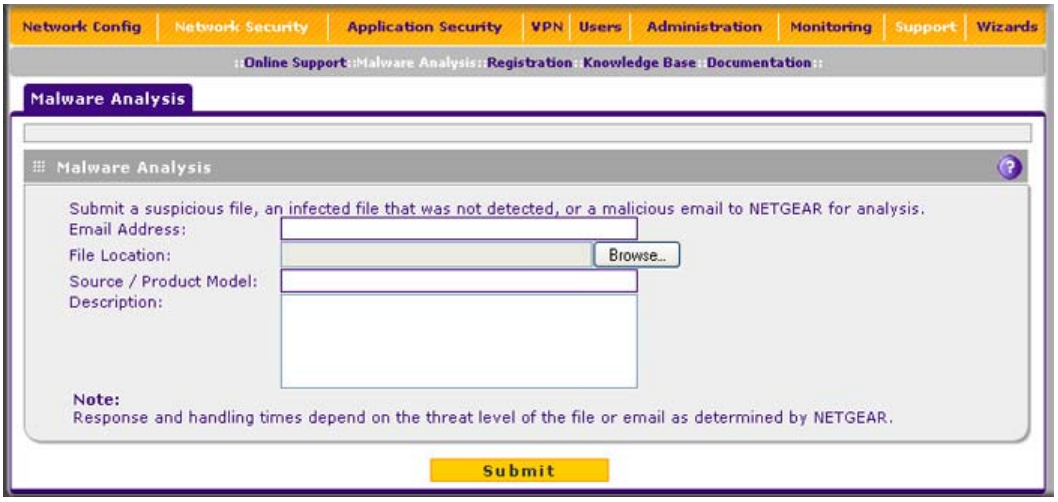


Figure 12-3

2. Enter the settings as explained in Table 12-1.

Table 12-1. Malware Analysis Settings

Setting	Description (or Subfield and Description)
Email Address	The e-mail 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 e-mail address if received via e-mail) and, if known, which product or scan feature (for example, the UTM or a desktop anti-virus application) detected the file.
Description	As an option, include a description or any information that is relevant.

3. Click **Submit**.

Accessing the Knowledge Base and Documentation

To access NETGEAR's Knowledge Base for the UTM, select **Support** > **Knowledge Base** from the menu. To access NETGEAR's documentation library for your UTM model, select **Support** > **Documentation** from the menu.

Appendix A
Default Settings and Technical Specifications

You can use the 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 "Reverting to Factory Default Settings" on page 10-18).

- To perform a hard reset, press and hold the Reset button for approximately eight seconds (until the TEST LED blinks rapidly). The UTM returns to the factory configuration settings that are shown in Table A-1 below.
- Pressing the Reset button for a shorter period of time simply causes the UTM to reboot.

Table A-1 shows the default configuration settings for the UTM.

Table A-1. 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
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

Table A-1. UTM Default Configuration Settings (continued)

Feature		Default behavior
(continued)	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	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

Table A-2 shows the physical and technical specifications for the UTM.

Table A-2. UTM Physical and Technical Specifications

Feature			Specification
Network Protocol and Standards Compatibility			
	Data and Routing Protocols		TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter			
	Universal input		100-240V, AC/50-60Hz, 1.2 Amp maximum
Physical Specifications			
	Dimensions (W x H x D)	cm	33 x 4.3 x 20.9
		inches	13 x 1.7 x 8.2
	Weight	kg.	2.1
		lb.	4.6

Table A-2. UTM Physical and Technical Specifications (continued)

Feature			Specification
Environmental Specifications			
	Operating temperatures	C	0º to 45º
		F	32º to 113º
	Storage temperatures	C	-20º to 70º
		F	-4º to 158º
	Operating humidity		90% maximum relative humidity, noncondensing
	Storage humidity		95% maximum relative humidity, noncondensing
Major Regulatory Compliance			
	Meets requirements of		FCC Class A
			CE
			WEEE
			RoHS
Interface Specifications			
	4 LAN, one of which is a configurable DMZ interface		AutoSense 10/100/1000BASE-T, RJ-45
	Dual-WAN port models: 2 WAN Single-WAN port models: 1 WAN		AutoSense 10/100/1000BASE-T, RJ-45
	1 administrative console port		RS-232
	1 USB		non-functioning, included for future management enhancements.

Table A-3 shows the IPsec VPN specifications for the UTM.

Table A-3. 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 1-1 on page 1-7).
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

Table A-3. UTM IPsec VPN Specifications (continued)

Setting	Specification
IPsec authentication types	Local User database, RADIUS PAP, RADIUS CHAP
IPsec certificates supported	CA digital certificate, Self digital certificate

Table A-4 shows the SSL VPN specifications for the UTM.

Table A-4. 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 marketing 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, WIKI-PAP, WIKID-CHAP, MIAS-PAP, MIAS-CHAP, NT Domain
SSL certificates supported	CA digital certificate, Self digital certificate

Note: For default e-mail and Web scan settings, see Table 6-1 on page 6-2.

Appendix B
Network Planning for Dual WAN Ports (Dual-WAN Port Models Only)

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

The UTM is a powerful and versatile solution for your networking needs. To make the configuration process easier and to understand all of the choices that are available to you, consider the following 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 a FQDN e to implement features such as exposed hosts and virtual private networks.
            - For load balancing mode, you might still need a 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 Figure B-1, with two ISPs connected to the UTM through separate physical facilities.
   - Each WAN port must 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.

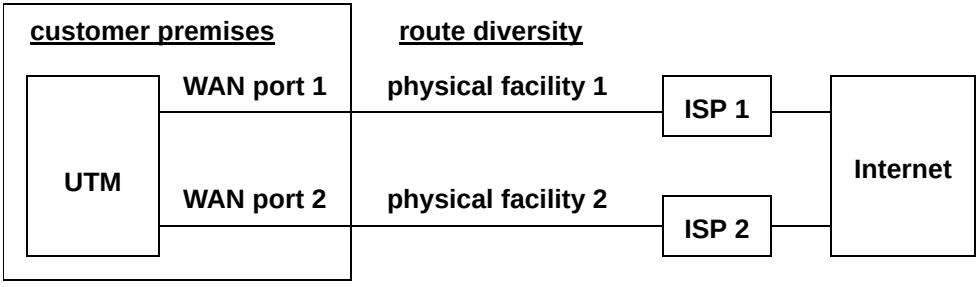


Figure B-1

   - 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.

