NETGEAR®

ProSAFE Gigabit Quad WAN SSL VPN Firewall SRX5308

Reference Manual

April 2013
202-10536-05

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

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

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx.*

Trademarks

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10536-05	–	April 2013	Added the following features: • Auto-rollover support with failure detection for IPv6 WAN interfaces (see *Configure Auto-Rollover for IPv6 Interfaces* and *Create an IPv6 Gateway-to-Gateway VPN Tunnel with the Wizard*) • Multicast pass-through with alternate networks (see *Configure Multicast Pass-Through for IPv4 Traffic*) • SNMP access from the WAN and SNMP trap events (see *Use a Simple Network Management Protocol Manager*) • Option to define what constitutes a UCP flood attack (see *Attack Checks*) • Authentication and encryption for the PPTP server (see *Configure the PPTP Server*) • Authentication for the L2TP server (see *Configure the L2TP Server*) • Option to select a gateway when you ping or send a trace packet and option to select a VPN policy when you ping or send a trace packet through a VPN tunnel (see *Send a Ping Packet* and *Trace a Route*)
202-10536-04	1.0	July 2012	A major revision. Added the following features: • Support for IPv6 with multiple IPv6 features, including a new general menu structure that provides both IPv4 and IPv6 radio buttons (very extensive revisions throughout the manual) • IPSec VPN autoinitiate support (see *Manually Add or Edit a VPN Policy*) • SNMPv3 support (see *Use a Simple Network Management Protocol Manager*) • Option to reboot with a different firmware version (see *Select the Firmware and Reboot the VPN Firewall*) • Extensive list of factory default settings (see *Appendix A, Default Settings and Technical Specifications*)

202-10536-03	1.0	November 2011	Incorporated nontechnical edits only (there are no feature changes).
202-10536-02	1.0	July 2011	Added new features that are documented in the following sections: • *Configure WAN QoS Profiles* • *Inbound Rules (Port Forwarding)* and *Create LAN WAN Inbound Service Rules* • *Attack Checks* • *Set Limits for IPv4 Sessions* • *Create IP Groups* • *Use the NETGEAR VPN Client Wizard to Create a Secure Connection* • *Manually Create a Secure Connection Using the NETGEAR VPN Client* • *Configure the ProSafe VPN Client for Mode Config Operation* • *Configure Date and Time Service* • *Configure and Enable the LAN Traffic Meter*
202-10536-01	1.0	April 2010	Initial publication of this reference manual.

Contents

Chapter 3 LAN Configuration

Chapter 4 Firewall Protection

Introduction

1

This chapter provides an overview of the features and capabilities of the ProSAFE Gigabit Quad WAN SSL VPN Firewall SRX5308 and explains how to log in to the device and use its web management interface. The chapter contains the following sections:

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

Note: Firmware updates with new features and bug fixes are made available from time to time on *downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product do not match what is described in this guide, you might need to update your firmware.

What Is the ProSAFE Gigabit Quad WAN SSL VPN Firewall SRX5308?

The ProSAFE Gigabit Quad WAN SSL VPN Firewall SRX5308, hereafter referred to as the VPN firewall, connects your local area network (LAN) to the Internet through up to four external broadband access devices such as cable or DSL modems or satellite or wireless Internet dishes. Four wide area network (WAN) ports allow you to increase effective data rate to the Internet by utilizing all WAN ports to carry session traffic or to maintain backup connections in case of failure of your primary Internet connection.

The VPN firewall routes both IPv4 and IPv6 traffic. A powerful, flexible firewall protects your IPv4 and IPv6 networks from denial of service (DoS) attacks, unwanted traffic, and traffic with objectionable content. IPv6 traffic is supported through 6to4 and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels.

The VPN firewall is a security solution that protects your network from attacks and intrusions. For example, the VPN firewall provides support for stateful packet inspection (SPI), denial of service (DoS) attack protection, and multi-NAT support. The VPN firewall supports multiple web content filtering options, plus browsing activity reporting and instant alerts—both through email. Network administrators can establish restricted access policies based on time of day, website addresses, and address keywords.

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

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

Key Features and Capabilities

- *Quad-WAN Ports for Increased Reliability and Load Balancing*
- *Advanced VPN Support for Both IPSec and SSL*
- *A Powerful, True Firewall with Content Filtering*
- *Security Features*
- *Autosensing Ethernet Connections with Auto Uplink*
- *Extensive Protocol Support*
- *Easy Installation and Management*
- *Maintenance and Support*

The VPN firewall provides the following key features and capabilities:

- Four 10/100/1000 Mbps Gigabit Ethernet WAN ports for load balancing and failover protection of your Internet connection, providing increased data rate and increased system reliability.
- Built-in four-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for fast data transfer between local network resources and support for up to 200,000 internal or external connections.
- Both IPv4 and IPv6 support
- Advanced IPSec VPN and SSL VPN support with support for up to 125 concurrent IPSec VPN tunnels and up to 50 concurrent SSL VPN tunnels.
- Bundled with a single-user license of the NETGEAR ProSafe VPN Client software (VPN01L).
- L2TP tunnel and PPTP tunnel support
- Advanced stateful packet inspection (SPI) firewall with multi-NAT support.
- Quality of Service (QoS) and SIP 2.0 support for traffic prioritization, voice, and multimedia.
- Extensive protocol support.
- One console port for local management.
- SNMP support with SNMPv1, SNMPv2c, and SNMPv3, and management optimized for the NETGEAR ProSafe Network Management Software (NMS200) over a LAN connection.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.
- Internal universal switching power supply.
- Rack-mounting kit for 1U rackmounting.

Quad-WAN Ports for Increased Reliability and Load Balancing

The VPN firewall provides four broadband WAN ports. These WAN ports allow you to connect additional broadband Internet lines that can be configured to:

- Load-balance outbound traffic between up to four lines for maximum bandwidth efficiency.
- Provide backup and rollover if one line is inoperable, ensuring that you are never disconnected.

See *Appendix B, Network Planning for Multiple WAN Ports* for the planning factors to consider when implementing the following capabilities with multiple WAN port gateways:

- Single or multiple exposed hosts.
- Virtual private networks (VPNs).

Advanced VPN Support for Both IPSec and SSL

The VPN firewall 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.
  - Up to 125 simultaneous IPSec VPN connections.
  - Bundled with a 30-day trial license for the ProSafe VPN Client software (VPN01L).
- SSL VPN provides remote access for mobile users to selected corporate resources without requiring a preinstalled VPN client on their computers.
  - Uses the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, to provide client-free access with customizable user portals and support for a wide variety of user repositories.
  - Up to 50 simultaneous SSL VPN connections.
  - Allows browser-based, platform-independent remote access through a number of popular browsers, such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.
  - Provides granular access to corporate resources based on user type or group membership.

A Powerful, True Firewall with Content Filtering

Unlike simple NAT routers, the VPN firewall 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.
- **Content filtering**. Prevents objectionable content from reaching your computers. You can control access to Internet content by screening for web services, web addresses, and keywords within web addresses.
- **Schedule policies**. Permits scheduling of firewall policies by day and time.
- **Logs security incidents**. Logs security events such as logins and secure logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the VPN firewall to send immediate alert messages to your email address or email pager when a significant event occurs.

Security Features

The VPN firewall is equipped with several features designed to maintain security:

- **Computers 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 computers on the LAN, the VPN firewall allows you to direct incoming traffic to specific computers based on the service port number of the incoming request.
- **DMZ port**. Incoming traffic from the Internet is usually discarded by the VPN firewall unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can use the dedicated demilitarized zone (DMZ) port to forward the traffic to one computer on your network.

Autosensing Ethernet Connections with Auto Uplink

With its internal four-port 10/100/1000 Mbps switch and four 10/100/1000 WAN ports, the VPN firewall can connect to a 10-Mbps standard Ethernet network, a 100-Mbps Fast Ethernet network, a 1000-Mbps Gigabit Ethernet network, or a combination of these networks. All LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The VPN firewall 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 computer or an uplink connection such as to a switch or hub. That port then configures itself correctly. This feature eliminates the need for you to think about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

Extensive Protocol Support

The VPN firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). The VPN firewall provides the following protocol support:

- **IP address sharing by NAT**. The VPN firewall allows many networked computers to share an Internet account using only a single IP address, which might be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.
- **Automatic configuration of attached computers by DHCP**. The VPN firewall dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached computers on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of computers on your local network.

- **DNS proxy**. When DHCP is enabled and no DNS addresses are specified, the VPN firewall provides its own address as a DNS server to the attached computers. 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 VPN firewall supports QoS, including traffic prioritization and traffic classification with Type of Service (ToS) and Differentiated Services Code Point (DSCP) marking.
- **Layer 2 Tunneling Protocol (L2TP)**. A tunneling protocol that is used to support virtual private networks (VPNs).
- **Point to Point Tunneling Protocol (PPTP)**. Another tunneling protocol that is used to support VPNs.

Easy Installation and Management

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

- **Browser-based management**. Browser-based configuration allows you to easily configure the VPN firewall from almost any type of operating system, such as Windows, Macintosh, or Linux. Online help documentation is built into the browser-based web management interface.
- **Auto-detection of ISP**. The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **IPSec VPN Wizard**. The VPN firewall includes the NETGEAR IPSec VPN Wizard so you can easily configure IPSec VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC). This ensures that the IPSec VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.
- **SNMP**. The VPN firewall 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 VPN firewall incorporates built-in diagnostic functions such as ping, traceroute, DNS lookup, and remote reboot.
- **Remote management**. The VPN firewall allows you to log in to the web management interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.
- **Visual monitoring**. The VPN firewall'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 VPN firewall:

- Flash memory for firmware upgrades.
- Technical support seven days a week, 24 hours a day. Information about support is available on the NETGEAR website at *http://support.netgear.com/app/answers/detail/a_id/212*.

Package Contents

The VPN firewall product package contains the following items:

- ProSAFE Gigabit Quad WAN SSL VPN Firewall SRX5308
- One AC power cable
- One Category 5 (Cat 5) Ethernet cable
- One rack-mounting kit
- *ProSAFE Gigabit Quad WAN SSL VPN Firewall SRX5308 Installation Guide*
- *Resource CD*, including:
  - Application Notes and other helpful information
  - ProSafe VPN Client software (VPN01L)

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

- *Front Panel*
- *Rear Panel*
- *Bottom Panel with Product Label*

The front panel ports and LEDs, rear panel ports, and bottom label of the VPN firewall are described in the following sections.

Front Panel

Viewed from left to right, the VPN firewall front panel contains the following ports (see the following figure).

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

The front panel also contains three groups of status indicator light-emitting diodes (LEDs), including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are described in the following table.

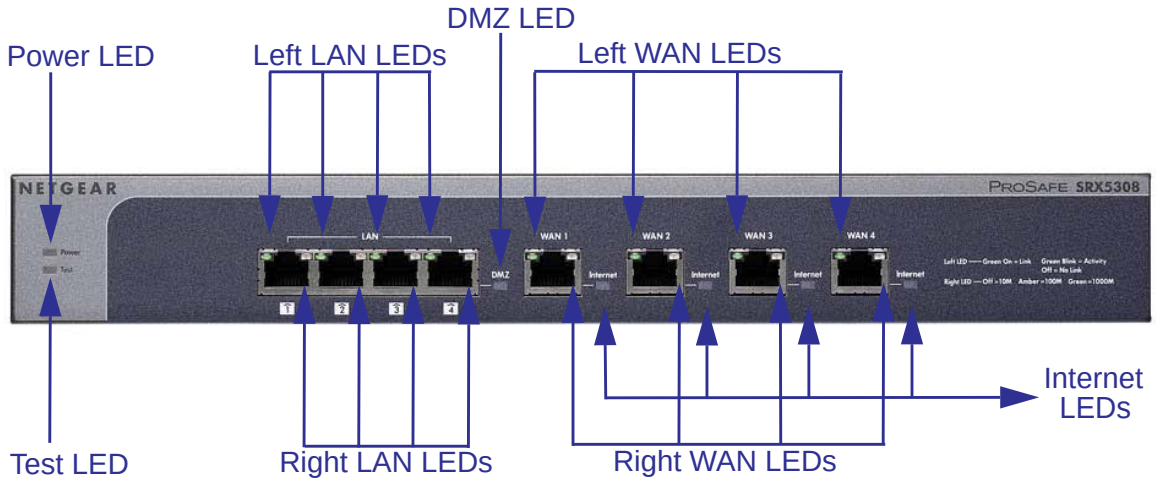

Figure 1.

Table 1. LED descriptions

LED	Activity	Description
Power	On (green)	Power is supplied to the VPN firewall.
	Off	Power is not supplied to the VPN firewall.
Test	On (amber) during startup.	Test mode: The VPN firewall is initializing. After approximately 2 minutes, when the VPN firewall has completed its initialization, the Test LED goes off.
	On (amber) during any other time	The initialization has failed, or a hardware failure has occurred.
	Blinking (amber)	The VPN firewall is writing to flash memory (during upgrading or resetting to defaults).
	Off	The system has booted successfully.
LAN Ports		
Left LED	On (green)	The LAN port has detected a link with a connected Ethernet device.
	Blinking (green)	The LAN port receives or transmits data.
	Off	The LAN port has no link.
Right LED	On (green)	The LAN port operates at 1000 Mbps.
	On (amber)	The LAN port operates at 100 Mbps.
	Off	The LAN port operates at 10 Mbps.

Table 1. LED descriptions (continued)

LED	Activity	Description
DMZ LED	On (green)	Port 4 operates as a dedicated hardware DMZ port.
	Off	Port 4 operates as a normal LAN port.
WAN Ports		
Left LED	On (green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blinking (green)	The WAN port receives or transmits data.
	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the VPN firewall.
Right LED	On (green)	The WAN port operates at 1000 Mbps.
	On (amber)	The WAN port operates at 100 Mbps.
	Off	The WAN port operates at 10 Mbps.
Internet LED	On (green)	The WAN port has a valid Internet connection.
	Off	The WAN port is either not enabled or has no link to the Internet.

Rear Panel

The rear panel of the VPN firewall includes a console port, a Factory Defaults Reset button, a cable lock receptacle, an AC power connection, and a power switch.

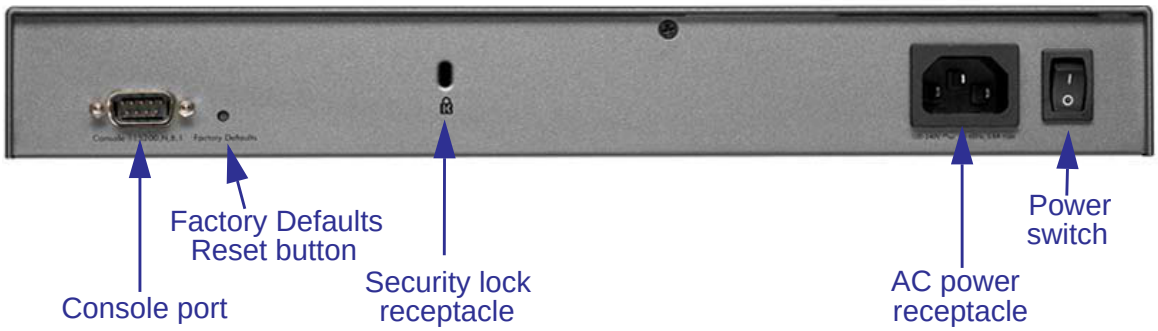

Figure 2.

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

- Cable security lock receptacle.
- Console port. Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 115200 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd. For information about accessing the command-line interface (CLI) using the console port, see *Use the Command-Line Interface* on page 342.

- Factory Defaults Reset button. Using a sharp object, press and hold this button for about 8 seconds until the front panel Test LED flashes to reset the VPN firewall to factory default settings. All configuration settings are lost, and the default password is restored.
- AC power receptacle. Universal AC input (100–240 VAC, 50–60 Hz).
- A power on/off switch.

Bottom Panel with Product Label

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

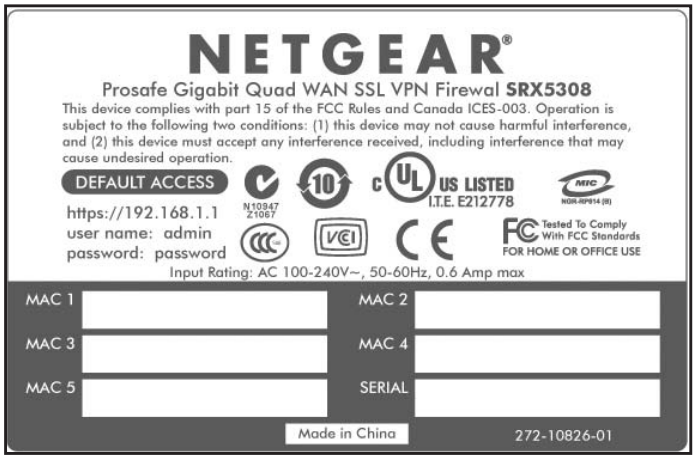

Figure 3.

Choose a Location for the VPN Firewall

The VPN firewall is suitable for use in an office environment where it can be freestanding (on its runner feet) or mounted into a standard 19-inch equipment rack. Alternatively, you can rack-mount the VPN firewall in a wiring closet or equipment room.

Consider the following when deciding where to position the VPN firewall:

- 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 VPN firewall, see *Appendix A, Default Settings and Technical Specifications*.

Use the Rack-Mounting Kit

Use the mounting kit for the VPN firewall to install the appliance in a rack. Attach the mounting brackets using the hardware that is supplied with the mounting kit.

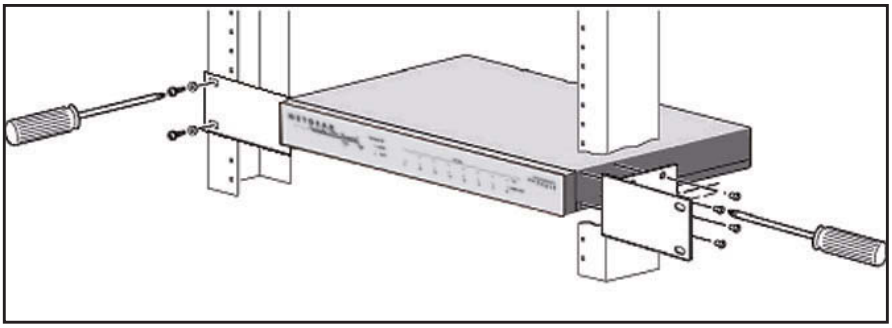

Figure 4.

Before mounting the VPN firewall in a rack, verify that:

- You have the correct screws (supplied with the installation kit).
- The rack onto which you plan to mount the VPN firewall is suitably located.