   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 must 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

To use the UTM in your network, each computer must have an Ethernet Network Interface Card (NIC) installed and must be equipped with an Ethernet cable. If the computer will connect to your network at 100 Mbps or higher speeds, you must use a Category 5 (CAT5) cable.

Computer Network Configuration Requirements

The UTM integrates a Web Management Interface. To access the configuration menus on the UTM, your must use a Java-enabled Web browser that supports HTTP uploads such as Microsoft Internet Explorer 6 or higher, Mozilla Firefox 3 or higher, or Apple Safari 3 or higher with JavaScript, cookies, and you must 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 must connect a computer to the UTM, and the computer must be configured to automatically get its TCP/IP configuration from the UTM via DHCP.

Note: For help with the DHCP configuration, see the "TCP/IP Networking Basics" document that you can access from the link in Appendix E, "Related Documents."

The cable or DSL modem broadband access device must provide a standard 10 Mbps (10BASE-T) Ethernet interface.

Internet Configuration Requirements

Depending on how your ISPs 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 ore 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 ISPs to provide it to you 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 page.
  - 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 page.
  - 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 must be entered exactly as given by your ISP. For AOL customers, the login name is their primary screen name. Some ISPs use your full e-mail 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 e-mail 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 DSN Service Provider: _____

  FQDN: _____

Overview of the Planning Process

The areas that require planning when using 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:

- auto-rollover for increased reliability, or
- 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 between either 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 must be known in advance in order for the other tunnel end point to establish (or re-establish) the VPN tunnel.

	Note: When the UTM's WAN port rolls over, the VPN tunnel collapses and must be re-established using the new WAN IP address. However, you can configure automatic IPsec VPN rollover to ensure that an IPsec VPN tunnel is re-established.

- **Dual WAN Ports in Auto-Rollover Mode**. Rollover for an 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.

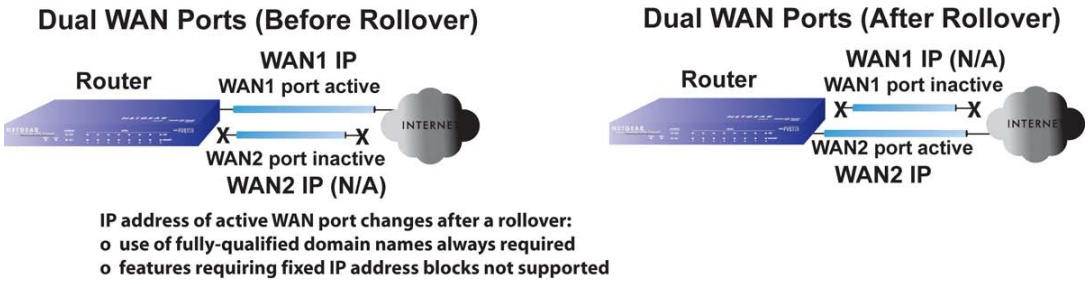


Figure B-2

Features such as multiple exposed hosts are not supported in auto-rollover mode because the IP addresses of each WAN port must be in the identical range of fixed addresses.

- **Dual WAN Ports in Load Balancing Mode**. Load balancing for an 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 must use FQDNs when the IP address is dynamic but FQDNs are optional when the IP address is static.

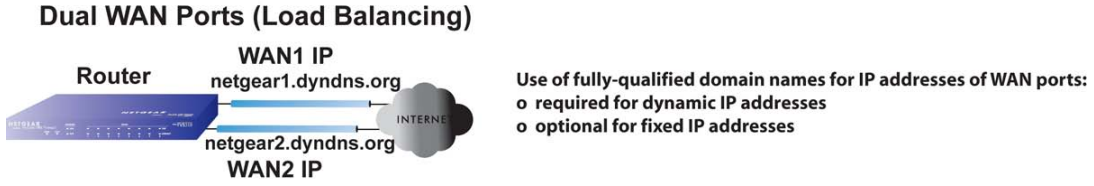


Figure B-3

Inbound Traffic

Incoming traffic from the Internet is normally 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 B-1. 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	Load Balancing
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 must 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 a FQDN if the IP address is dynamic.

Figure B-4

Inbound Traffic to a Dual WAN Port System

The IP address range of the UTM's WAN port must 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 must use a FQDN that toggles between the IP addresses of the WAN ports (that is, WAN1 or WAN2).

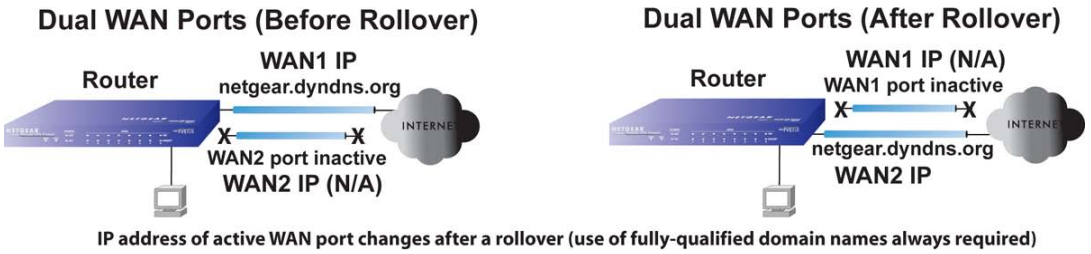


Figure B-5

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 a FQDN if the IP address is dynamic (see Figure B-6 on page B-9).

	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.