Log In to the VPN Firewall

Note: To connect the VPN firewall physically to your network, connect the cables and restart your network according to the instructions in the *ProSAFE Gigabit Quad WAN SSL VPN Firewall SRX5308 Installation Guide*. A PDF of this guide is on the NETGEAR support website at *http://kb.netgear.com/app/products/model/a_id/13568*.

To configure the VPN firewall, you need to use a web browser such as Microsoft Internet Explorer 7.0 or later, Mozilla Firefox 4.0 or later, or Apple Safari 3.0 or later with JavaScript, cookies, and SSL enabled.

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

➢ **To log in to the VPN firewall:**

1. Start any of the qualified web browsers.
2. In the address field, enter **https://192.168.1.1**. The NETGEAR Configuration Manager Login screen displays in the browser.

Note: The VPN firewall factory default IP address is 192.168.1.1. If you change the IP address, you need to use the IP address that you assigned to the VPN firewall to log in to the VPN firewall.

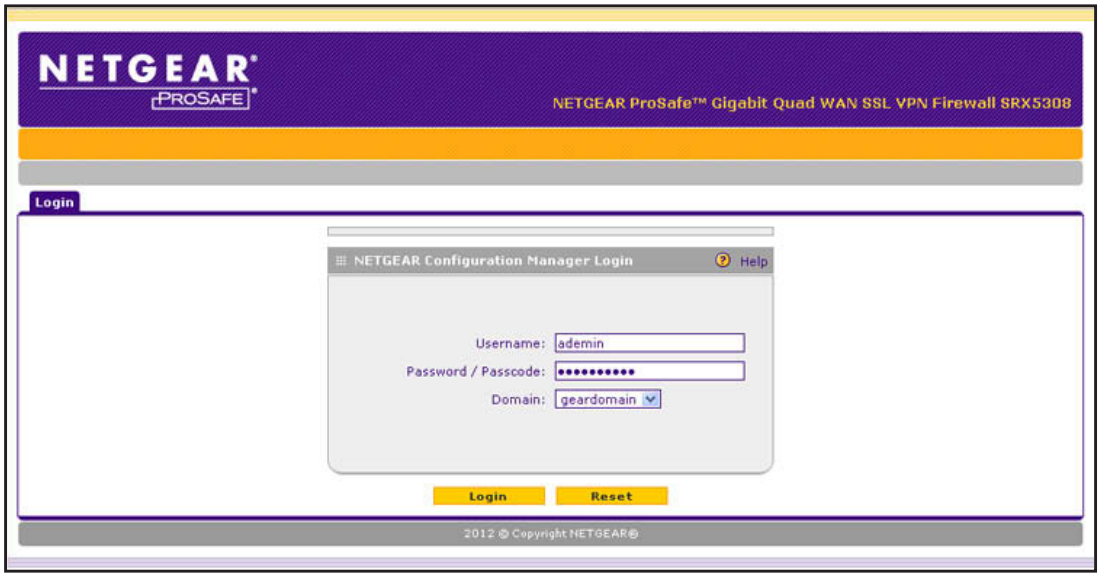

Figure 5.

Note: The first time that you remotely connect to the VPN firewall with a browser through an SSL connection, you might get a warning message regarding the SSL certificate. Follow the directions of your browser to accept the SSL certificate.

3. In the User Name field, type **admin**. Use lowercase letters.
4. In the Password / Passcode field, type **password**. Here, too, use lowercase letters.

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

Note: Leave the domain as it is (geardomain).

5. Click **Login**. The web management interface displays, showing the Router Status screen. The following figure shows the top part of the Router Status screen. For more information, see *View the System Status* on page 369.

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

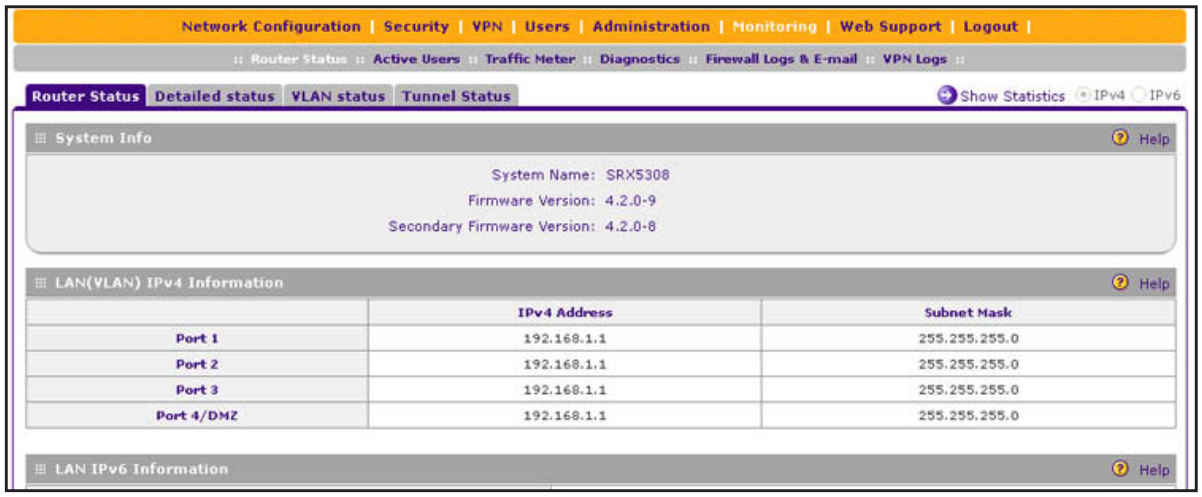

Figure 6.

Web Management Interface Menu Layout

The following figure shows the menu at the top the web management interface:

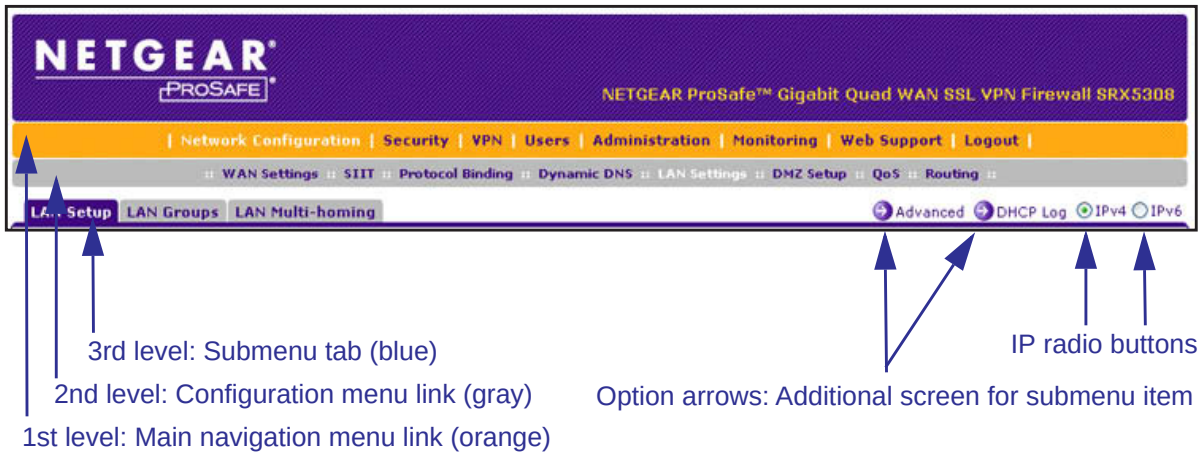

Figure 7.

The web management interface menu consists of the following components:

- **1st level: Main navigation menu links**. The main navigation menu in the orange bar across the top of the web management interface provides access to all the configuration functions of the VPN firewall, and remains constant. When you select a main navigation menu link, the letters are displayed in white against an orange background.
- **2nd level: Configuration menu links**. The configuration menu links in the gray bar (immediately below the main navigation menu bar) change according to the main navigation menu link that you select. When you select a configuration menu link, the letters are displayed in white against a gray background.
- **3rd level: Submenu tabs**. Each configuration menu item has one or more submenu tabs that are listed below the gray menu bar. When you select a submenu tab, the text is displayed in white against a blue background.
- **Option arrows**. If there are additional screens for the submenu item, links to the screens display on the right side in blue letters against a white background, preceded by a white arrow in a blue circle.
- **IP radio buttons**. The IPv4 and IPv6 radio buttons let you select the IP version for the feature to be configured onscreen. There are four options:
  - **Both buttons are operational**. 

You can configure the feature onscreen for IPv4 functionality or for IPv6 functionality. After you have correctly configured the feature for both IP versions, the feature can function with both IP versions simultaneously.
  - **The IPv4 button is operational but the IPv6 button is disabled**. 

You can configure the feature onscreen for IPv4 functionality only.
  - **The IPv6 button is operational but the IPv4 button is disabled**. 

You can configure the feature onscreen for IPv6 functionality only.
  - **Both buttons are disabled**. 

IP functionality does not apply.

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

Figure 8.

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

- **Apply**. Save and apply the configuration.
- **Reset**. Reset the configuration to the previously saved configuration.
- **Test**. Test the configuration.
- **Auto Detect**. Enable the VPN firewall to detect the configuration automatically and suggest values for the configuration.
- **Cancel**. Cancel the operation.

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

Figure 9.

Any of the following table buttons might display onscreen:

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

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

Requirements for Entering IP Addresses

To connect to the VPN firewall, your computer needs to be configured to obtain an IP address automatically from the VPN firewall, either an IPv4 address through DHCP or an IPv6 address through DHCPv6, or both.

IPv4

The fourth octet of an IP address needs to be between 0 and 255 (both inclusive). This requirement applies to any IP address that you enter on a screen of the web management interface.

IPv6

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted.

The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

2. IPv4 and IPv6 Internet and WAN Settings

This chapter explains how to configure the IPv4 and IPv6 Internet and WAN settings. The chapter contains the following sections:

Internet and WAN Configuration Tasks

- *Roadmap to Setting Up IPv4 Internet Connections to Your ISPs*
- *Roadmap to Setting Up IPv6 Internet Connections to Your ISPs*

Typically, the VPN firewall is installed as a network gateway to function as a combined LAN switch and firewall to protect the network from incoming threats and provide secure connections. To complement the firewall protection, NETGEAR advises that you use a gateway security appliance such as a NETGEAR ProSecure STM appliance.

The tasks that are required to complete the Internet connection of your VPN firewall depend on whether you use an IPv4 connection, an IPv6 connection, or both to your Internet service provider (ISP).

Note: The VPN firewall supports simultaneous IPv4 and IPv6 connections.

Roadmap to Setting Up IPv4 Internet Connections to Your ISPs

Setting up IPv4 Internet connections to your ISP or ISPs includes seven tasks, five of which are optional.

➢ **Complete these tasks:**

1. **Configure the IPv4 routing mode**. Select either NAT or classical routing.

   This task is described in *Configure the IPv4 WAN Mode* on page 29.

2. **Configure the IPv4 Internet connections to your ISPs**. Connect to one or more ISPs by configuring up to four WAN interfaces.

   You have two configuration options. These tasks are described in the following sections:

   - *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 31
   - *Manually Configure an IPv4 Internet Connection* on page 34

3. **(Optional) Configure either load balancing or auto-rollover**. By default, the WAN interfaces are configured for primary (single) WAN mode. You can select load balancing or auto-rollover and a failure detection method. If you configure load balancing, you can also configure protocol binding.

   This task is described in *Configure Load Balancing or Auto-Rollover for IPv4 Interfaces* on page 40.

4. **(Optional) Configure secondary WAN addresses on the WAN interfaces**. Configure aliases for each WAN interface.

   This task is described in *Configure Secondary WAN Addresses* on page 47.

5. **(Optional) Configure Dynamic DNS on the WAN interfaces**. If necessary, configure your fully qualified domain names.

   This task is described in *Configure Dynamic DNS* on page 49.

6. **(Optional) Configure the WAN options**. If necessary, change the factory default MTU size, port speed, and MAC address of the VPN firewall. These are advanced features, and you usually do not need to change the settings.

   This task is described in *Configure Advanced WAN Options and Other Tasks* on page 71.

7. **(Optional) Configure the WAN traffic meters**.

   This task is described in *Configure and Enable the WAN Traffic Meter* on page 356.

Roadmap to Setting Up IPv6 Internet Connections to Your ISPs

Setting up IPv6 Internet connections to your ISP or ISPs includes six tasks, four of which are optional.

➢ **Complete these tasks:**

1. **Configure the IPv6 routing mode**. Configure the VPN firewall to support both devices with IPv4 addresses and devices with IPv6 addresses.

   This task is described in *Configure the IPv6 Routing Mode* on page 53.

2. **Configure the IPv6 Internet connections to your ISPs**. Connect to an ISP by configuring a WAN interface.

   You have three configuration options. These tasks are described in the following sections:

   - *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 55
   - *Configure a Static IPv6 Internet Connection* on page 58
   - *Configure a PPPoE IPv6 Internet Connection* on page 61

3. **(Optional) Configure the IPv6 tunnels**. Enable 6to4 tunnels and configure ISATAP tunnels.

   These tasks are described in the following sections:

   - *Configure 6to4 Automatic Tunneling* on page 64
   - *Configure ISATAP Automatic Tunneling* on page 65

4. **(Optional) Configure Stateless IP/ICMP Translation (SIIT)**. Enable IPv6 devices that do not have permanently assigned IPv4 addresses to communicate with IPv4-only devices.

   This task is described in *Configure Stateless IP/ICMP Translation* on page 67.

5. **(Optional) Configure auto-rollover**. By default, the WAN interfaces are configured for primary (single) WAN mode. You can enable auto-rollover and configure the failure detection settings.

   These tasks are described in *Configure Auto-Rollover for IPv6 Interfaces* on page 68.

6. **(Optional) Configure the WAN options**. If necessary, change the factory default MTU size, port speed, and MAC address of the VPN firewall. These are advanced features, and you usually do not need to change the settings.

   These tasks are described in *Configure Advanced WAN Options and Other Tasks* on page 71.

Configure the IPv4 Internet Connection and WAN Settings

- *Configure the IPv4 WAN Mode*
- *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection*
- *Manually Configure an IPv4 Internet Connection*
- *Configure Load Balancing or Auto-Rollover for IPv4 Interfaces*
- *Configure Secondary WAN Addresses*
- *Configure Dynamic DNS*

To set up your VPN firewall for secure IPv4 Internet connections, you need to determine the IPv4 WAN mode (see the next section) and then configure the IPv4 Internet connection to your ISP on the WAN port. The web management interface offers two connection configuration options, described in the following sections:

- *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 31
- *Manually Configure an IPv4 Internet Connection* on page 34

Configure the IPv4 WAN Mode

By default, IPv4 is supported and functions in NAT mode but can also function in classical routing mode. IPv4 functions the same way in IPv4-only mode that it does in IPv4 / IPv6 mode. The latter mode adds IPv6 functionality (see *Configure the IPv6 Routing Mode* on page 53).

Network Address Translation

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

Note the following about NAT:

- The VPN firewall uses NAT to select the correct computer (on your LAN) to receive any incoming data.
- If you have only a single public Internet IP address, you need to use NAT (the default setting).

- If your ISP has provided you with multiple public IP addresses, you can use one address as the primary shared address for Internet access by your computers, and you can map incoming traffic on the other public IP addresses to specific computers on your LAN. This one-to-one inbound mapping is configured using an inbound firewall rule.

Classical Routing

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

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

To view the status of the WAN ports, you can view the Router Status screen (see *View the System Status* on page 369).

Configure the IPv4 Routing Mode

➢ **To configure the IPv4 routing mode:**

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays:

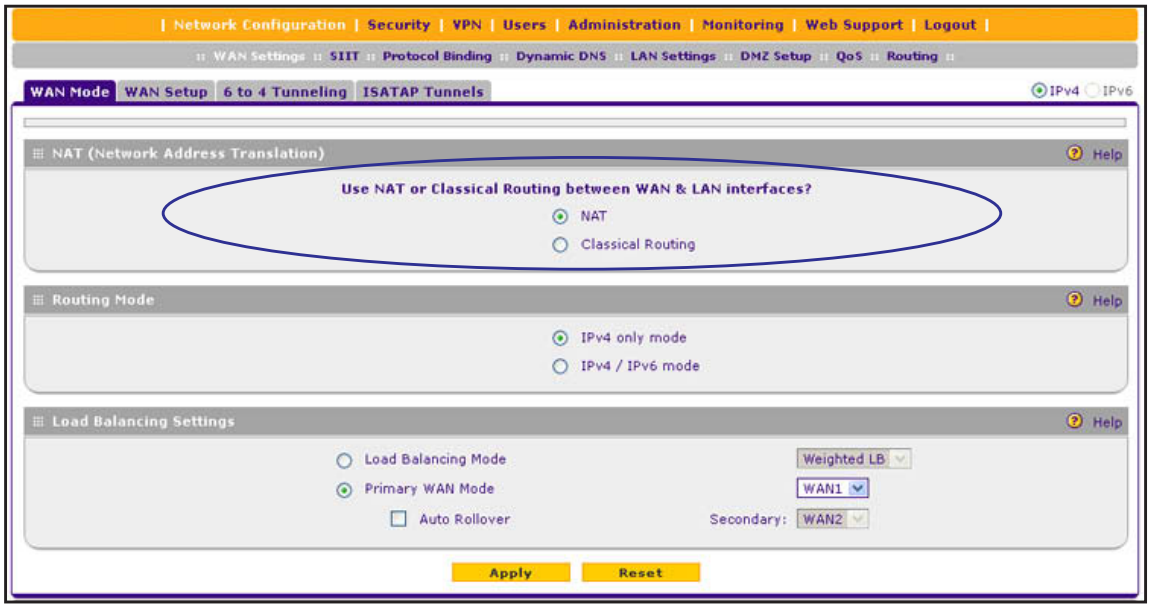

Figure 10.