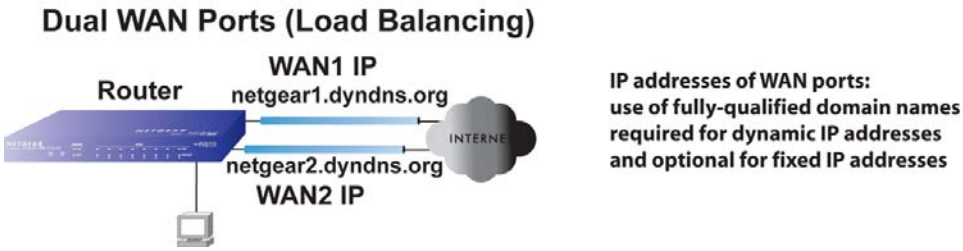


Figure B-6

Virtual Private Networks (VPNs)

When implementing virtual private network (VPN) tunnels, a mechanism must be used for determining the IP addresses of the tunnel end points. The addressing of the firewall's dual WAN port depends on the configuration being implemented:

Table B-2. 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[a]	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

a. All tunnels must be re-established after a rollover using the new WAN IP address.

For a single WAN gateway configuration, use a 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 must be re-established using the new WAN IP address. However, you can configure automatic IPsec VPN rollover to ensure that an IPsec VPN tunnel is re-established.

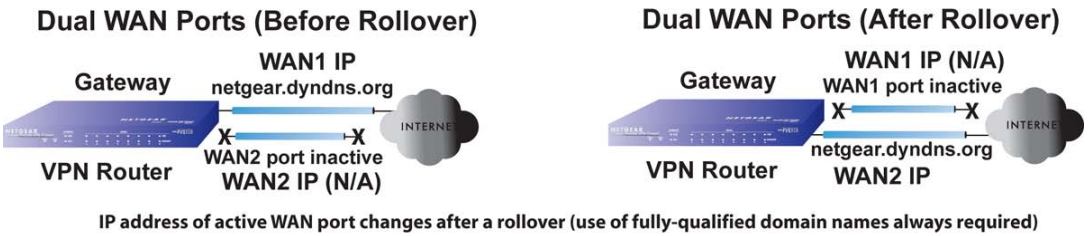


Figure B-7

- **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 must use FQDNs when the IP address is dynamic and FQDNs are optional when the IP address is static.

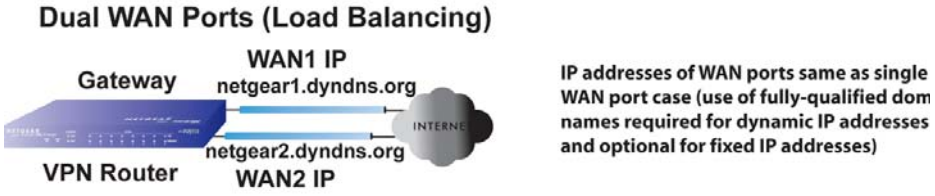


Figure B-8

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 must act as the responder.

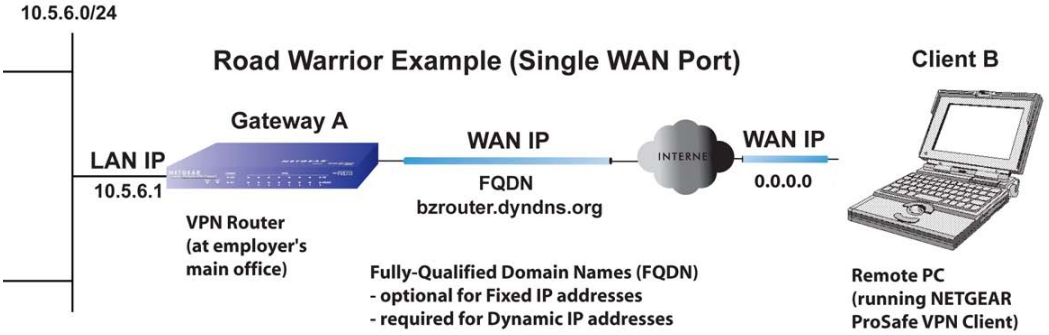


Figure B-9

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, a FQDN must be used. If the IP address is fixed, a 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 Figure B-10 on page B-12) because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as a responder.

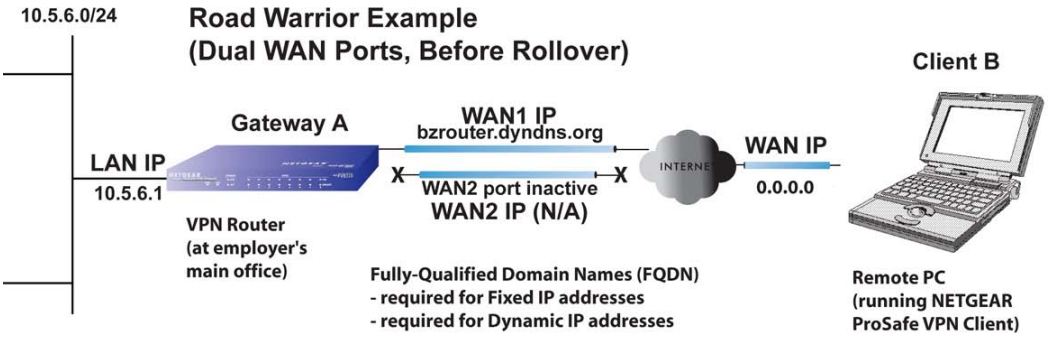


Figure B-10

The IP addresses of the WAN ports can be either fixed or dynamic, but you must always use a 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 Figure B-11) and the remote PC client must re-establish the VPN tunnel. The gateway WAN port must act as the responder.

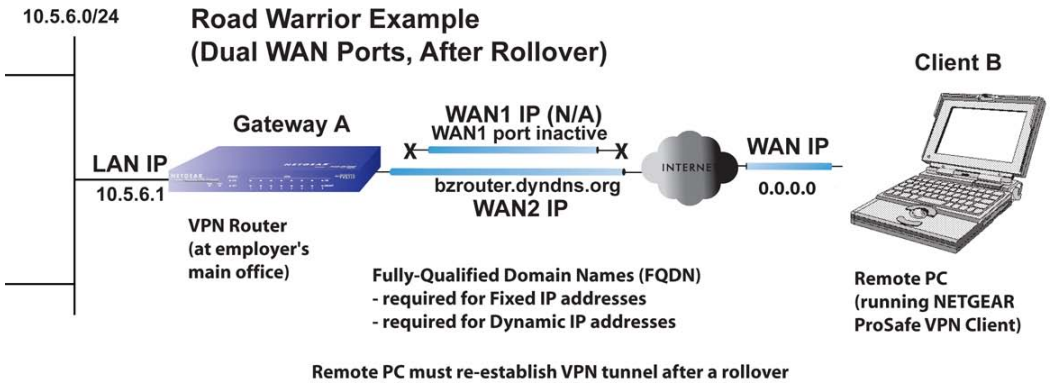


Figure B-11

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 re-establish 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 must act as the responder.