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

WARNING:

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

3. Click **Apply** to save your settings. These settings apply to all WAN ports.

Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection

➢ **To automatically configure a WAN port for an IPv4 connection to the Internet:**

1. Select **Network Configuration > WAN Settings > WAN Setup**. In the upper right of the screen, the IPv4 radio button is selected by default. The WAN Setup screen displays the IPv4 settings:

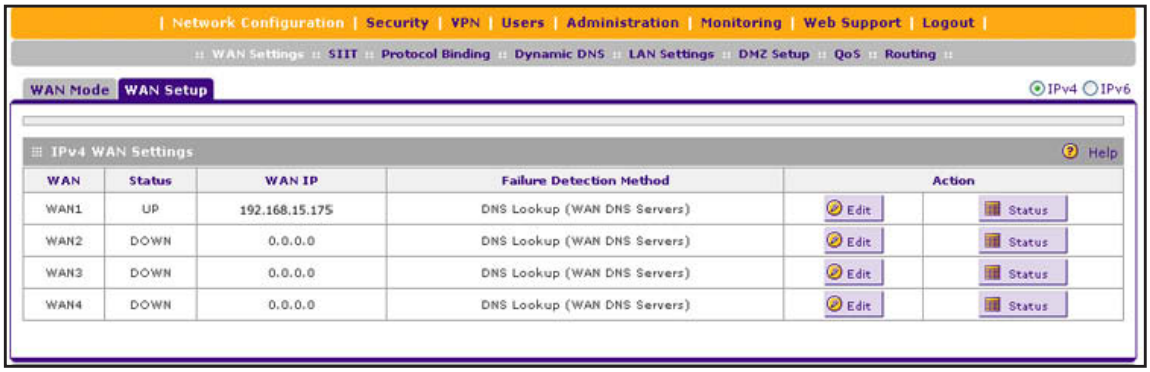

Figure 11.

The IPv4 WAN Settings table displays the following fields:

- **WAN**. The WAN interface (WAN1, WAN2, WAN3, and WAN4).
- **Status**. The status of the WAN interface (UP or DOWN).
- **WAN IP**. The IPv4 address of the WAN interface.
- **Failure Detection Method**. The failure detection method that is active for the WAN interface. The following methods can be displayed:
  - None
  - DNS Lookup (WAN DNS Servers)
  - DNS Lookup (the configured IP address is displayed)
  - PING (the configured IP address is displayed)

  You can set the failure detection method for each WAN interface on its corresponding WAN Advanced Options screen (see *Configure the Auto-Rollover Mode and Failure Detection Method for IPv4 Interfaces* on page 45).

- **Action**. The Edit table button provides access to the WAN IPv4 ISP Settings screen (see *Step 2*) for the corresponding WAN interface; the Status button provides access to the Connection Status screen (see *Step 4*) for the corresponding WAN interface.

2. Click the **Edit** table button in the Action column of the WAN interface for which you want to automatically configure the connection to the Internet. The WAN IPv4 ISP Settings screen displays. (The following figure shows the WAN2 IPv4 ISP Settings screen as an example.)

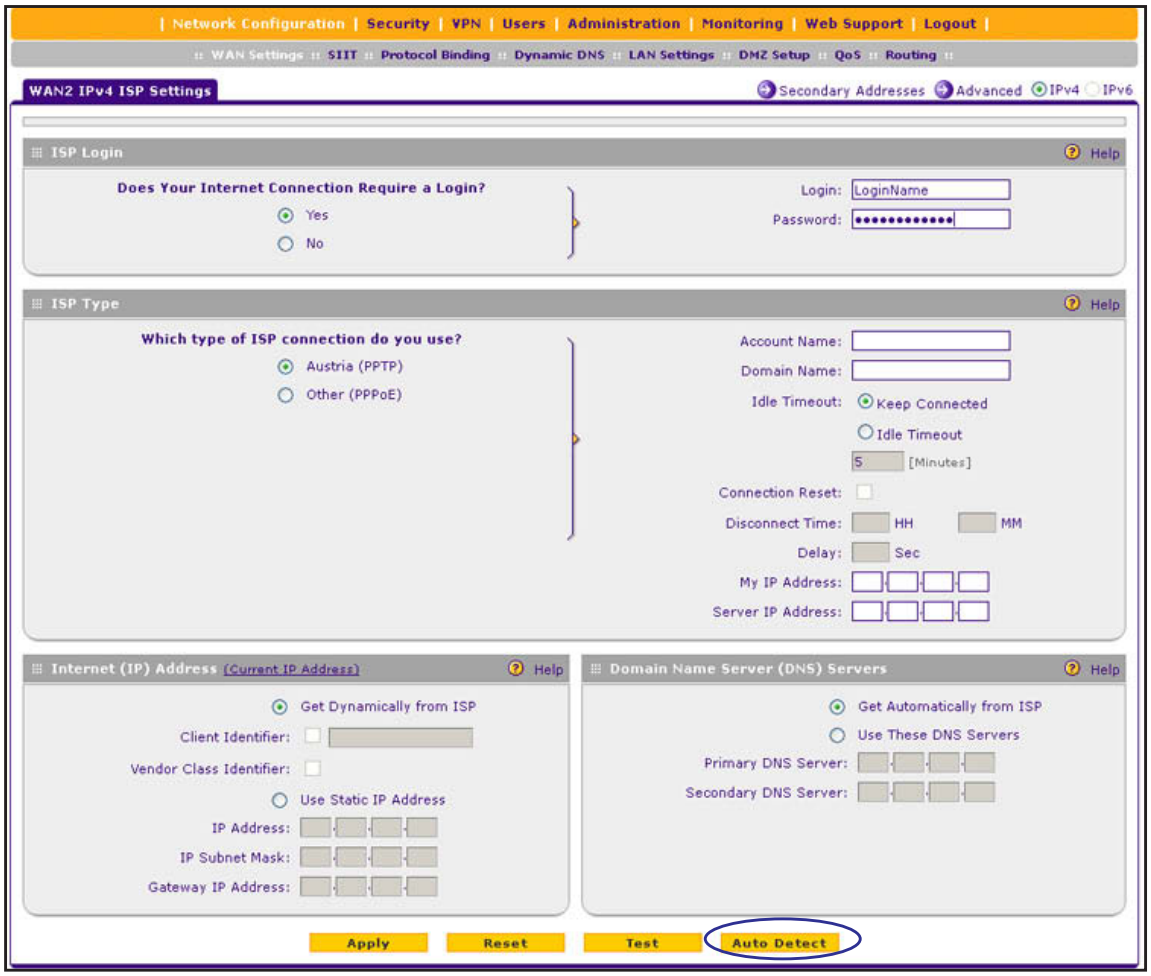

Figure 12.

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

   The autodetect process returns one of the following results:

   - If the autodetect process is successful, a status bar at the top of the screen displays the results (for example, *DHCP service detected*).
   - If the autodetect process senses a connection method that requires input from you, it prompts you for the information. The following table explains the settings that you might have to enter:

Table 2. IPv4 Internet connection methods

Connection Method	Manual Data Input Required
DHCP (Dynamic IP)	No manual data input is required.
PPPoE	The following fields are required: • Login • Password • Account Name • Domain Name
PPTP	The following fields are required: • Login • Password • Account Name • Domain Name • My IP Address • Server IP Address
Fixed (Static) IP	The following fields are required: • IP Address • IP Subnet Mask • Gateway IP Address • Primary DNS Server • Secondary DNS Server

- If the autodetect process does not find a connection, you are prompted either to check the physical connection between your VPN firewall and the cable, DSL line, or satellite or wireless Internet dish, or to check your VPN firewall's MAC address. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 71 and *Troubleshoot the ISP Connection* on page 396.

4. Verify the connection:
   a. Select **Network Configuration > WAN Settings > WAN Setup**. The WAN Setup screen displays the IPv4 settings (see *Figure 11* on page 31).
   b. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen. (The following figure shows a static IP address configuration.)

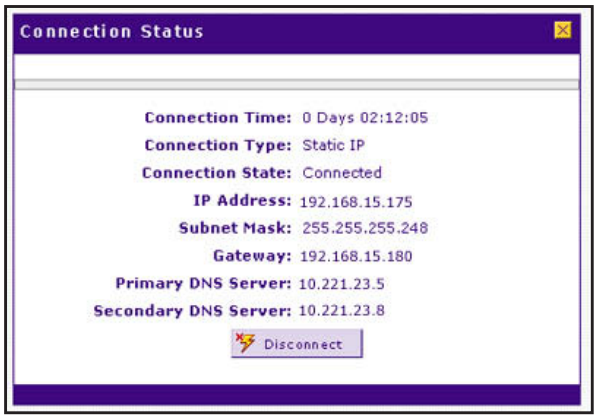

Figure 13.

The Connection Status screen should show a valid IP address and gateway, and you are connected to the Internet. If the configuration was not successful, skip ahead to *Manually Configure an IPv4 Internet Connection* on page 34, or see *Troubleshoot the ISP Connection* on page 396.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 382.

Manually Configure an IPv4 Internet Connection

Unless your ISP automatically assigns your configuration through a DHCP server, you need to obtain configuration parameters from your ISP to manually establish an Internet connection. The required parameters for various connection types are listed in *Table 2* on page 33.

➢ **To manually configure the WAN IPv4 ISP settings:**

1. Select **Network Configuration > WAN Settings > WAN Setup**. In the upper right of the screen, the IPv4 radio button is selected by default. The WAN Setup screen displays the IPv4 settings:

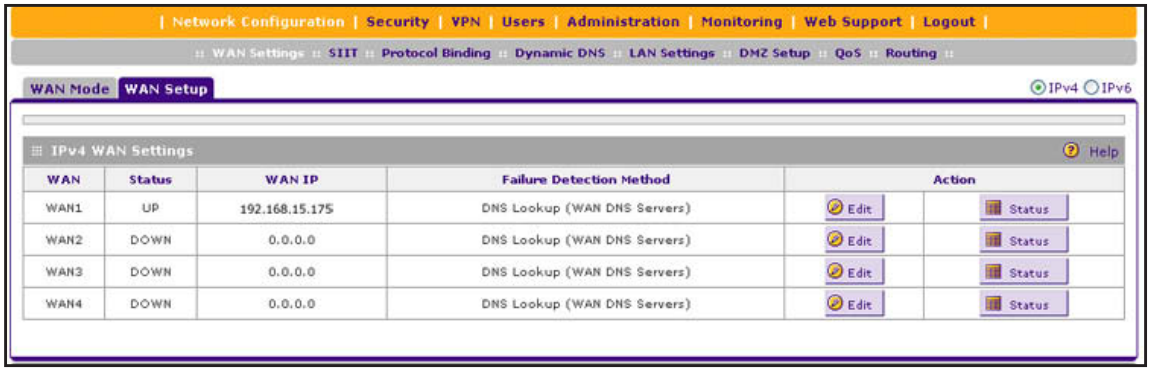

Figure 14.

The IPv4 WAN Settings table displays the following fields:

- **WAN**. The WAN interface (WAN1, WAN2, WAN3, and WAN4).
- **Status**. The status of the WAN interface (UP or DOWN).
- **WAN IP**. The IPv4 address of the WAN interface.
- **Failure Detection Method**. The failure detection method that is active for the WAN interface. The following methods can be displayed:
  - None
  - DNS Lookup (WAN DNS Servers)
  - DNS Lookup (the configured IP address is displayed)
  - PING (the configured IP address is displayed)

  You can set the failure detection method for each WAN interface on its corresponding WAN Advanced Options screen (see *Configure the Auto-Rollover Mode and Failure Detection Method for IPv4 Interfaces* on page 45).
- **Action**. The Edit table button provides access to the WAN IPv4 ISP Settings screen (see *Step 2*) for the corresponding WAN interface; the Status button provides access to the Connection Status screen (see *Step 11*) for the corresponding WAN interface.

2. Click the **Edit** table button in the Action column of the WAN interface for which you want to manually configure the connection to the Internet. The WAN IPv4 ISP Settings screen displays (see *Figure 12* on page 32, which shows the WAN2 IPv4 ISP Settings screen as an example).
3. Locate the ISP Login section on the screen:

Figure 15.

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

- If your ISP requires an initial login to establish an Internet connection, select **Yes**. (The default is No.)
- If a login is not required, select **No**, and ignore the Login and Password fields.

4. If you selected Yes, enter the login name in the Login field and the password in the Password field. This information is provided by your ISP.
5. In the ISP Type section of the screen, select the type of ISP connection that you use from the two listed options. By default, Austria (PPTP) is selected, as shown in the following figure:

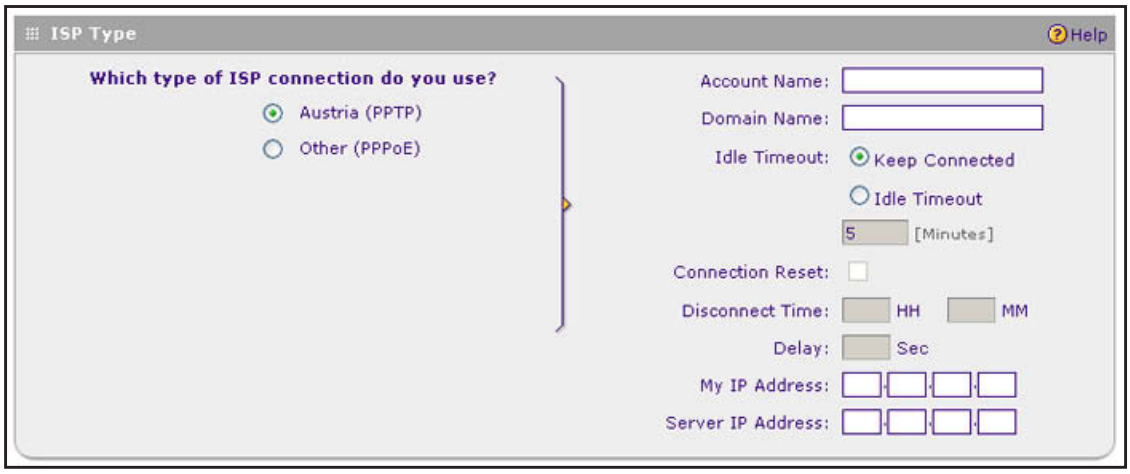

Figure 16.

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

Table 3. PPTP and PPPoE settings

Setting	Description	
Austria (PPTP) **Note:** For login and password information, see *Step 3* and *Step 4*.	If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this radio button, and enter the following settings:	
	Account Name	The account name is also known as the host name or system name. Enter the valid account name for the PPTP connection (usually your email ID assigned by your ISP). Some ISPs require you to enter your full email address here.
	Domain Name	Your domain name or workgroup name assigned by your ISP, or your ISP's domain name. You can leave this field blank.
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period, select the **Idle Timeout** radio button and, in the Idle 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.

Table 3. PPTP and PPPoE settings (continued)

Setting	Description		
Other (PPPoE) **Note:** For login and password information, see *Step 3* and *Step 4*.	If you have installed login software, your connection type is PPPoE. Select this radio button, and enter the following settings:		
	Account Name	The valid account name for the PPPoE connection.	
	Domain Name	The name of your ISP's domain or your domain name if your ISP has assigned one. You can leave this field blank.	
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period, select the **Idle Timeout** radio button and, in the Idle 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.	
	Connection Reset	Select the **Connection Reset** check box to specify a time when the PPPoE WAN connection is reset, that is, the connection is disconnected momentarily and then reestablished. Then specify the disconnect time and delay.	
		Disconnect Time	Specify the hour and minutes when the connection should be disconnected.
		Delay	Specify the period in seconds after which the connection should be reestablished.

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

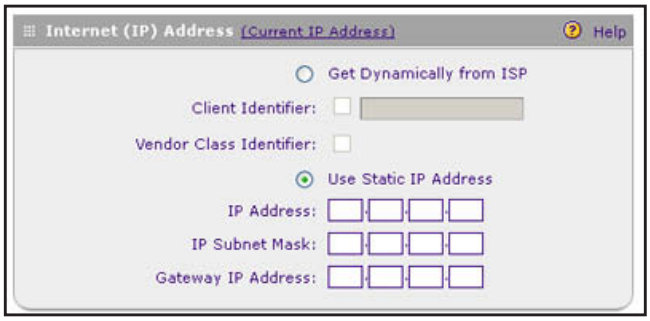

Figure 17.

Table 4. Internet IP address settings

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

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

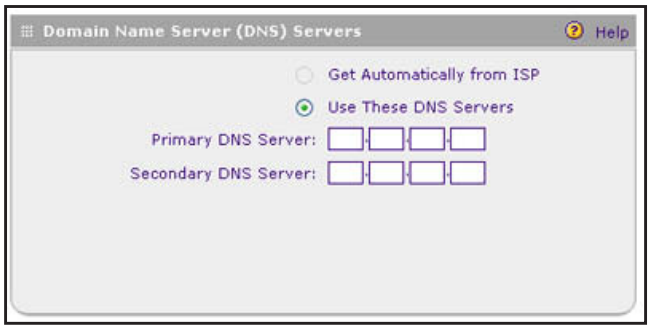

Figure 18.

Table 5. DNS server settings

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

9. Click **Apply** to save your changes.
10. Click **Test** to evaluate your entries. The VPN firewall attempts to make a connection according to the settings that you entered.
11. Verify the connection:
    a. Select **Network Configuration > WAN Settings > WAN Setup**. The WAN Setup screen displays the IPv4 settings (see *Figure 14* on page 34).
    b. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen. (The following figure shows a PPPoE configuration; the IP addresses are not related to any other examples in this manual.)

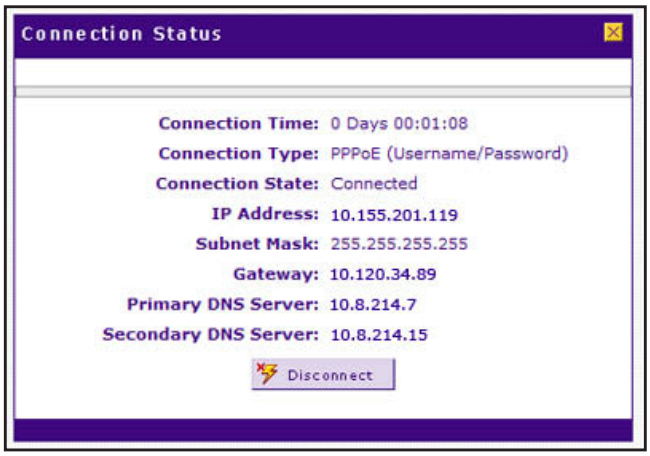

Figure 19.

The Connection Status screen should show a valid IP address and gateway, and you are connected to the Internet. If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 396.

Note: If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, you need to enter that address on the WAN Advanced Options screen for the WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 71).

Configure Load Balancing or Auto-Rollover for IPv4 Interfaces

You can configure the VPN firewall's IPv4 interfaces on a mutually exclusive basis for either auto-rollover (for increased system reliability) or load balancing (for maximum bandwidth efficiency). If you do not select load balancing, you need to specify one WAN interface as the primary interface.

The VPN firewall supports the following modes for IPv4 interfaces:

- **Load balancing mode**. The VPN firewall distributes the outbound traffic equally among the WAN interfaces that are functional. You can configure up to four WAN interfaces. The VPN firewall supports weighted load balancing and round-robin load balancing (see *Configure Load Balancing Mode and Optional Protocol Binding for IPv4 Interfaces* on page 41).