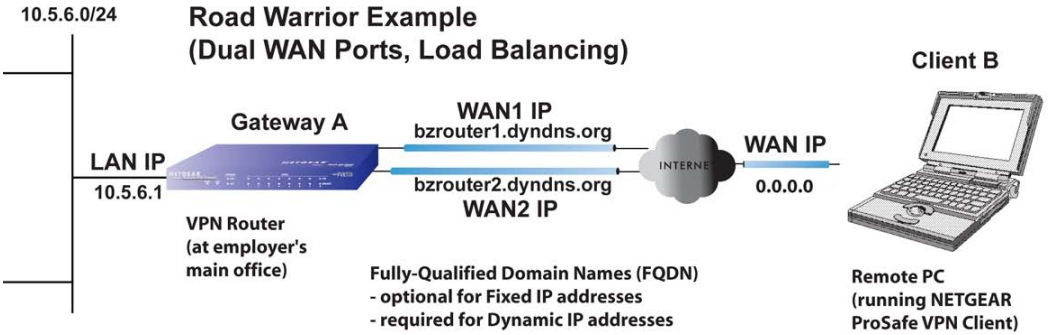


Figure B-12

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you must use a 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 (see Figure B-13 on page B-14).

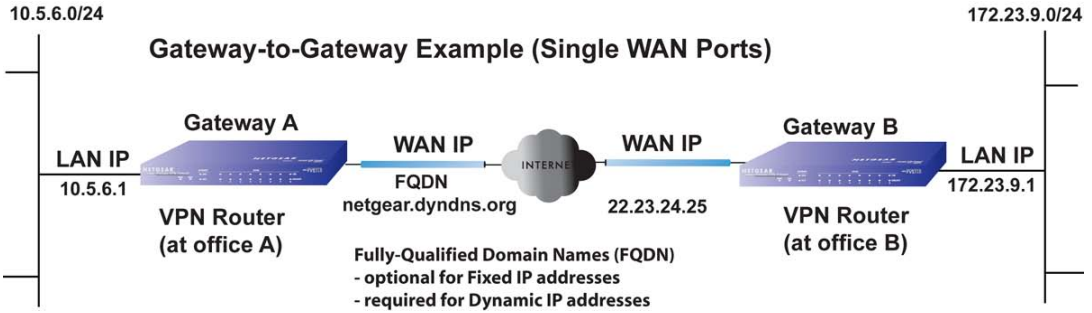


Figure B-13

The IP address of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you must 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 Figure B-14), 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.

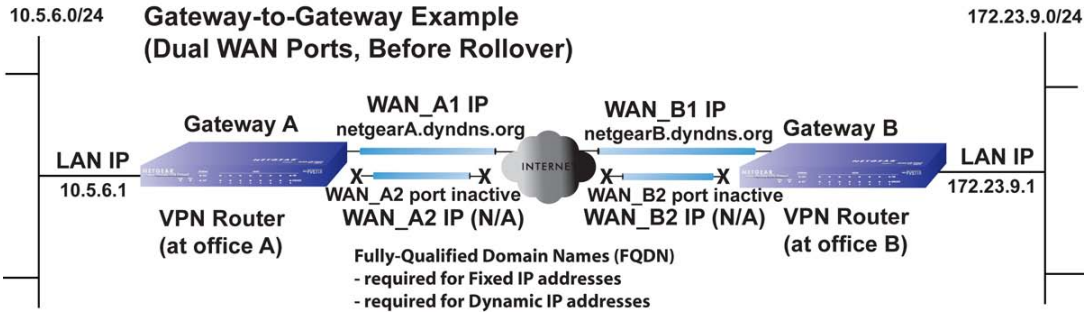


Figure B-14

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you must always use a 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 Figure B-15) and one of the gateways must re-establish the VPN tunnel.

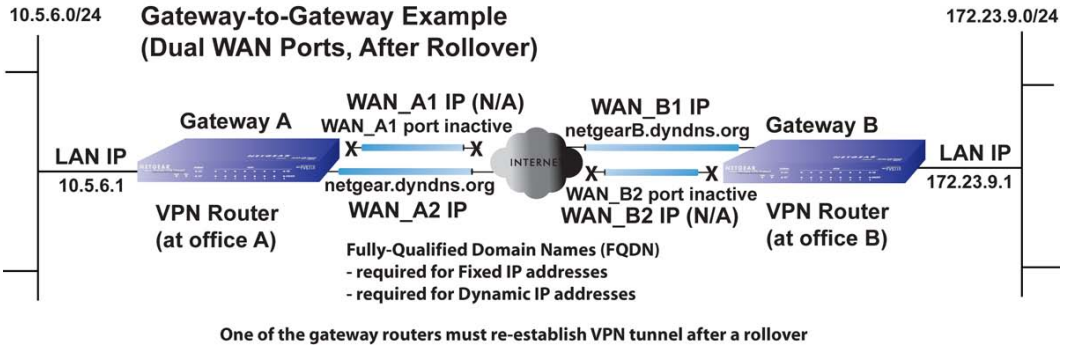


Figure B-15

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 Figure B-15) so that the other end of the tunnel has a known gateway IP address to establish or re-establish 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.

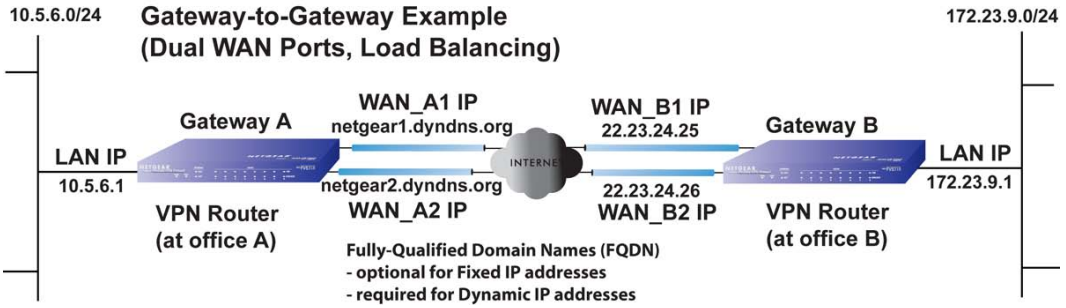


Figure B-16

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you must use a FQDN. If an IP address is fixed, an FQDN is optional.

VPN Telecommuter (Client-to-Gateway Through a NAT Router)

Note: The telecommuter case presumes 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 must act as the responder.

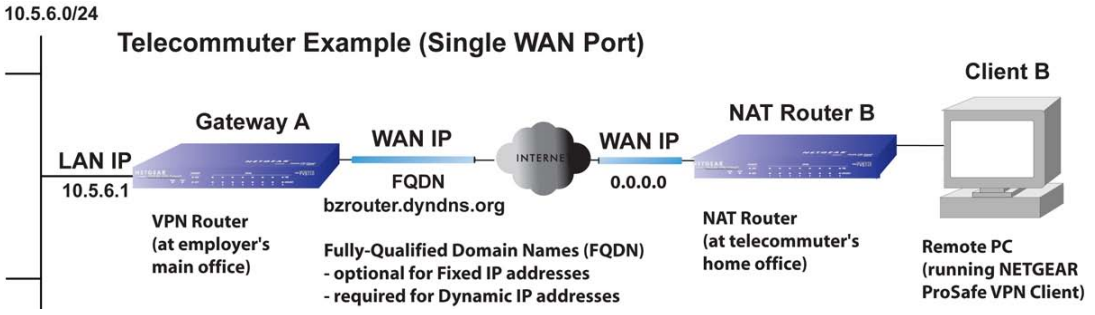


Figure B-17

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, you must use a FQDN. If the IP address is fixed, a 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 Figure B-18) because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

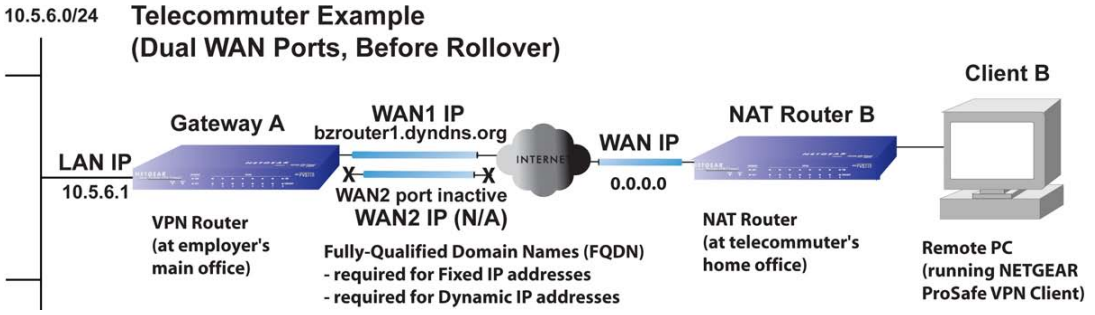


Figure B-18

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you must always use a 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 Figure B-19) and the remote PC must re-establish the VPN tunnel. The gateway WAN port must act as the responder.

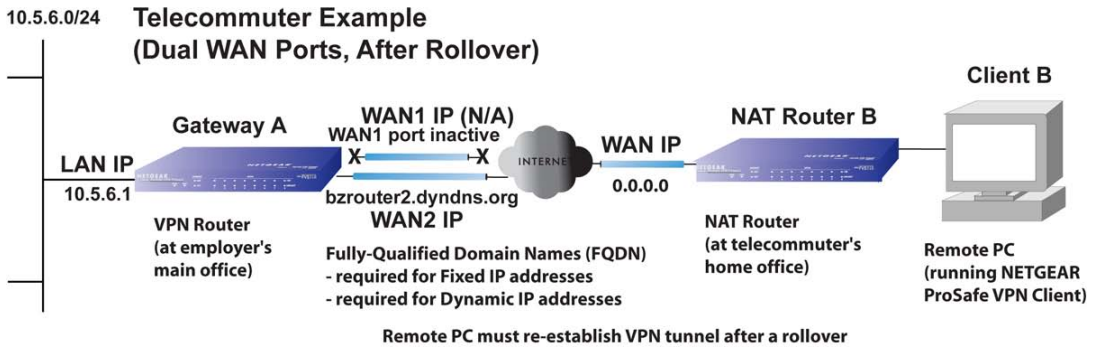


Figure B-19

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 re-establish 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 must act as the responder.

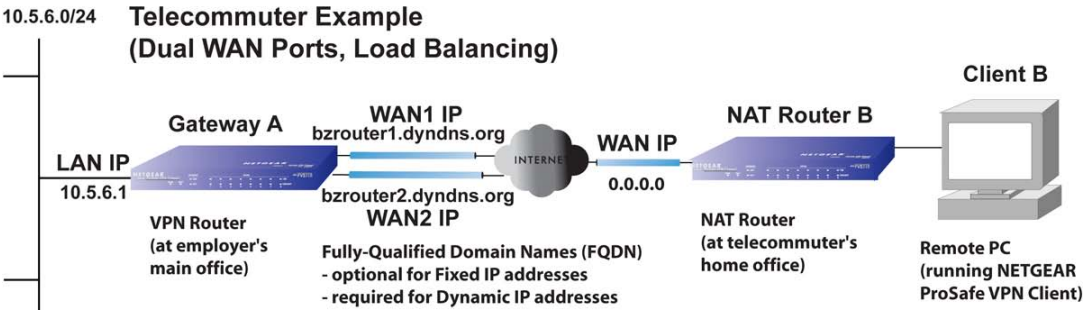


Figure B-20

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you must use a FQDN. If an IP address is fixed, an FQDN is optional.