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

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

  If you want to use a redundant ISP link for backup purposes, select the WAN port that should function 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 Advanced Options screen to support auto-rollover (see *Configure the Auto-Rollover Mode and Failure Detection Method for IPv4 Interfaces* on page 45).

  Note: If the VPN firewall functions in IPv4 / IPv6 mode, you cannot configure load balancing.

Configure Load Balancing Mode and Optional Protocol Binding for IPv4 Interfaces

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

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

Protocol binding addresses two issues:

- Segregation of traffic between links that are not of the same speed.
  High-volume traffic can be routed through the WAN port connected to a high-speed link, and low-volume traffic can be routed through the WAN port connected to the low-speed link.
- Continuity of source IP address for secure connections.
  Some services, particularly HTTPS, cease to respond when a client's source IP address changes shortly after a session has been established.

Configure Load Balancing Mode for IPv4 Interfaces

➢ **To configure load balancing mode:**

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays:

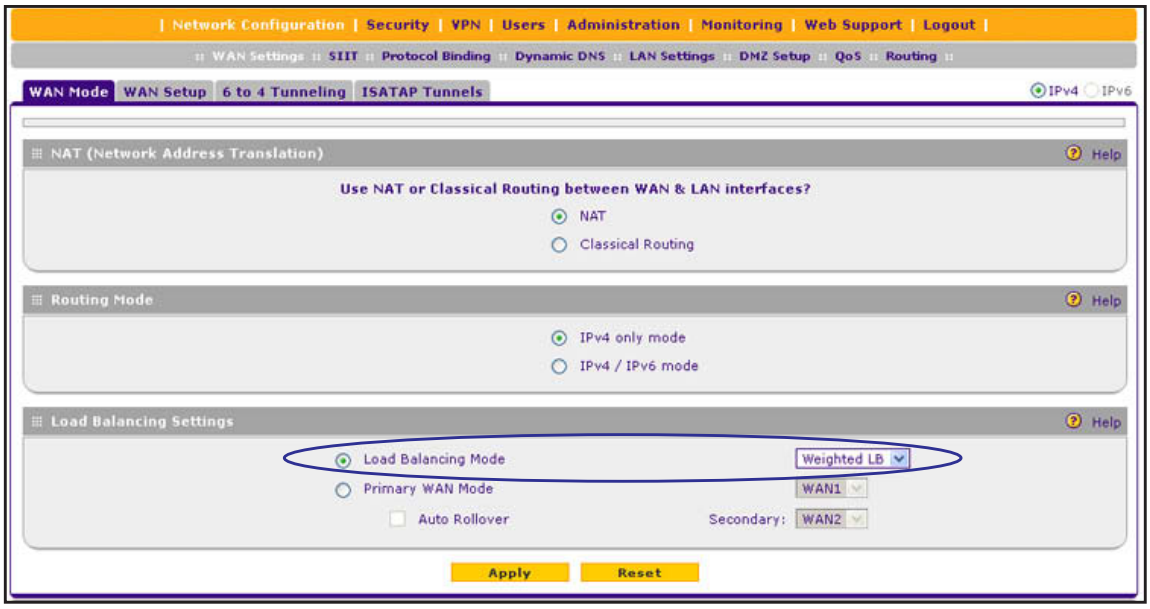

Figure 20.

2. In the Load Balancing Settings section of the screen, configure the following settings:
   a. Select the **Load Balancing Mode** radio button.

b. From the corresponding drop-down list on the right, select one of the following load balancing methods:

- **Weighted LB**. With weighted load balancing, balance weights are calculated based on WAN link speed and available WAN bandwidth. This is the default setting and most efficient load balancing algorithm.
- **Round-robin**. With round-robin load balancing, new traffic connections are sent over a WAN link in a serial method irrespective of bandwidth or link speed. For example, if the WAN1, WAN2, and WAN3 interfaces are active in round-robin load balancing mode, an HTTP request could first be sent over the WAN1 interface, then a new FTP session could start on the WAN2 interface, and then any new connection to the Internet could be made on the WAN3 interface. This load balancing method ensures that a single WAN interface does not carry a disproportionate distribution of sessions.

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

Configure Protocol Binding for IPv4 Interfaces (Optional)

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

1. Select **Network Configuration > Protocol Binding**.
2. Select the **Load Balancing** radio button. The Protocol Bindings screen displays. (The following figure shows two examples in the Protocol Bindings table.)

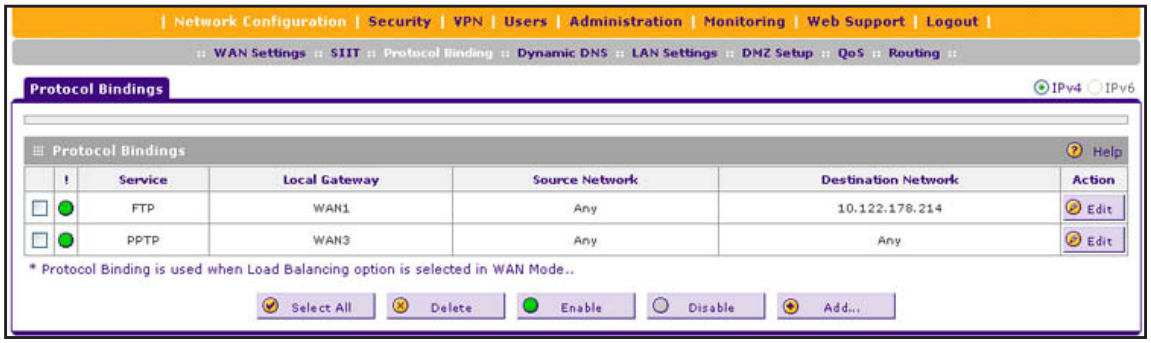

Figure 21.

The Protocol Bindings table displays the following fields:

- **Check box**. Allows you to select the protocol binding rule in the table.
- **Status icon**. Indicates the status of the protocol binding rule:
  - Green circle. The protocol binding rule is enabled.
  - Gray circle. The protocol binding rule is disabled.
- **Service**. The service or protocol for which the protocol binding rule is set up.
- **Local Gateway**. The WAN interface to which the service or protocol is bound.
- **Source Network**. The computers or groups on your network that are affected by the protocol binding rule.

- **Destination Network**. The Internet locations (based on their IP address) or groups that are covered by the protocol binding rule.
- **Action**. The Edit table button, which provides access to the Edit Protocol Binding screen for the corresponding service.

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

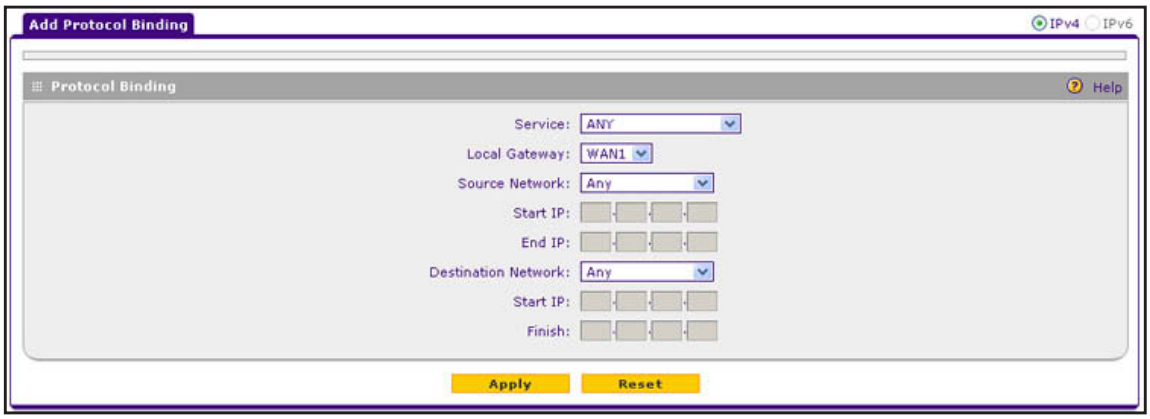

Figure 22.

4. Configure the protocol binding settings as described in the following table:

Table 6. Add Protocol Binding screen settings

Setting	Description	
Service	From the drop-down list, select a service or application to be covered by this rule. If the service or application does not appear in the list, you need to define it using the Services screen (see *Add Customized Services* on page 177).	
Local Gateway	From the drop-down list, select one of the WAN interfaces.	
Source Network	The source network settings determine which computers on your network are affected by this rule. Select one of the following options from the drop-down list:	
	Any	All devices on your LAN.
	Single address	In the Start IP field, enter the IP address to which the rule is applied.
	Address Range	In the Start IP field and End IP field, enter the IP addresses for the range to which the rule is applied.
	Group	If this option is selected, the rule is applied to the selected group. The group can be a LAN group or an IP (LAN) group. **Note:** For information about LAN groups, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 96. For information about IP groups, see *Create IP Groups* on page 179.

Table 6. Add Protocol Binding screen settings (continued)

Setting	Description	
Destination Network	The destination network settings determine which Internet locations (based on their IP address) are covered by the rule. Select one of the following options from the drop-down list:	
	Any	All Internet IP address.
	Single address	In the Start IP field, enter the IP address to which the rule is applied.
	Address range	In the Start IP field and Finish field, enter the IP addresses for the range to which the rule is applied.
	Group	If this option is selected, the rule is applied to the selected IP (WAN) group. **Note:** For information about IP groups, see *Create IP Groups* on page 179.

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

➢ **To edit a protocol binding:**

1. On the Protocol Bindings screen (see *Figure 21* on page 42), in the Protocol Bindings table, click the **Edit** table button to the right of the binding that you want to edit. The Edit Protocol Bindings screen displays. This screen shows the same fields as the Add Protocol Bindings screen (see the previous figure).
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

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

1. On the Protocol Bindings screen (see *Figure 21* on page 42), select the check box to the left of the protocol binding that you want to enable, disable, or delete, or click the **Select All** table button to select all bindings.
2. Click one of the following table buttons:
   - **Enable**. Enables the binding or bindings. The ! status icon changes from a gray circle to a green circle, indicating that the selected binding or bindings are enabled. (By default, when a binding is added to the table, it is automatically enabled.)
   - **Disable**. Disables the binding or bindings. The ! status icon changes from a green circle to a gray circle, indicating that the selected binding or bindings are disabled.
   - **Delete**. Deletes the binding or bindings.

Configure the Auto-Rollover Mode and Failure Detection Method for IPv4 Interfaces

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

When the VPN firewall is configured in auto-rollover mode, it uses the selected WAN failure detection method to detect the status of the primary link connection at regular intervals. For IPv4 interfaces, the VPN firewall detects link failure in one of the following ways:

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

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

Configure Auto-Rollover Mode for IPv4 Interfaces

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

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays:

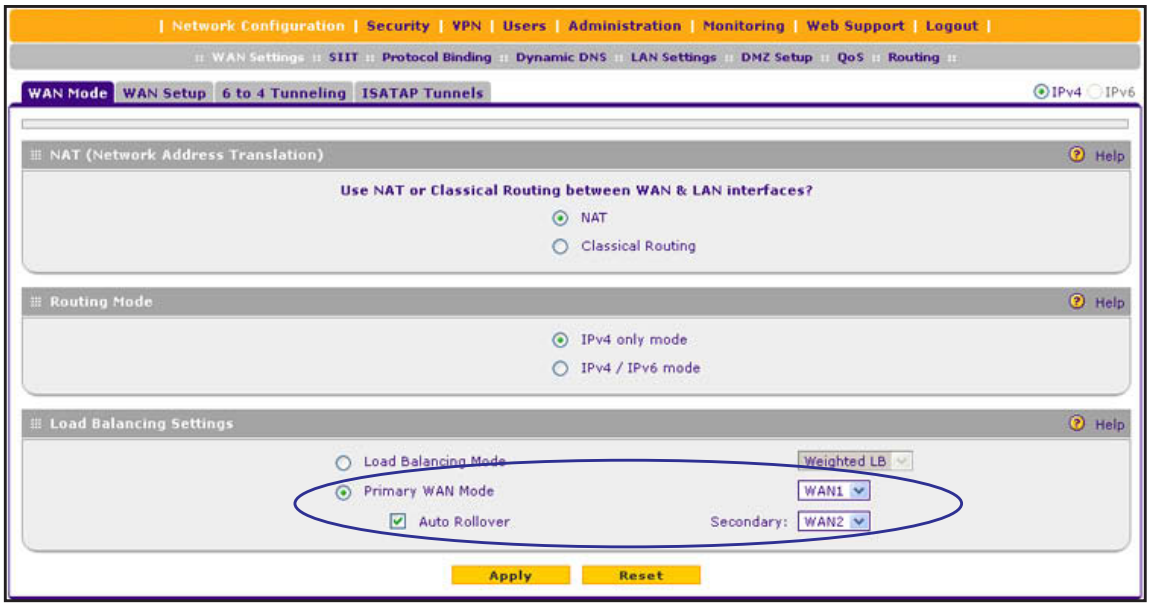

Figure 23.

2. In the Load Balancing Settings section of the screen, configure the following settings:
   a. Select the **Primary WAN Mode** radio button.
   b. From the corresponding drop-down list on the right, select a WAN interface to function as the primary WAN interface. The other WAN interfaces become disabled.
   c. Select the **Auto Rollover** check box.
   d. From the corresponding drop-down list on the right, select a WAN interface to function as the backup WAN interface.

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

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

Configure the Failure Detection Method for IPv4 Interfaces

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

1. Select **Network Configuration > WAN Settings > WAN Setup**. In the upper right of the screen, the IPv4 radio button is selected by default. The WAN Setup screen displays the IPv4 settings (see *Figure 11* on page 31).
2. Click the **Edit** table button in the Action column of the WAN interface that you selected as the primary WAN interface. The WAN IPv4 ISP Settings screen displays (see *Figure 12* on page 32, which shows the WAN2 IPv4 ISP Settings screen as an example).
3. Click the **Advanced** option arrow in the upper right of the screen. The WAN Advanced Options screen displays for the WAN interface that you selected. (For an image of the entire screen, see *Figure 46* on page 73).
4. Locate the Failure Detection Method section on the screen. Enter the settings as described in the following table.

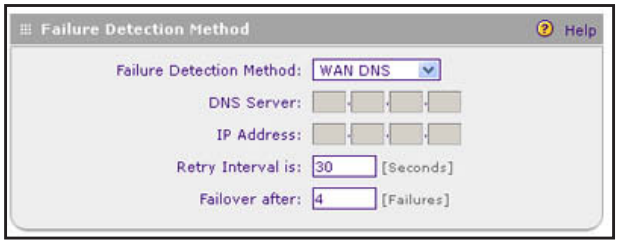

Figure 24.

Table 7. Failure detection method settings

Setting	Description
Failure Detection Method	Select a failure detection method from the drop-down list: • **WAN DNS**. DNS queries are sent to the DNS server that is configured in the Domain Name Server (DNS) Servers section of the WAN ISP screen (see *Manually Configure an IPv4 Internet Connection* on page 34). • **Custom DNS**. DNS queries are sent to a DNS server that you need to specify in the DNS Server fields. • **Ping**. Pings are sent to a public IP address that you need to specify in the IP Address field. **Note:** DNS queries or pings are sent through the WAN interface that is being monitored. The retry interval and number of failover attempts determine how quickly the VPN firewall switches from the primary link to the backup link if the primary link fails, or when the primary link comes back up, switches back from the backup link to the primary link.
DNS Server	The IP address of the DNS server.
IP Address	The IP address of the interface that should receive the ping request. The interface should not reject the ping request and should not consider ping traffic to be abusive.
Retry Interval is	The retry interval in seconds. The DNS query or ping is sent after every retry interval. The default retry interval is 30 seconds.
Failover after	The number of failover attempts. The primary WAN interface is considered down after the specified number of queries have failed to elicit a reply. The backup interface is brought up after this situation has occurred. The failover default is 4 failures.

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

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

You can configure the VPN firewall to generate a WAN status log and email this log to a specified address (see *Configure Logging, Alerts, and Event Notifications* on page 362).

Configure Secondary WAN Addresses

You can set up a single WAN Ethernet port to be accessed through multiple IPv4 addresses by adding aliases to the port. An alias is a secondary WAN address. One advantage is, for example, that you can assign different virtual IP addresses to a web server and an FTP server, even though both servers use the same physical IP address. You can add several secondary IP addresses to a single WAN port.

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

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

For more information about firewall rules, see *Overview of Rules to Block or Allow Specific Kinds of Traffic* on page 136).

Note: 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 VPN firewall. However, primary and secondary WAN addresses can be in the same subnet.

The following is an example of correctly configured IP addresses:

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 Configuration > WAN Settings > WAN Setup**. In the upper right of the screen, the IPv4 radio button is selected by default. The WAN Setup screen displays the IPv4 settings (see *Figure 11* on page 31).
2. Click the **Edit** table button in the Action column of the WAN interface for which you want to add a secondary WAN address. The WAN IPv4 ISP Settings screen displays (see *Figure 12* on page 32, which shows the WAN2 IPv4 ISP Settings screen as an example).
3. Click the **Secondary Addresses** option arrow in the upper right of the screen. The WAN Secondary Addresses screen displays for the WAN interface that you selected. (The following figure shows the WAN1 Secondary Addresses screen as an example and includes one entry in the List of Secondary WAN addresses table.)

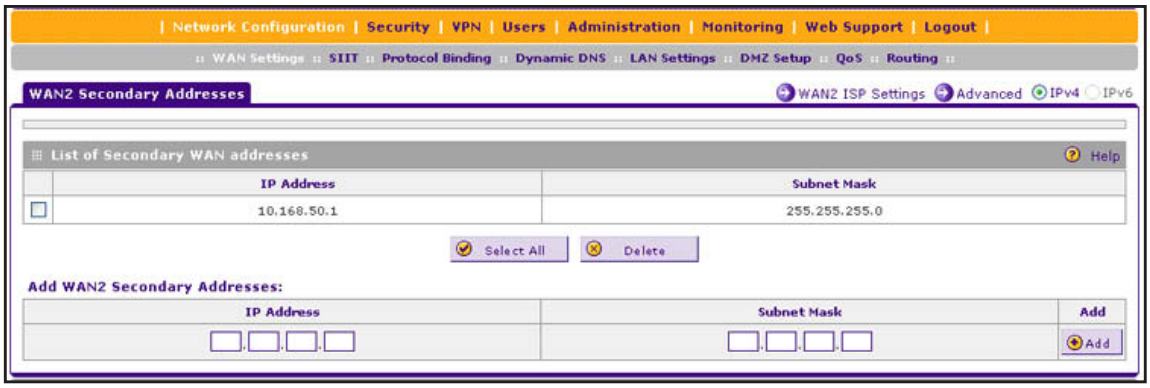

Figure 25.

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

4. In the Add WAN Secondary Addresses section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the WAN port.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.
5. Click the **Add** table button in the rightmost column to add the secondary IP address to the List of Secondary WAN addresses table.
6. (Optional) Repeat *Step 4* and *Step 5* for each secondary IP address that you want to add to the List of Secondary WAN addresses table.

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

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

Configure Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows devices with varying public IPv4 addresses to be located using Internet domain names. To use DDNS, you need to set up an account with a DDNS provider such as DynDNS.org, TZO.com, Oray.net, or 3322.org. (Links to DynDNS, TZO, Oray, and 3322 are provided for your convenience as option arrows on the DDNS configuration screens.) The VPN firewall firmware includes software that notifies DDNS servers of changes in the WAN IP address so that the services running on this network can be accessed by others on the Internet.

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

After you have configured your account information on the VPN firewall, when your ISP-assigned IP address changes, your VPN firewall 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 DDNS service does not work because private addresses are not routed on the Internet.

➢ **To configure DDNS:**

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

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

2. Click the submenu tab for your DDNS service provider:
   - **Dynamic DNS** for DynDNS.org (which is shown in the following figure)
   - **DNS TZO** for TZO.com
   - **DNS Oray** for Oray.net
   - **3322 DDNS** for 3322.org

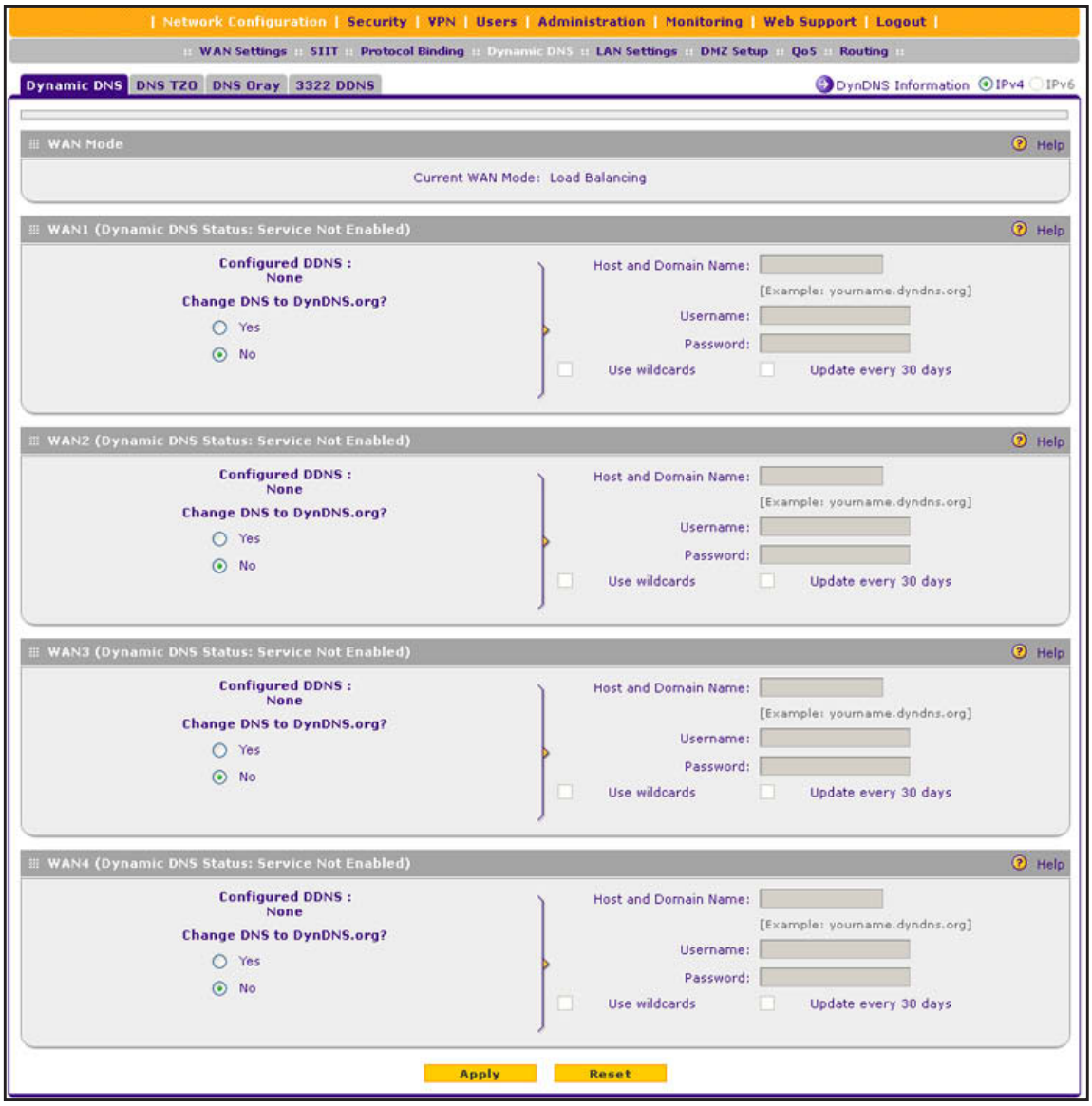

Figure 26.

3. Click the **Information** option arrow in the upper right of a DNS screen for registration information (for example, DynDNS Information).

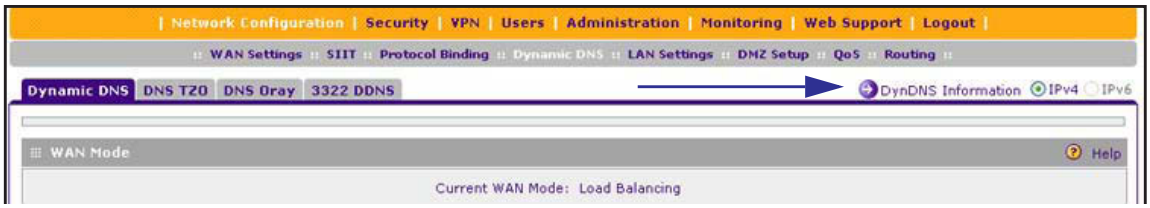

Figure 27.

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

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

Table 8. DDNS service settings

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

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

Configure the IPv6 Internet Connection and WAN Settings

- *Configure the IPv6 Routing Mode*
- *Use a DHCPv6 Server to Configure an IPv6 Internet Connection*
- *Configure a Static IPv6 Internet Connection*
- *Configure a PPPoE IPv6 Internet Connection*
- *Configure 6to4 Automatic Tunneling*
- *Configure ISATAP Automatic Tunneling*
- *View the Tunnel Status and IPv6 Addresses*
- *Configure Stateless IP/ICMP Translation*

Note: You can configure only one WAN interface for IPv6. This restriction might be lifted in a later release. You can configure the other three WAN interfaces for IPv4.

The nature of your IPv6 network determines how you need to configure the IPv6 Internet connections:

- **Native IPv6 network**. Your network is a native IPv6 network if the VPN firewall has an IPv6 address and is connected to an IPv6 ISP and if your network consists of IPv6-only devices. However, because we are in a IPv4-to-IPv6 transition period, native IPv6 is not yet common.
- **Isolated IPv6 network**. If your network is an isolated IPv6 network that is not connected to an IPv6 ISP, you need to make sure that the IPv6 packets can travel over the IPv4 Internet backbone; you do this by enabling automatic 6to4 tunneling (see *Configure 6to4 Automatic Tunneling* on page 64).
- **Mixed network with IPv4 and IPv6 devices**. If your network is an IPv4 network that consists of both IPv4 and IPv6 devices, you need to make sure that the IPv6 packets can travel over the IPv4 intranet; you do this by enabling and configuring ISATAP tunneling (see *Configure ISATAP Automatic Tunneling* on page 65).

Note: A network can be both an isolated IPv6 network and a mixed network with IPv4 and IPv6 devices.

After you have configured the IPv6 routing mode (see the next section), you need to configure one or more WAN interfaces with a global unicast address to enable secure IPv6 Internet connections on your VPN firewall. A global unicast address is a public and routable IPv6 WAN address that can be statically or dynamically assigned. The web management interface offers two connection configuration options:

- Automatic configuration of the network connection (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 55)
- Manual configuration of the network connection (see *Configure a Static IPv6 Internet Connection* on page 58 or *Configure a PPPoE IPv6 Internet Connection* on page 61)

Configure the IPv6 Routing Mode

By default the VPN firewall supports IPv4 only. To use IPv6, you need to enable the VPN firewall to support both devices with IPv4 addresses and devices with IPv6 addresses. The routing mode does not include an IPv6-only option; however, you can still configure a native IPv6 network if your ISP supports IPv6.

These are the options:

- **IPv4-only mode**. The VPN firewall communicates only with devices that have IPv4 addresses.
- **IPv4/IPv6 mode**. The VPN firewall communicates with both devices that have IPv4 addresses and devices that have IPv6 addresses.

Note: IPv6 always functions in classical routing mode between the WAN interface and the LAN interfaces; NAT does not apply to IPv6.

Note: When the Load Balancing Mode radio button is selected in the Load Balancing Settings section of the WAN Mode screen, the IPv4 / IPv6 mode radio button is dimmed, preventing you from selecting it. You can select the IPv4 / IPv6 mode radio button only when the Primary WAN Mode radio button is selected.

➢ **To configure the IPv6 routing mode:**

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays:

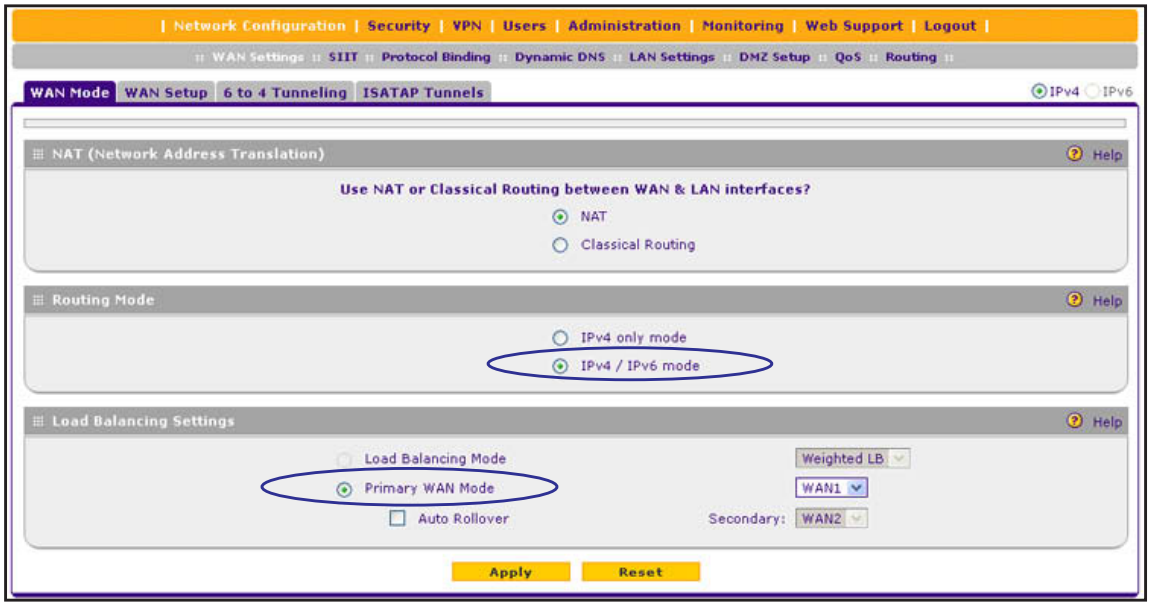

Figure 28.

2. In the Routing Mode section of the screen, select the **IPv4 / IPv6 mode** radio button. By default, the IPv4 only mode radio button is selected, and IPv6 is disabled.

WARNING:

Changing the IP routing mode causes the VPN firewall to reboot.

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

Use a DHCPv6 Server to Configure an IPv6 Internet Connection

The VPN firewall can autoconfigure its ISP settings through a DHCPv6 server by using either stateless or stateful address autoconfiguration:

- **Stateless address autoconfiguration**. The VPN firewall generates its own IP address by using a combination of locally available information and router advertisements, but receives DNS server information from a DHCPv6 server.

  Router advertisements include a prefix that identifies the subnet that is associated with the WAN port. The IP address is formed by combining this prefix and the MAC address of the WAN port. The IP address is a dynamic address.

  As an option for stateless address autoconfiguration, the ISP's *stateful* DHCPv6 server can assign a prefix through prefix delegation. The VPN firewall's own *stateless* DHCPv6 server can assign this prefix to its IPv6 LAN clients. For more information about prefix delegation, see *Stateless DHCPv6 Server With Prefix Delegation* on page 103.

- **Stateful address autoconfiguration**. The VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from a DHCPv6 server. The IP address is a dynamic address.

➢ **To automatically configure a WAN interface for an IPv6 connection to the Internet:**

1. Select **Network Configuration > WAN Settings > WAN Setup**.
2. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings:

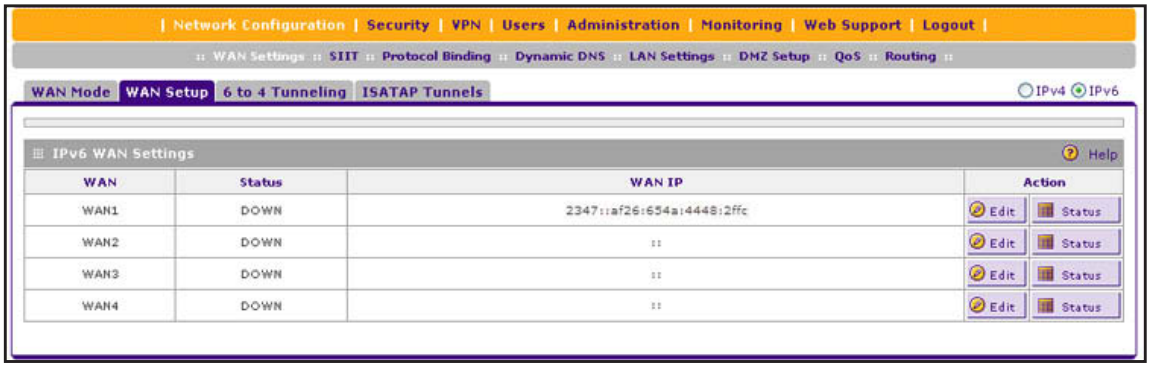

Figure 29.

The IPv6 WAN Settings table displays the following fields:

- **WAN**. The WAN interface (WAN1, WAN2, WAN3, and WAN4).
- **Status**. The status of the WAN interface (UP or DOWN).
- **WAN IP**. The IPv6 address of the WAN interface.
- **Action**. The Edit table button provides access to the WAN IPv6 ISP Settings screen (see *Step 3*) for the corresponding WAN interface; the Status button provides access to the Connection Status screen (see *Step 8*) for the corresponding WAN interface.

3. Click the **Edit** table button in the Action column of the WAN interface for which you want to automatically configure the connection to the Internet. The WAN IPv6 ISP Settings screen displays. (The following figure shows the WAN2 IPv6 ISP Settings screen as an example.)

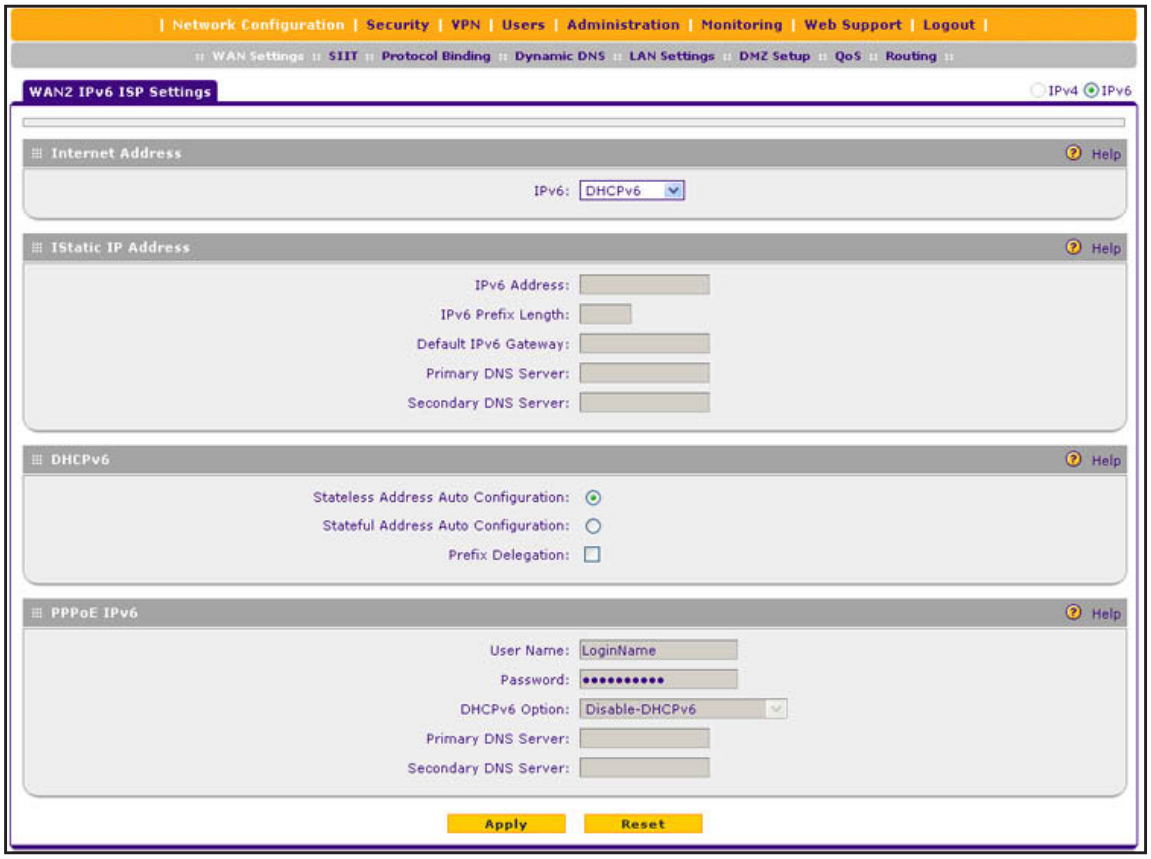

Figure 30.