Appendix C
System Logs and Error Messages

This appendix explains provides examples and explanations of system logs and error message. When applicable, a recommended action is provided.

This appendix contains the following sections:

This appendix uses the following log message terms.

Table C-1. Log Message Terms

Term	Description (or Subfield and Description)
[UTM]	System identifier
[kernel]	Message from the kernel.
CODE	Protocol code (e.g., 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 where 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 NTP, the WAN daemon, and others.

System Startup

This section describes log messages generated during system startup.

Table C-2. 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 C-3. 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 C-4. System Logs: Service

Message	2008-12-31 23:59:48 error Firmware update failed! Either the subscription is not yet registered, or has been 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: Thu Jan 01 00:01:52 GMT 1970.
- The resynchronization interval is governed by the specification defined in: DOC-00045_Ntp_Spec.pdf.

Table C-5. System Logs: NTP

Message 1 Message 2 Message 3 Message 4 Message 5 Message 6 Example	Nov 28 12:31:13 [UTM] [ntpdate] Looking Up time-f.netgear.com Nov 28 12:31:13 [UTM] [ntpdate] Requesting time from time-f.netgear.com Nov 28 12:31:14 [UTM] [ntpdate] adjust time server 69.25.106.19 offset 0.140254 sec Nov 28 12:31:14 [UTM] [ntpdate] Synchronized time with time-f.netgear.com Nov 28 12:31:16 [UTM] [ntpdate] Date and Time Before Synchronization: Tue Nov 28 12:31:13 GMT+0530 2006 Nov 28 12:31:16 [UTM] [ntpdate] Date and Time After Synchronization: Tue Nov 28 12:31:16 GMT+0530 2006 Nov 28 12:31:16 [UTM] [ntpdate] Next Synchronization after 2 Hours
Explanation	Message1: DNS resolution for the NTP server (time-f.netgear.com) Message2: request for NTP update from the time server. Message3: Adjust time by re-setting system time. Message4: Display date and time before synchronization, that is when resynchronization started Message5: Display the new updated date and time. Message6: Next synchronization will be after the specified time mentioned. Example: In the above logs the next synchronization will be after two hours.
Recommended Action	None

Login/Logout

This section describes logs that are generated by the administrative interfaces of the device.

Table C-6. 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 C-7. 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 log is logged when firewall restarts after applying any changes in the configuration.
Recommended Action	None

IPsec Restart

This section describes logs that are generated when the IPsec restarts.

Table C-8. 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 log is logged when IPsec restarts after applying any changes in the configuration.
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 secondary 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 device 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.

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_

System Logs: WAN Status, Auto Rollover (continued)

Explanation	The logs suggest that the fail-over was detected after five attempts instead of three. However, the reason the messages appear as above is because of the WAN state transition logic which is part of the failover algorithm. The above logs can be interpreted as below. The primary link failure is properly detected after the 3rd attempt. Thereafter the algorithm attempts to restart WAN and checks once again to see if WAN1 is still down. This results in the 4th failure detection message. If it is then it starts secondary link and once secondary link is up, secondary link is marked as active. Meanwhile secondary link has failed once more and that results 5th failure detection message. Note that the 5th failure detection and the message suggesting that the secondary link is active have the same timestamp and so they happen in the same algorithm state-machine cycle. So, although it appears that the failover did not happen immediately after three failures, internally, the failover process is triggered after the 3rd failure and transition to secondary link is completed by the 5th failure. The primary link is also restarted every three failures till it is functional again. In the above log, primary link was restarted after the 6th failure, that is, three 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 C-9. 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 which 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 (see “Manually Configuring the Internet Connection” on page 3-5).

- PPPoE Idle-Timeout Logs

Table C-10. System Logs: WAN Status, PPPoE Idle-Timeout

Message 1 Message 2 Message 3 Message 4 Message 5 Message 6 Message 7 Message 8 Message 9 Message 10 Message 11	Nov 29 13:12:46 [UTM] [pppd] Starting connection Nov 29 13:12:49 [UTM] [pppd] Remote message: Success Nov 29 13:12:49 [UTM] [pppd] PAP authentication succeeded Nov 29 13:12:49 [UTM] [pppd] local IP address 50.0.0.62 Nov 29 13:12:49 [UTM] [pppd] remote IP address 50.0.0.1 Nov 29 13:12:49 [UTM] [pppd] primary DNS address 202.153.32.3 Nov 29 13:12:49 [UTM] [pppd] secondary DNS address 202.153.32.3 Nov 29 11:29:26 [UTM] [pppd] Terminating connection due to lack of activity. Nov 29 11:29:28 [UTM] [pppd] Connect time 8.2 minutes. Nov 29 11:29:28 [UTM] [pppd] Sent 1408 bytes, received 0 bytes. Nov 29 11:29:29 [UTM] [pppd] Connection terminated.
Explanation	Message 1: PPPoE connection establishment started. Message 2: Message from PPPoE server for correct login Message 3: Authentication for PPP succeeded. Message 4: Local IP address assigned by the server. Message 5: Server side IP address. Message 6: primary DNS configured in WAN status page. Message 7: secondary DNS configured in WAN status page. Message 8: The PPP link has transitioned to idle mode. This event occurs if there is no traffic from the LAN network. Message 9: The time in minutes for which the link has been up. Message 10: Data sent and received at the LAN side during the link was up. Message 11: PPP connection terminated after idle timeout
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPTP Idle-Timeout Logs