4. In the Internet Address section of the screen, from the IPv6 drop-down list, select **DHCPv6**.
5. In the DHCPv6 section of the screen, select one of the following radio buttons:
   - **Stateless Address Auto Configuration**
   - **Stateful Address Auto Configuration**

6. As an optional step: If you have selected the Stateless Address Auto Configuration radio button, you can select the Prefix Delegation check box:
   - **Prefix delegation check box is selected**. A prefix is assigned by the ISP's *stateful* DHCPv6 server through prefix delegation, for example, 2001:db8:: /64. The VPN firewall's own *stateless* DHCPv6 server can assign this prefix to its IPv6 LAN clients. For more information about prefix delegation, see *Stateless DHCPv6 Server With Prefix Delegation* on page 103.
   - **Prefix delegation check box is cleared**. Prefix delegation is disabled. This is the default setting.
7. Click **Apply** to save your changes.
8. Verify the connection:
   a. Select **Network Configuration > WAN Settings > WAN Setup**.
   b. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings (see *Figure 29* on page 55).
   c. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen. (The following figure shows a dynamic IP address configuration.)

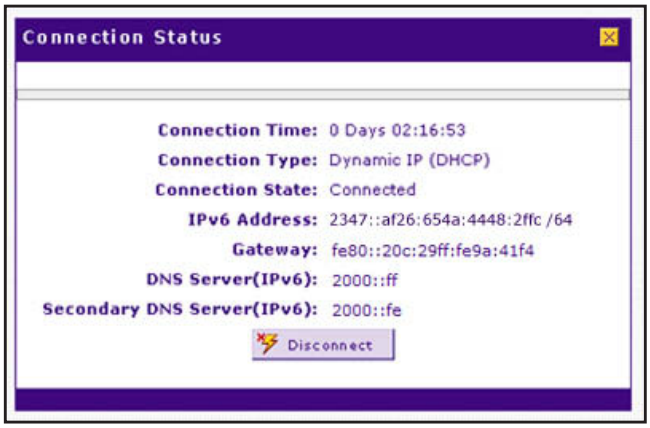

Figure 31.

The Connection Status screen should show a valid IP address and gateway, and you are connected to the Internet. If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 396.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 382.

Configure a Static IPv6 Internet Connection

To configure a static IPv6 or PPPoE IPv6 Internet connection, you need to enter the IPv6 address information that you should have received from your ISP.

➢ **To configure static IPv6 ISP settings for a WAN interface:**

1. Select **Network Configuration > WAN Settings > WAN Setup**.
2. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings:

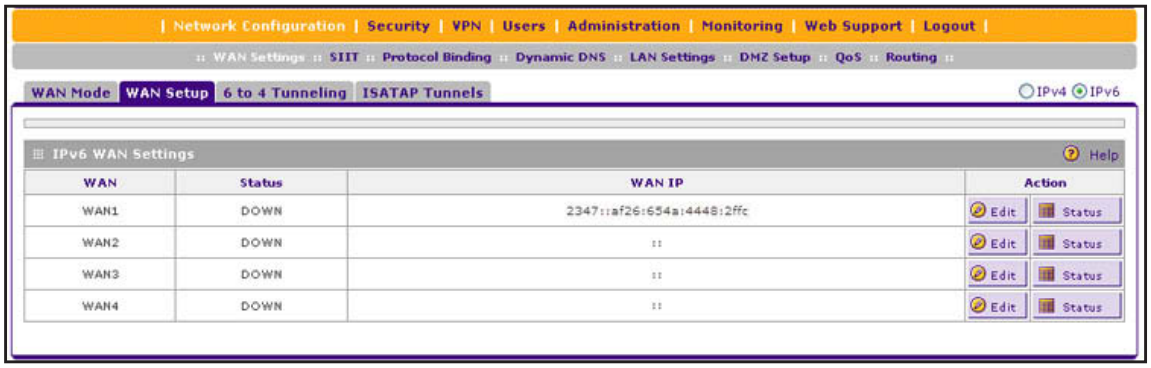

Figure 32.

The IPv6 WAN Settings table displays the following fields:

- **WAN**. The WAN interface (WAN1, WAN2, WAN3, and WAN4).
- **Status**. The status of the WAN interface (UP or DOWN).
- **WAN IP**. The IPv6 address of the WAN interface.
- **Action**. The Edit table button provides access to the WAN IPv6 ISP Settings screen (see *Step 3*) for the corresponding WAN interface; the Status button provides access to the Connection Status screen (see *Step 7*) for the corresponding WAN interface.

3. Click the **Edit** table button in the Action column of the WAN interface for which you want to automatically configure the connection to the Internet. The WAN IPv6 ISP Settings screen displays. (The following figure shows the WAN2 IPv6 ISP Settings screen as an example.)

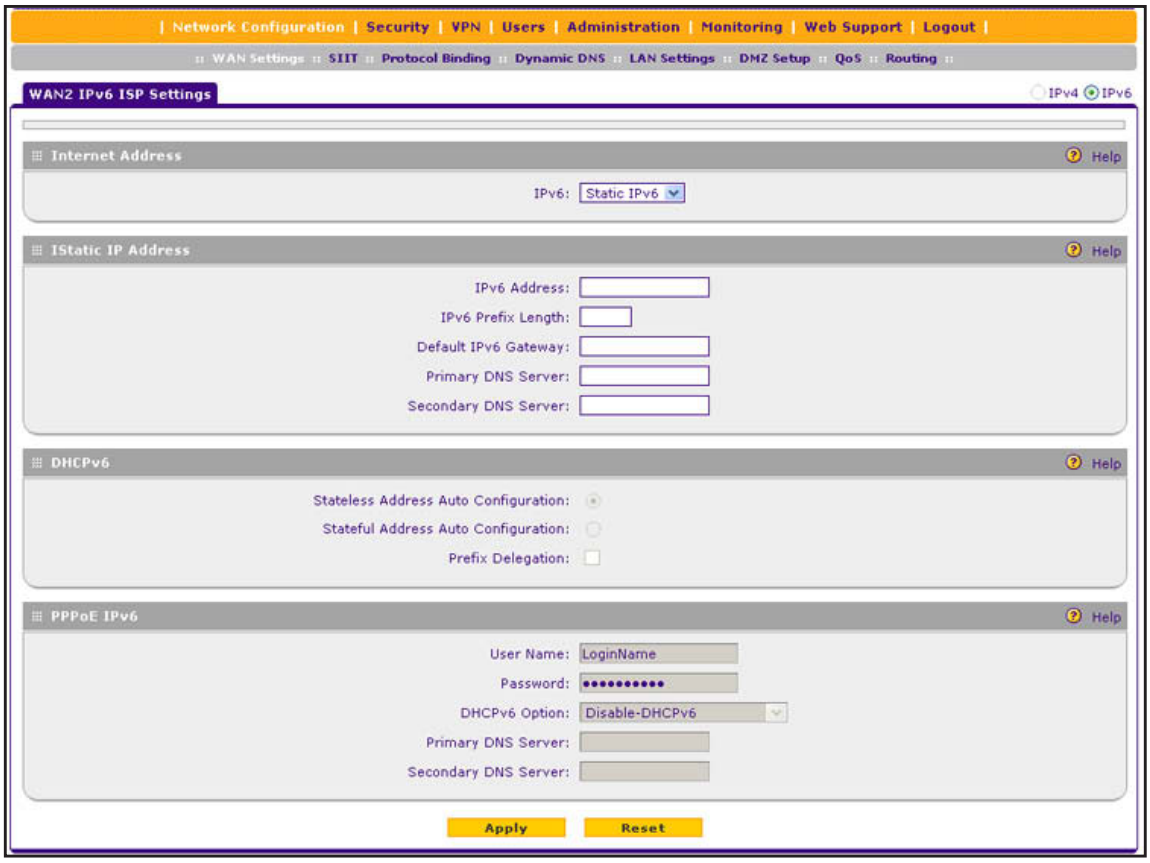

Figure 33.

4. In the Internet Address section of the screen, from the IPv6 drop-down list, select **Static IPv6**.
5. In the Static IP Address section of the screen, enter the settings as described in the following table. You should have received static IPv6 address information from your IPv6 ISP:

Table 9. WAN ISP IPv6 Settings screen settings for a static IPv6 address

Setting	Description
IPv6 Address	The IP address that your ISP assigned to you. Enter the address in *one* of the following formats (all four examples specify the same IPv6 address): • 2001:db8:0000:0000:020f:24ff:febf:dbcb • 2001:db8:0:0:20f:24ff:febf:dbcb • 2001:db8::20f:24ff:febf:dbcb • 2001:db8:0:0:20f:24ff:128.141.49.32
IPv6 Prefix Length	The prefix length that your ISP assigned to you, typically 64.
Default IPv6 Gateway	The IPv6 IP address of the ISP's default IPv6 gateway.
Primary DNS Server	The IPv6 IP address of the ISP's primary DNS server.
Secondary DNS Server	The IPv6 IP address of the ISP's secondary DNS server.

6. Click **Apply** to save your changes.
7. Verify the connection:
   a. Select **Network Configuration > WAN Settings > WAN Setup**.
   b. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings (see *Figure 32* on page 58).
   c. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen. (The following figure shows a static IP address configuration; the IP addresses are not related to any other examples in this manual.)

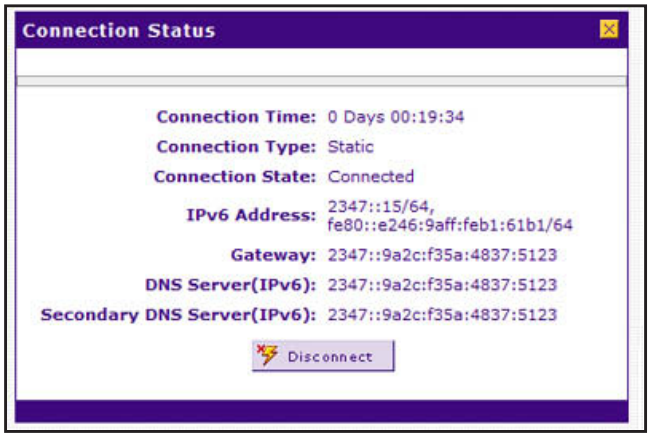

Figure 34.

The Connection Status screen should show a valid IP address and gateway, and you are connected to the Internet. If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 396.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 382.

Note: If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, you need to enter that address on the WAN Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 71).

Configure a PPPoE IPv6 Internet Connection

To configure a PPPoE IPv6 Internet connection, you need to enter the PPPoE IPv6 information that you should have received from your ISP.

➢ **To configure PPPoE IPv6 ISP settings for a WAN interface:**

1. Select **Network Configuration > WAN Settings > WAN Setup**.
2. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings:

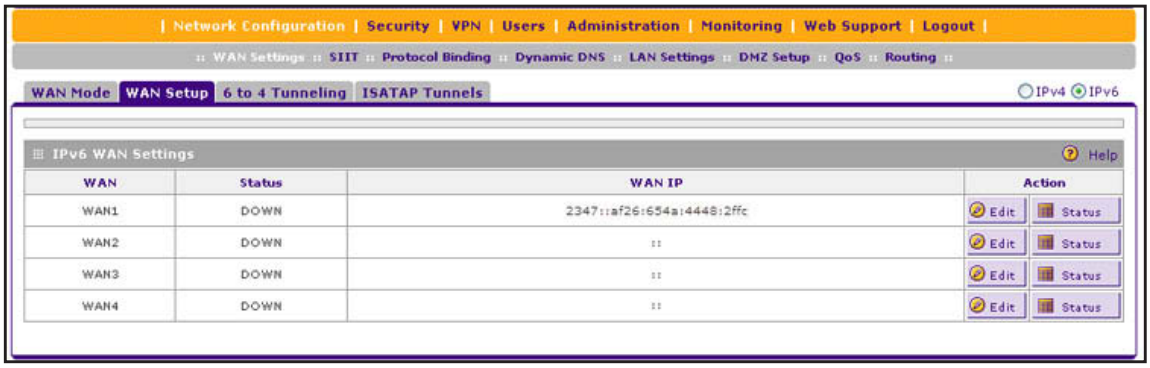

Figure 35.

The IPv6 WAN Settings table displays the following fields:

- **WAN**. The WAN interface (WAN1, WAN2, WAN3, and WAN4).
- **Status**. The status of the WAN interface (UP or DOWN).
- **WAN IP**. The IPv6 address of the WAN interface.
- **Action**. The Edit table button provides access to the WAN IPv6 ISP Settings screen (see *Step 3*) for the corresponding WAN interface; the Status button provides access to the Connection Status screen (see *Step 7*) for the corresponding WAN interface.

3. Click the **Edit** table button in the Action column of the WAN interface for which you want to automatically configure the connection to the Internet. The WAN IPv6 ISP Settings screen displays. (The following figure shows the WAN2 IPv6 ISP Settings screen as an example.)

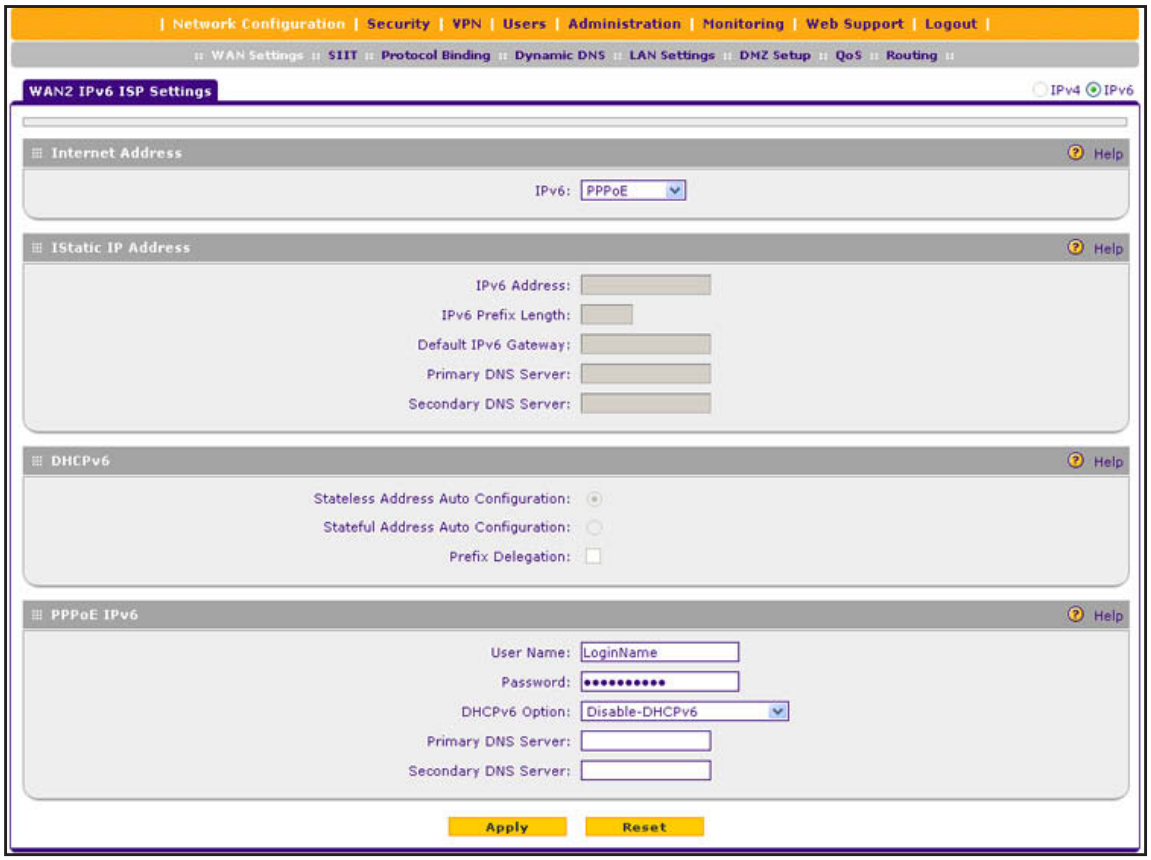

Figure 36.

4. In the Internet Address section of the screen, from the IPv6 drop-down list, select **PPPoE**.
5. In the PPPoE IPv6 section of the screen, enter the settings as described in the following table. You should have received PPPoE IPv6 information from your ISP:

Table 10. WAN IPv6 ISP Settings screen settings for a PPPoE IPv6 connection

Setting	Description
User Name	The PPPoE user name that is provided by your ISP.
Password	The PPPoE password that is provided by your ISP.

Table 10. WAN IPv6 ISP Settings screen settings for a PPPoE IPv6 connection (continued)

Setting	Description
DHCPv6 Option	From the DHCPv6 Option drop-down list, select one of the following DHCPv6 server options, as directed by your ISP: • **Disable-DHCPv6**. DHCPv6 is disabled. You need to specify the DNS servers in the Primary DNS Server and Secondary DNS Server fields in order to receive an IP address from the ISP. • **DHCPv6 StatelessMode**. The VPN firewall generates its own IP address by using a combination of locally available information and router advertisements, but receives DNS server information from the ISP's DHCPv6 server. Router advertisements include a prefix that identifies the subnet that is associated with the WAN port. The IP address is formed by combining this prefix and the MAC address of the WAN port. The IP address is a dynamic address. • **DHCPv6 StatefulMode**. The VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from the ISP's DHCPv6 server. The IP address is a dynamic address. • **DHCPv6 Prefix Delegation**. The VPN firewall obtains a prefix from the ISP's DHCPv6 server through prefix delegation, for example, 2001:db8:: /64. The VPN firewall's own stateless DHCPv6 server can assign this prefix to its IPv6 LAN clients. For more information about prefix delegation, see *Stateless DHCPv6 Server With Prefix Delegation* on page 103.
Primary DNS Server	If you have selected the Disable-DHCPv6 from the DHCPv6 Options drop-down list, the IPv6 IP address of the ISP's primary DNS server.
Secondary DNS Server	If you have selected the Disable-DHCPv6 from the DHCPv6 Options drop-down list, the IPv6 IP address of the ISP's secondary DNS server.

6. Click **Apply** to save your changes.
7. Verify the connection:
   a. Select **Network Configuration > WAN Settings > WAN Setup**.
   b. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings (see *Figure 35* on page 61).
   c. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen. (See *Figure 34* on page 60, which shows a static IP address configuration; the screen for PPPoE is similar.)

The Connection Status screen should show a valid IP address and gateway, and you are connected to the Internet. If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 396.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 382.

Note: If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, you need to enter that address on the WAN Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 71).

Configure 6to4 Automatic Tunneling

If your network is an isolated IPv6 network that is not connected to an IPv6 ISP, you need to make sure that the IPv6 packets can travel over the IPv4 Internet backbone by enabling automatic 6to4 tunneling.