Table C-11. System Logs: WAN Status, PPTP Idle-Timeout

Message 1 Message 2 Message 3 Message 4 Message 5 Message 6 Message 7 Message 8 Message 9	Nov 29 11:19:02 [UTM] [pppd] Starting connection Nov 29 11:19:05 [UTM] [pppd] CHAP authentication succeeded Nov 29 11:19:05 [UTM] [pppd] local IP address 192.168.200.214 Nov 29 11:19:05 [UTM] [pppd] remote IP address 192.168.200.1 Nov 29 11:19:05 [UTM] [pppd] primary DNS address 202.153.32.2 Nov 29 11:19:05 [UTM] [pppd] secondary DNS address 202.153.32.2 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. Nov 29 11:20:45 [UTM] [pppd] Sent 520 bytes, received 80 bytes. Nov 29 11:20:51 [UTM] [pppd] Connection terminated.
Explanation	Message 1: Starting PPP connection process Message 2: Message from server for authentication success Message 3: Local IP address assigned by the server. Message 4: Server side IP address. Message 5: primary DNS configured in WAN status page. Message 6: secondary DNS configured in WAN status page. Message 7: Sensing idle link Message 8: Data sent and received at the LAN side while the link was up. Message 9: PPP connection terminated after idle timeout.
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPP Authentication Logs

Table C-12. System Logs: WAN Status, PPP Authentication

Message	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	Starting link: Starting PPPoE connection process Remote message: Login incorrect: Message from PPPoE server for incorrect login PAP authentication failed: PPP authentication failed due to incorrect login Connection terminated: PPP connection terminated
Recommended Action	If authentication fails, then check the login/password and enter the correct one.

Traffic Metering Logs

This section describes logs that are generated when the traffic meter has reached a limit.

Table C-13. 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 “Enabling the WAN Traffic Meter” on page 11-1), 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 Logs

This section describes logs that are generated when the UTM processes unicast packets.

Table C-14. 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 destined to the device from the WAN network. • For other parameters, see Table C-1.
Recommended Action	None

ICMP Redirect Logs

This section describes logs that are generated when the UTM processes ICMP Redirect messages.

Table C-15. 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 parameters, see Table C-1.
Recommended Action	None

Multicast/Broadcast Logs

This section describes logs that are generated when the UTM processes multicast and broadcast packets.

Table C-16. 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	• This packet (broadcast) is destined to the device from the WAN network. • For other settings, see Table C-1.
Recommended Action	None

Invalid Packet Logging

This section describes logs that are generated when the UTM processes invalid packets.

Table C-17. 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
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

Table C-17. System Logs: Invalid Packets (continued)

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
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 re-open/close 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

Table C-17. System Logs: Invalid Packets (continued)

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 C-18. Content Filtering and Security Logs: Web Filtering and Content Filtering

Message	2009-08-01 00:00:01 HTTP 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 it exceeds the allowed size limit. The message shows the date and time, protocol, client IP address, server IP address, URL, reason for the action, and action that is taken.
Recommended Action	None
Message	2009-08-01 00:00:01 HTTP 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 it violates a blocked Web category. The message shows the date and time, protocol, client IP address, server IP address, URL, reason for the action, and action that is taken.
Recommended Action	None
Message	2009-08-01 00:00:01 HTTP 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 it violates a blocked file extension. The message shows the date and time, protocol, client IP address, server IP address, URL, reason for the action, and action that is taken.
Recommended Action	None

Table C-18. Content Filtering and Security Logs: Web Filtering and Content Filtering

Message	2009-08-01 00:00:01 HTTP 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 it uses a proxy. The message shows the date and time, protocol, client IP address, server IP address, URL, reason for the action, and action that is taken.
Recommended Action	None
Message	2009-08-01 00:00:01 HTTP 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 it violates a blocked keyword. The message shows the date and time, protocol, client IP address, server IP address, URL, reason for the action, and action that is taken.
Recommended Action	None

Spam Logs

This section describes logs that are generated when the UTM filters spam e-mail messages.

Table C-19. Content Filtering and Security Logs: Spam

Message	2009-02-28 23:59:59 SMTP 192.168.1.2 192.168.35.165 xlzimap@test.com xlzpop3@test.com Blocked by customized blacklist. 0 RBL Block
Explanation	Logs that are generated when spam messages are blocked by the RBL. The message shows the date and time, protocol, client IP address, server IP address, sender, recipient, subject line, mechanism that detected the spam, and action that is taken.
Recommended Action	None
Message	2009-02-28 23:59:59 SMTP 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 Distributed Spam Analysis. The message shows the date and time, protocol, client IP address, server IP address, sender, recipient, subject line, mechanism that detected the spam, and action that is taken.
Recommended Action	None

Traffic Logs

This section describes logs that are generated when the UTM processes Web and e-mail traffic.

Table C-20. Content Filtering and Security Logs: Traffic

Message	2009-02-28 23:59:59 HTTP 99 192.168.1.2 192.168.33.8 xlzimap@test.com xlzpop3@test.com [MALWARE INFECTED] Fw: cleanvirus
Explanation	Web and e-mail traffic logs for HTTP, SMTP, POP3, IMAP, HTTPS, and FTP traffic. In this example message, a malware threat was cleaned from the traffic. The message shows the date and time, protocol, size of the Web file or e-mail, client IP address, server IP address, sender, recipient, and Web URL or e-mail subject line.
Recommended Action	None

Virus Logs

This section describes logs that are generated when the UTM detects viruses.

Table C-21. Content Filtering and Security Logs: Virus

Message	2008-02-29 23:59:00 POP3 OF97/Jerk Delete cleanvirus.zip 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, action that is taken, file name, client IP address, server IP address, sender, recipient, and Web URL or e-mail subject line.
Recommended Action	None

E-mail Filter Logs

This section describes logs that are generated when the UTM filters e-mail content.

Table C-22. Content Filtering and Security Logs: E-mail Filter

Message	2009-04-31 23:59:59 SMTP 192.168.1.2 192.168.35.165 xlzimap@test.com xlzpop3@test.com test Keyword test BlockMail
Explanation	Logs that are generated when e-mails are blocked because of a keyword violation in the subject line. The message shows the date and time, protocol, client IP address, server IP address, sender, recipient, e-mail subject line, reason for the action, details, and action that is taken.
Recommended Action	None

IPS Logs

This section describes logs that are generated when traffic matches IPS rules.

Table C-23. 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, 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 C-24. 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

Instant Messaging/Peer-to-Peer Logs

This section describes logs that are generated when the UTM filters instant messaging and peer to peer traffic.

Table C-25. Content Filtering and Security Logs: Instant Messaging/Peer-to-Peer

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, 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 C-26. 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 C-1.
Recommended Action	None

LAN to DMZ Logs

This section describes logs that are generated when the UTM processes LAN to DMZ traffic.