6to4 is a WAN tunnel mechanism for automatic tunneling of IPv6 traffic between a device with an IPv6 address and a device with an IPv4 address, or the other way around. 6to4 tunneling is used to transfer IPv6 traffic between LAN IPv6 hosts and WAN IPv6 networks over the IPv4 network.

With 6to4 tunnels, IPv6 packets are embedded within the IPv4 packet and then transported over the IPv4 network. You do not need to specify remote tunnel endpoints, which are automatically determined by relay routers on the Internet. You cannot use 6to4 tunnels for traffic between IPv4-only devices and IPv6-only devices.

Note: If the VPN firewall functions as the endpoint for 6to4 tunnels in your network, make sure that the VPN firewall has a static IPv4 address (see *Manually Configure an IPv4 Internet Connection* on page 34). A dynamic IPv4 address can cause routing problems on the 6to4 tunnels.

Note: If you do not use a stateful DHCPv6 server in your LAN, you need to configure the Router Advertisement Daemon (RADVD), and set up 6to4 advertisement prefixes for 6to4 tunneling to function correctly. For more information, see *Manage the IPv6 LAN* on page 102.

Typically, 6to4 tunnel addresses start with a 2002 prefix (decimal notification). On the VPN firewall, a 6to4 tunnel is indicated by sit0-WAN1 (see *View the Tunnel Status and IPv6 Addresses* on page 67).

➢ **To enable 6to4 automatic tunneling:**

1. Select **Network Configuration > WAN Settings > 6 to 4 Tunneling**. The 6 to 4 Tunneling screen displays.

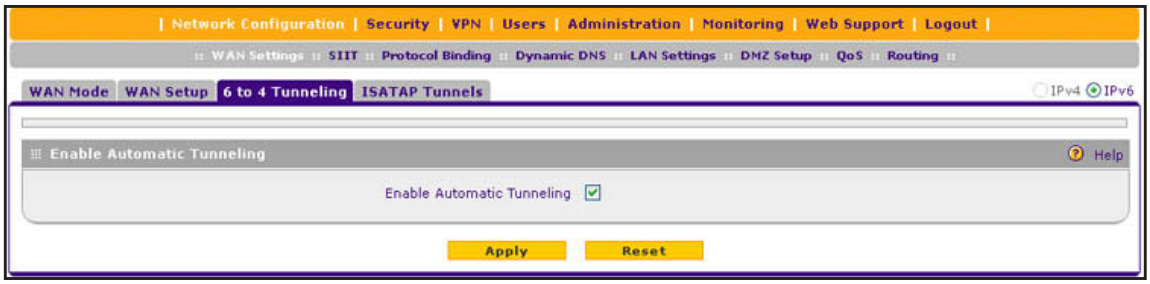

Figure 37.

2. Select the **Enable Automatic Tunneling** check box.
3. Click **Apply** to save your changes.

Configure ISATAP Automatic Tunneling

If your network is an IPv4 network or IPv6 network that consists of both IPv4 and IPv6 devices, you need to make sure that the IPv6 packets can travel over the IPv4 intranet by enabling and configuring Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunneling.

ISATAP is a LAN tunnel mechanism in which the IPv4 network functions as a virtual IPv6 local link. Each IPv4 address is mapped to a link-local IPv6 address, that is, the IPv4 address is used in the interface portion of the IPv6 address. ISATAP tunneling is used intra-site, that is, between addresses in the LAN. For more information about link-local addresses, see *Manage the IPv6 LAN* on page 102.

Note: If you do not use a stateful DHCPv6 server in your LAN, you need to configure the Router Advertisement Daemon (RADVD), and set up ISATAP advertisement prefixes (which are referred to as Global/Local/ISATAP prefixes) for ISATAP tunneling to function correctly. For more information, see *Manage the IPv6 LAN* on page 102.

The VPN firewall determines the link-local address by concatenating the IPv6 address with the 32 bits of the IPv4 host address:

- For a unique global address: fe80:0000:0000:0000:0000:5efe (or fe80::5efe) is concatenated with the IPv4 address. For example, fe80::5efe with 10.29.33.4 becomes fe80::5efe:10.29.33.4, or in hexadecimal format, fe80::5efe:a1d:2104.
- For a private address: fe80:0000:0000:0000:0200:5efe (or fe80::200:5efe) is concatenated with the IPv4 address. For example, fe80::200:5efe with 192.168.1.1 becomes fe80::200:5efe:192.168.1.1, or in hexadecimal format, fe80::200:5efe:c0a8:101.

➢ **To configure an ISATAP tunnel:**

1. Select **Network Configuration > WAN Settings > ISATAP Tunnels**. The ISATAP Tunnels screen displays. (The following figure shows some examples.)

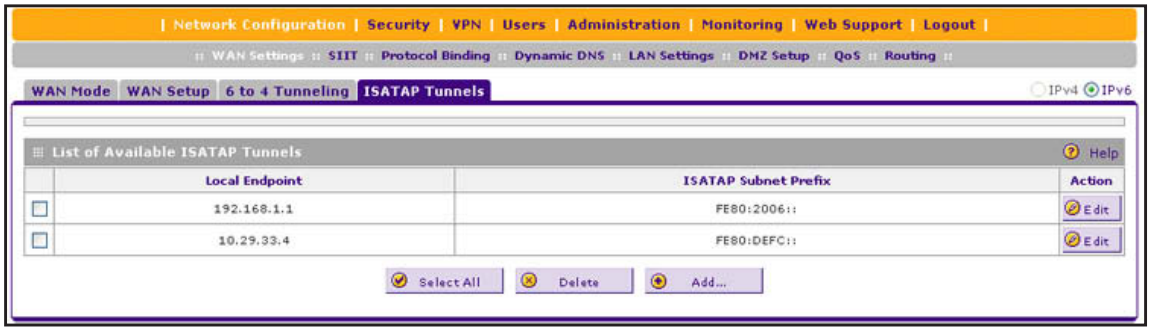

Figure 38.

2. Click the **Add** table button under the List of Available ISATAP Tunnels table. The Add ISATAP Tunnel screen displays:

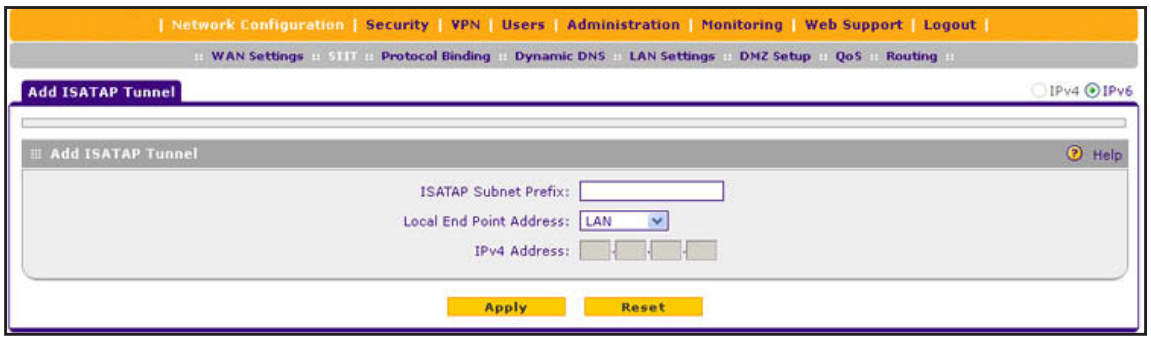

Figure 39.

3. Specify the tunnel settings as described in the following table.

Table 11. Add ISATAP Tunnel screen settings

Setting	Description
ISATAP Subnet Prefix	The IPv6 prefix for the tunnel.
Local End Point Address	From the drop-down list, select the type of local address: • **LAN**. The local endpoint address is the address of the default VLAN. • **Other IP**. The local endpoint address is another LAN IP address that you need to specify in the IPv4 Address fields.
IPv4 Address	If you select Other IP from the Local End Point Address drop-down list, enter the IPv4 address.

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

➢ **To edit an ISATAP tunnel:**

1. On the ISATAP Tunnels screen, click the **Edit** button in the Action column for the tunnel that you want to modify. The Edit ISATAP Tunnel screen displays. This screen is identical to the Add ISATAP Tunnel screen.
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more tunnels:**

1. On the ISATAP Tunnels screen, select the check box to the left of each tunnel that you want to delete, or click the **Select All** table button to select all tunnels.
2. Click the **Delete** table button.

View the Tunnel Status and IPv6 Addresses

The IPv6 Tunnel Status screen displays the status of all active 6to4 and ISATAP tunnels and their IPv6 addresses.

➢ **To view the status of the tunnels and IPv6 addresses:**

Select **Monitoring > Router Status > Tunnel Status**. The Tunnel Status screen displays:

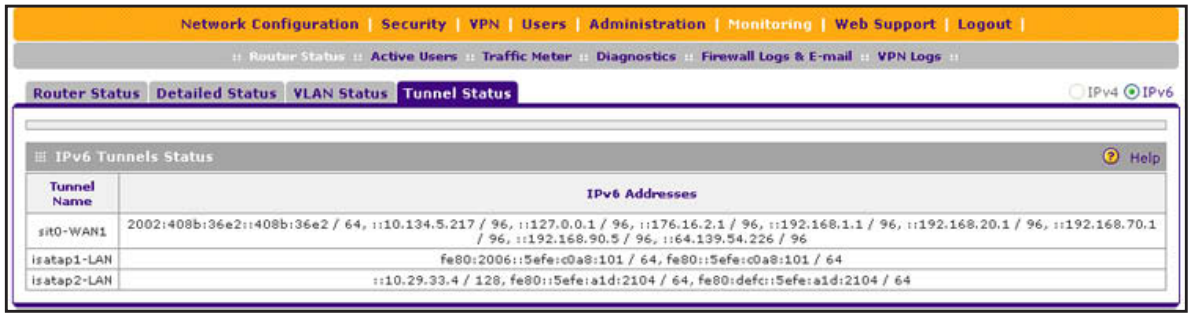

Figure 40.

The IPv6 Tunnel Status table shows the following fields:

- **Tunnel Name**. The tunnel name for the 6to4 tunnel is always sit0-WAN1 (SIT stands for simple Internet transition); the tunnel name for an ISATAP tunnel is isatapx-LAN, in which x is an integer.
- **IPv6 Address**. The IPv6 address of the local tunnel endpoint.

Configure Stateless IP/ICMP Translation

Stateless IP/ICMP Translation (SIIT) is a transition mechanism algorithm that translates between IPv4 and IPv6 packet headers. Using SIIT, an IPv6 device that does not have a permanently assigned IPv4 addresses can communicate with an IPv4-only device.

SIIT functions with IPv4-translated addresses, which are addresses of the format 0::ffff:0:0:0/96 for IPv6-enabled devices. You can substitute an IPv4 address in the format

a.b.c.d for part of the IPv6 address so that the IPv4-translated address becomes 0::ffff:0:a.b.c.d/96.

For SIIT to function, the routing mode needs to be IPv4 / IPv6. NETGEAR's implementation of SIIT lets you enter a single IPv4 address on the SIIT screen. This IPv4 address is then used in the IPv4-translated address for IPv6 devices to enable communication between IPv4-only devices on the VPN firewall's LAN and IPv6-only devices on the WAN.

➢ **To configure SIIT:**

1. Select **Network Configuration > SIIT**. The SIIT screen displays:

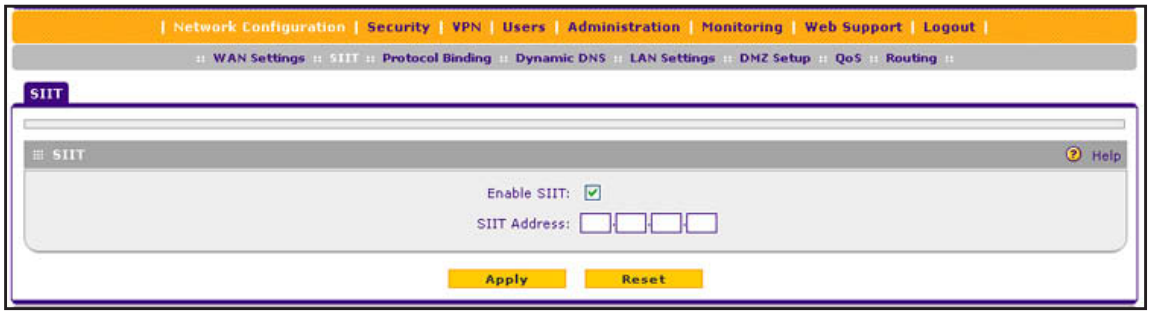

Figure 41.

2. Select the **Enable SIIT** check box.
3. In the SIIT Address fields, enter the IPv4 address that should be used in the IPv4-translated address for IPv6 devices.
4. Click **Apply** to save your changes.

Configure Auto-Rollover for IPv6 Interfaces

You can configure the VPN firewall's IPv6 interfaces for auto-rollover for increased system reliability. You need to specify one WAN interface as the primary interface.

The VPN firewall supports the following modes for IPv6 interfaces:

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

  If you want to use a redundant ISP link for backup purposes, select the WAN port that should function 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 Advanced Options screen to support auto-rollover.

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

When the VPN firewall is configured in auto-rollover mode, it uses the WAN failure detection method to detect the status of the primary link connection at regular intervals. For IPv6 interfaces, the VPN firewall detects link failure by sending a ping request to an IP address

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

Configure Auto-Rollover Mode for IPv6 Interfaces

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

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays:

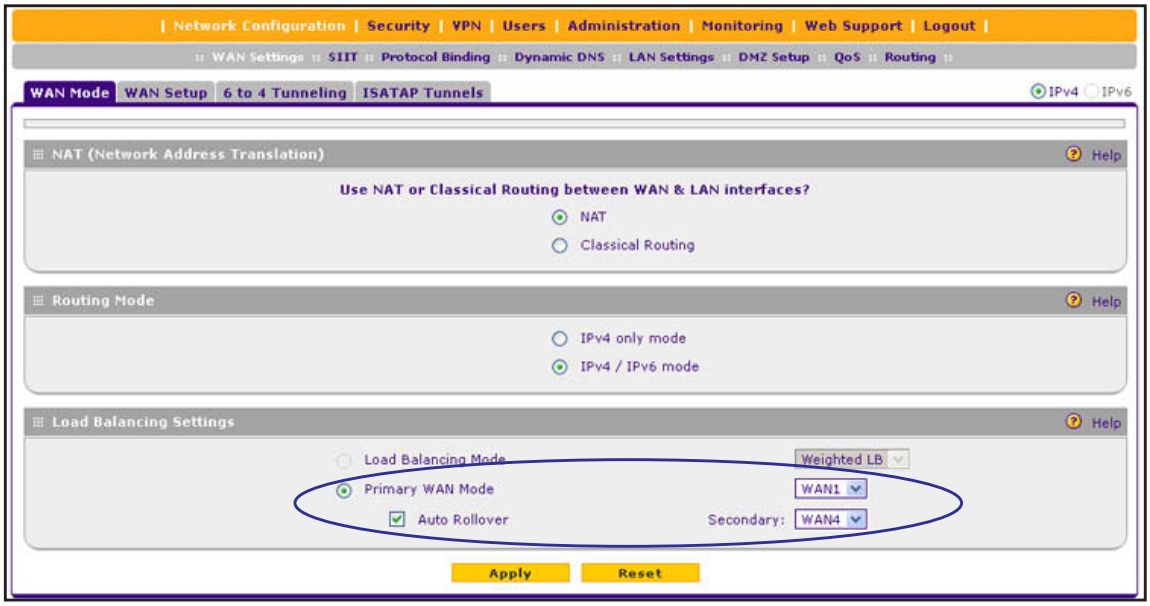

Figure 42.

2. In the Load Balancing Settings section of the screen, configure the following settings:
   a. Select the **Primary WAN Mode** radio button.
   b. From the corresponding drop-down list on the right, select a WAN interface to function as the primary WAN interface. The other WAN interfaces become disabled.
   c. Select the **Auto Rollover** check box.
   d. From the corresponding drop-down list on the right, select a WAN interface to function as the backup WAN interface.

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

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

Configure the Failure Detection Method for IPv6 Interfaces

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

1. Select **Network Configuration > WAN Settings > WAN Setup**.
2. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings (See *Figure 29* on page 55).
3. Click the **Edit** table button in the Action column of the WAN interface that you selected as the primary WAN interface. The WAN IPv6 ISP Settings screen displays (see *Figure 30* on page 56, which shows the WAN2 IPv6 ISP Settings screen as an example).
4. Click the **Advanced** option arrow in the upper right of the screen. The WAN IPv6 Advanced Options screen displays for the WAN interface that you selected:

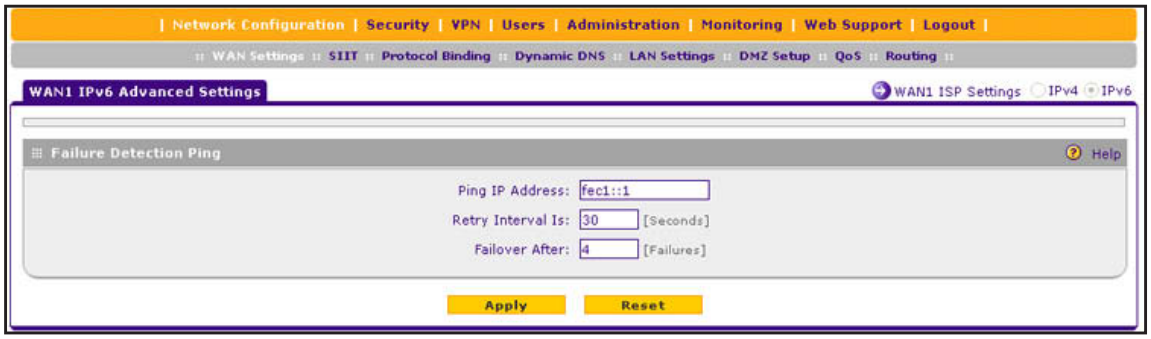

Figure 43.

5. Enter the settings as described in the following table.

Table 12. Failure detection settings

Setting	Description
Ping IP Address	The IP address of the interface that should receive the ping request. The interface should not reject the ping request and should not consider ping traffic to be abusive. **Note:** Pings are sent through the WAN interface that is being monitored. The retry interval and number of failover attempts determine how quickly the VPN firewall switches from the primary link to the backup link if the primary link fails, or when the primary link comes back up, switches back from the backup link to the primary link.
Retry Interval is	The retry interval in seconds. A ping is sent after every retry interval. The default retry interval is 30 seconds.
Failover after	The number of failover attempts. The primary WAN interface is considered down after the specified number of queries have failed to elicit a reply. The backup interface is brought up after this situation has occurred. The failover default is 4 failures.