Table C-27. 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 C-1.
Recommended Action	None

DMZ to WAN Logs

This section describes logs that are generated when the UTM processes DMZ to WAN traffic.

Table C-28. 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 C-1.
Recommended Action	None

WAN to LAN Logs

This section describes logs that are generated when the UTM processes WAN to LAN traffic.

Table C-29. 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 C-1.
Recommended Action	None

DMZ to LAN Logs

This section describes logs that are generated when the UTM processes DMZ to LAN traffic.

Table C-30. 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 C-1.
Recommended Action	None

WAN to DMZ Logs

This section describes logs that are generated when the UTM processes WAN to DMZ traffic.

Table C-31. 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 C-1.
Recommended Action	None

Appendix D
Two Factor Authentication

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 cyber crime activities used by many unethical hackers and cyber criminals 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 the results of these cyber crime 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 to the authentication process. NETGEAR has also recognized the need to provide more than just a firewall to protect the networks. As part the new maintenance firmware release, NETGEAR has implemented a more robust authentication system known as Two-Factor Authentication (2FA or T-FA) on its SSL and IPSec VPN firewall product line 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 via 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 new security solution that enhances and strengthens security by implementing multiple factors to 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 that you are who you said 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 either 6 to 8 digits in length.
- Something you are—for example, biometrics such as fingerprints or retinal.

This appendix focuses and discusses only the first two factors, something you know and something you have. This new 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 must have both of these factors to gain access to your bank account. Similar to the ATM card, access to the corporate networks and data can also be strengthen using combination of the 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), that 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. Here is an example of how WiKID works.

1. The user launches the WiKID token software, enter the PIN that has been given to them (*something they know*) and then press “continue” to receive the OTP from the WiKID authentication server:

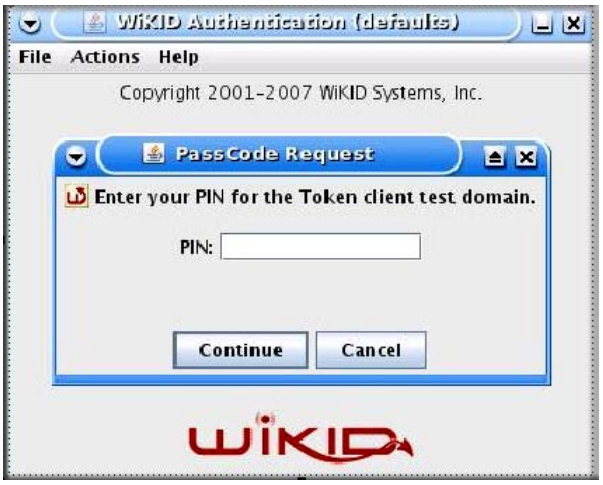


Figure D-1

2. A one-time passcode (*something they have*) is generated for this user.

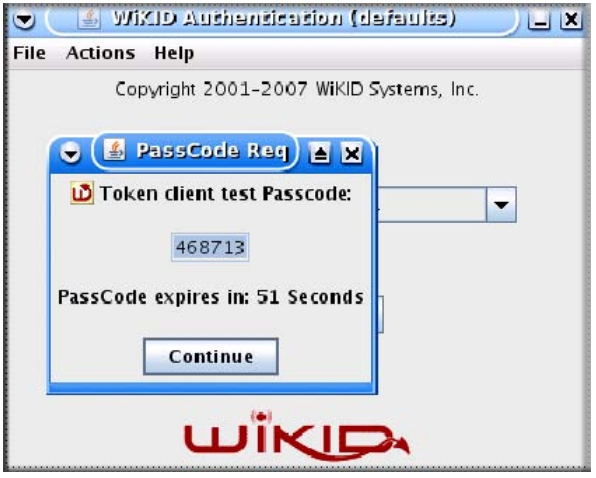


Figure D-2

Note: The one-time passcode is time synchronized to the authentication server so that the OTP can only be used once and must be used before the expiration time. If a user does not use this passcode before it is expired, the user must go through the request process again to generate a new OTP.

3. The user then proceeds to the Two-Factor Authentication login page and enters the generated one-time passcode as the login password.

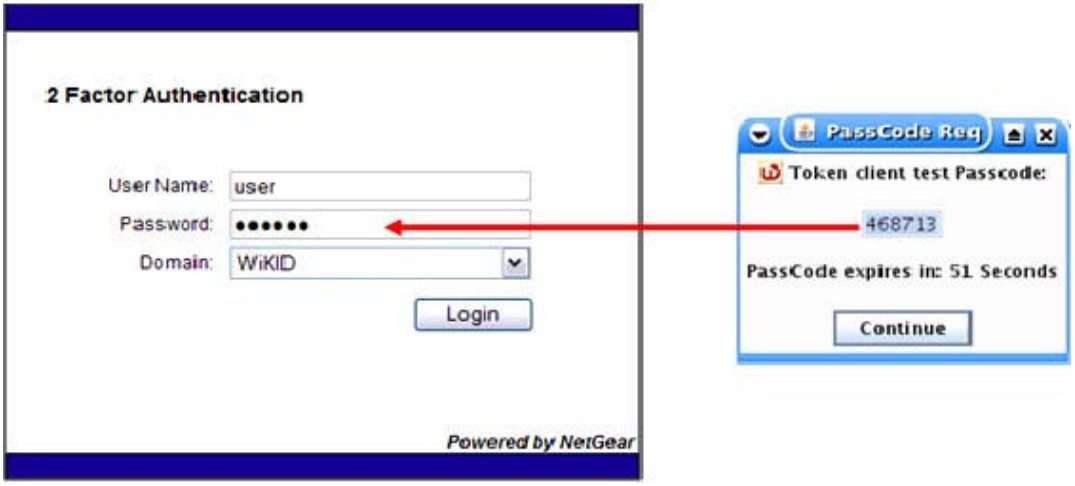


Figure D-3

Appendix E
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
TCP/IP Networking Basics	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Networking Basics	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing Your Network	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking Basics	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y