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

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

You can configure the VPN firewall to generate a WAN status log and email this log to a specified address (see *Configure Logging, Alerts, and Event Notifications* on page 362).

Configure Advanced WAN Options and Other Tasks

The advanced options include configuring the maximum transmission unit (MTU) size, port speed, and VPN firewall's MAC address, and setting a rate limit on the traffic that is being forwarded by the VPN firewall. You can also configure the failure detection method for the auto-rollover mode.

Note: Although you can access the WAN Advanced Options screen for a WAN interface only through the WAN IPv4 ISP Settings screen, the advanced options apply to both IPv4 and IPv6 WAN connections. However, the failure detection method applies only to IPv4 settings.

➢ **To configure advanced WAN options:**

1. Select **Network Configuration > WAN Settings > WAN Setup**. In the upper right of the screen, the IPv4 radio button is selected by default. The WAN Setup screen displays the IPv4 settings:

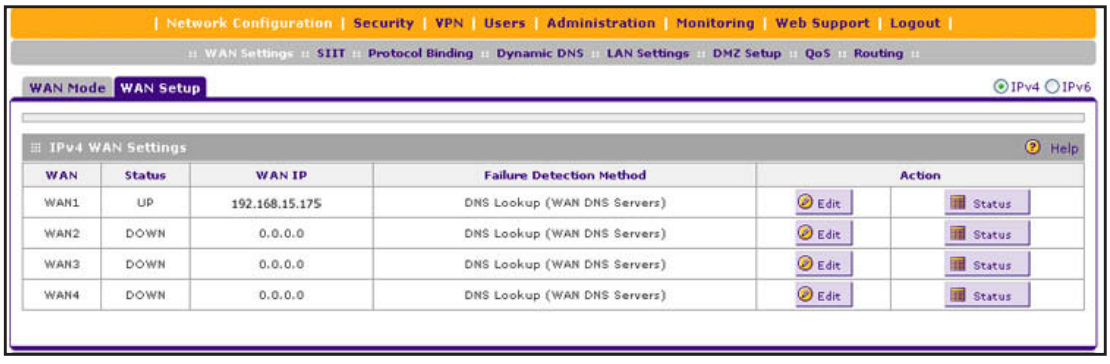

Figure 44.

2. Click the **Edit** table button in the Action column of the WAN interface for which you want to configure the advanced WAN options. The WAN IPv4 ISP Settings screen displays. (The following figure shows the WAN2 IPv4 ISP Settings screen as an example.)

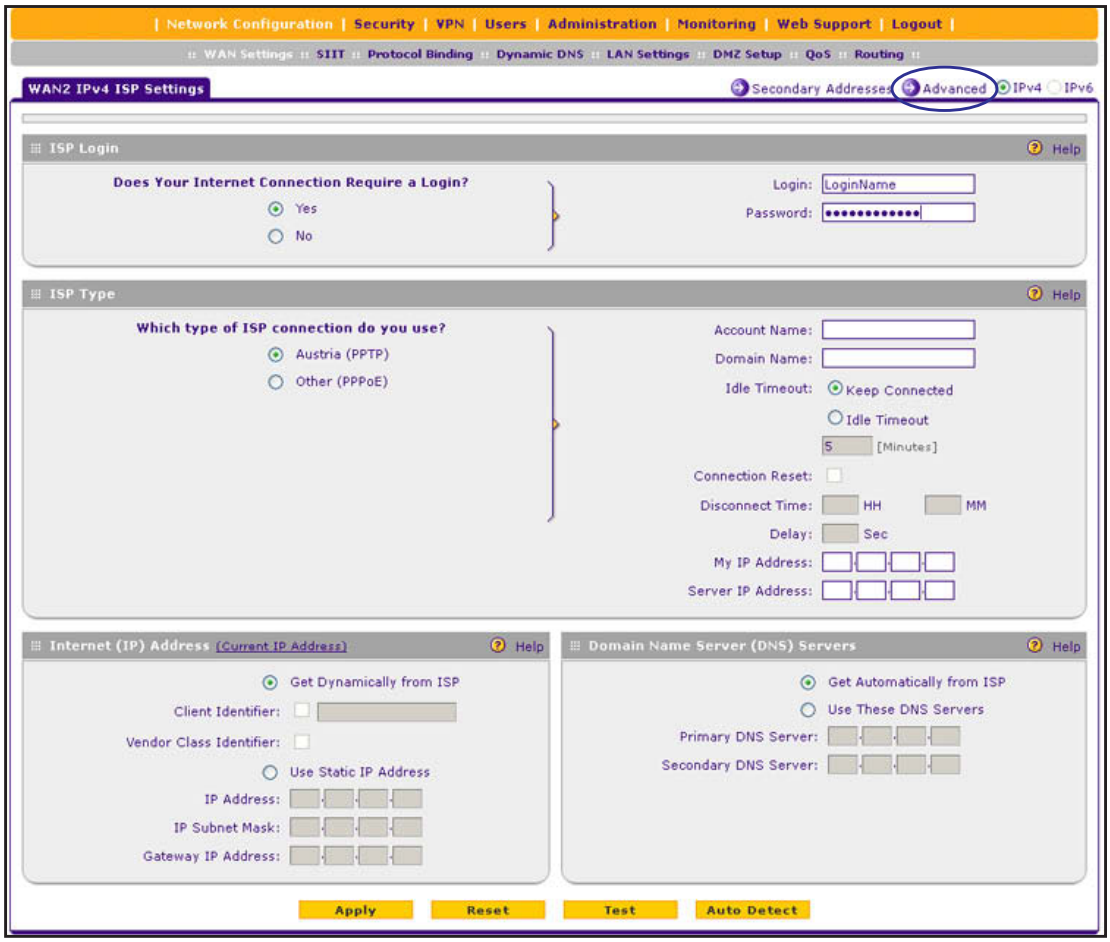

Figure 45.

3. Click the **Advanced** option arrow in the upper right of the screen. The WAN Advanced Options screen displays for the WAN interface that you selected. (The following figure shows the WAN2 Advanced Options screen as an example.)

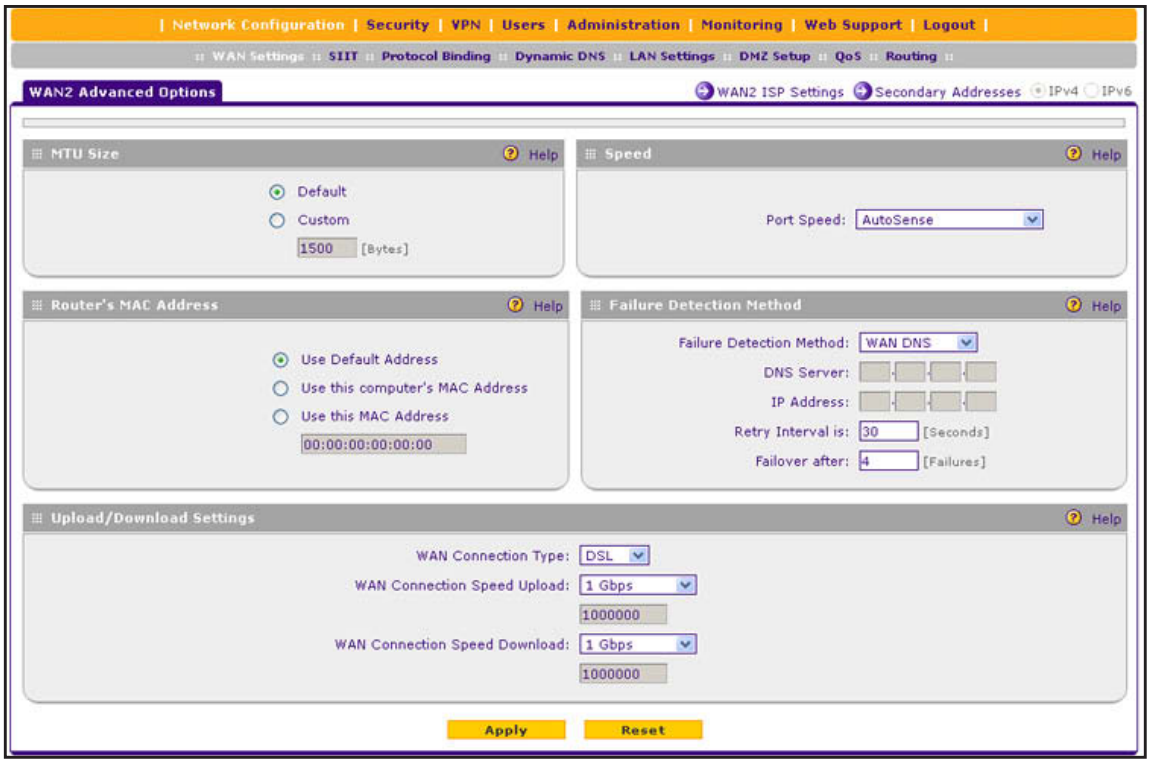

Figure 46.

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

Table 13. WAN Advanced Options screen settings

Setting	Description
MTU Size Make one of the following selections:	
Default	Select the **Default** radio button for the normal maximum transmit unit (MTU) value. For most Ethernet networks, this value is 1500 bytes, or 1492 bytes for PPPoE connections.
Custom	Select the **Custom** radio button, and enter an MTU value in the Bytes field. For some ISPs, you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure that it is necessary for your ISP connection.

Table 13. WAN Advanced Options screen settings (continued)

Setting	Description
Speed	
In most cases, the VPN firewall can automatically determine the connection speed of the WAN port of the device (modem, dish, 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, dish, or router, select it from the drop-down list. Use the half-duplex settings only if the full-duplex settings do not function correctly. Select one of the following speeds from the drop-down list: • **AutoSense**. Speed autosensing. This is the default setting, which can sense all Ethernet speeds and duplex modes, including 1000BASE-T speed at full duplex. • **10BaseT Half_Duplex**. Ethernet speed at half duplex. • **10BaseT Full_Duplex**. Ethernet speed at full duplex. • **100BaseT Half_Duplex**. Fast Ethernet speed at half duplex. • **100BaseT Full_Duplex**. Fast Ethernet speed at full duplex. • **1000BaseT Full_Duplex**. Gigabit Ethernet speed at full duplex.	
Router'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. 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 VPN firewall's own MAC address, select the **Use Default Address** radio button.
Use this computer's MAC Address	Select the **Use this computer's MAC Address** radio button to allow the VPN firewall to use the MAC address of the computer you are now using to access the web management interface. This setting is useful if your ISP requires MAC authentication.
Use this MAC Address	Select the **Use this MAC Address** radio button, and manually enter the MAC address in the field next to the radio button. You would typically enter the MAC address that your ISP is requiring for MAC authentication. **Note:** The format for the MAC address is 01:23:45:67:89:AB (numbers 0–9 and either uppercase or lowercase letters A–F). If you enter a MAC address, the existing entry is overwritten.

Table 13. WAN Advanced Options screen settings (continued)

Setting	Description
Failure Detection Method **Note:** This is the failure detection method for IPv4 interfaces. For information about failure detection for IPfv6 interfaces, see *Configure the Failure Detection Method for IPv6 Interfaces* on page 70.	
Failure Detection Method	Select a failure detection method from the drop-down list: • **WAN DNS**. DNS queries are sent to the DNS server that is configured in the Domain Name Server (DNS) Servers section of the WAN ISP screen (see *Manually Configure an IPv4 Internet Connection* on page 34). • **Custom DNS**. DNS queries are sent to a DNS server that you need to specify in the DNS Server fields. • **Ping**. Pings are sent to a server with a public IP address that you need to specify in the IP Address fields. The server should not reject the ping request and should not consider ping traffic to be abusive. **Note:** DNS queries or pings are sent through the WAN interface that is being monitored. The retry interval and number of failover attempts determine how quickly the VPN firewall switches from the primary link to the backup link if the primary link fails, or when the primary link comes back up, switches back from the backup link to the primary link.
DNS Server	The IP address of the DNS server.
IP Address	The IP address of the interface that should receive the ping request. The interface should not reject the ping request and should not consider ping traffic to be abusive
Retry Interval is	The retry interval in seconds. The DNS query or ping is sent after every retry interval. The default retry interval is 30 seconds.
Failover after	The number of failover attempts. The primary WAN interface is considered down after the specified number of queries have failed to elicit a reply. The backup interface is brought up after this situation has occurred. The failover default is 4 failures.
Upload/Download Settings These settings rate-limit the traffic that is being forwarded by the VPN firewall.	
WAN Connection Type	From the drop-down list, select the type of connection that the VPN firewall uses to connect to the Internet: **DSL**, **ADLS**, **T1**, **T3**, or **Other**.
WAN Connection Speed Upload	From the drop-down list, select the maximum upload speed that is provided by your ISP. You can select from 56 Kbps to 1 Gbps, or you can select **Custom** and enter the speed in Kbps in the field below the drop-down list.
WAN Connection Speed Download	From the drop-down list, select the maximum download speed that is provided by your ISP. You can select from 56 Kbps to 1 Gbps, or you can select **Custom** and enter the speed in Kbps in the field below the drop-down list.

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

WARNING:

Depending on the changes that you made, when you click Apply, the VPN firewall might restart, or services such as HTTP and SMTP might restart.

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

Configure WAN QoS Profiles

The VPN firewall can support multiple Quality of Service (QoS) profiles for each WAN interface. You can assign profiles to services such as HTTP, FTP, and DNS and to LAN groups or IP addresses. Profiles enforce either rate control with bandwidth allocation or priority queue control. You can configure both types of profiles, but either all profiles on the VPN firewall enforce rate control and the profiles that you configured for priority queue control are inactive, or the other way around. Both types of profiles cannot be active simultaneously.

- **Rate control with bandwidth allocation**. These types of profiles specify how bandwidth is distributed among the services and hosts. A profile with a high priority is offered excess bandwidth while the required bandwidth is still allocated to profiles that specify minimum and maximum bandwidth rates. The congestion priority represents the classification level of the packets among the priority queues within the system. If you select a default congestion priority, traffic is mapped based on the Type of Service (ToS) field in the packet's IP header.
- **Priority queue control**. These types of profiles specify the priority levels of the services. You can select a high-priority queue or a low-priority queue. Services in the high-priority queue share 60 percent of the interface bandwidth; services in the low-priority queue share 10 percent of the interface bandwidth. By default, all services are assigned the medium-priority queue in which they share 30 percent of the interface bandwidth.

Both types of profiles let you allocate the Differentiated Services (DiffServ) QoS packet matching and QoS packet marking settings, which you configure by specifying Differentiated Services Code Point (DSCP) values, from 0 to 63.

Note: Before you enable WAN QoS, make sure that the WAN connection type and speeds are configured correctly in the Upload/Download Settings section of the WAN Advanced Options screen for the WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 71).

Note: To configure and apply QoS profiles successfully, familiarity with QoS concepts such QoS priority queues, IP precedence, DHCP, and their values is helpful.

➢ **To enable and configure QoS for the WAN interfaces:**

1. Select **Network Configuration > QoS**. The QoS screen displays. (The following screen shows some profiles in the List of QoS Profiles table).

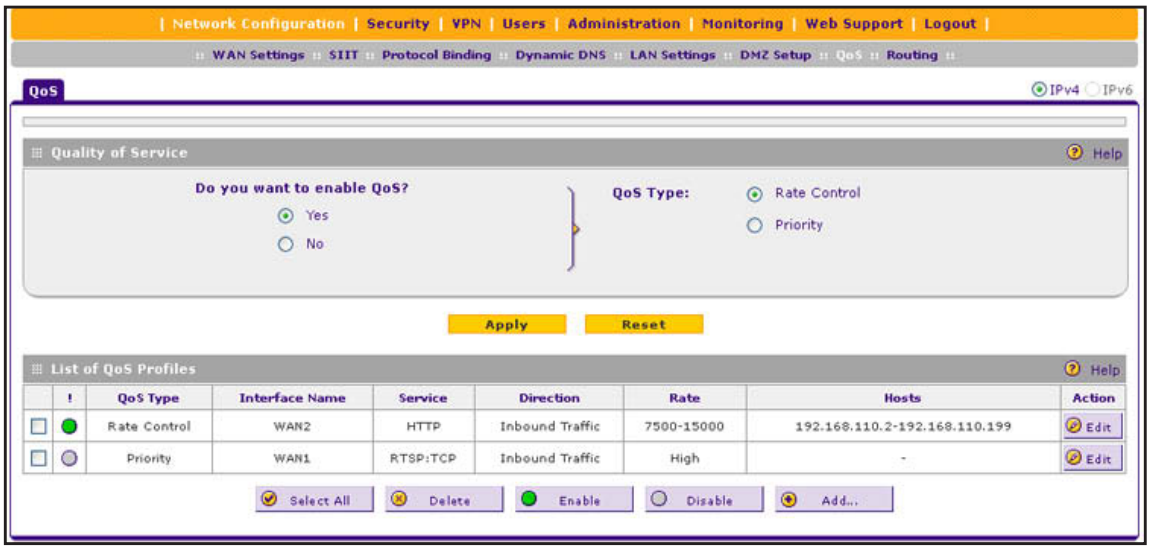

Figure 47.

2. To enable QoS, select the **Yes** radio button. By default, the No radio button is selected.
3. Specify the profile type that should be active by selecting one of the following radio buttons:
   - **Rate control**. All rate control QoS profiles that you configure are active, but priority QoS profiles are not.
   - **Priority**. All priority QoS profiles that you configure are active, but rate control QoS profiles are not.
4. Click **Apply** to save your settings.

   The List of QoS Profiles table shows the following columns, all of which are described in detail in the following table and *Table 15* on page 80.

   - **QoS Type**. The type of profile, either Rate Control or Priority.
   - **Interface Name**. The WAN interface to which the profile applies (WAN1, WAN2, WAN3, or WAN4).
   - **Service**. The service to which the profile applies.
   - **Direction**. The WAN direction to which the profile applies (inbound, outbound, or both).
   - **Rate**. The bandwidth rate in Kbps, or the priority.

- **Hosts**. The IP address, IP addresses, or group to which the rate control profile applies. (The information in this column does not apply to priority profiles).
- **Action**. The Edit table button provides access to the Edit QoS screen for the corresponding profile.

➢ **To add a rate control QoS profile:**

1. Select **Network Configuration > QoS**. The QoS screen displays.
2. Under the List of QoS Profiles table, click the **Add** table button. The Add QoS screen displays. The following figure shows settings for a rate control QoS profile:

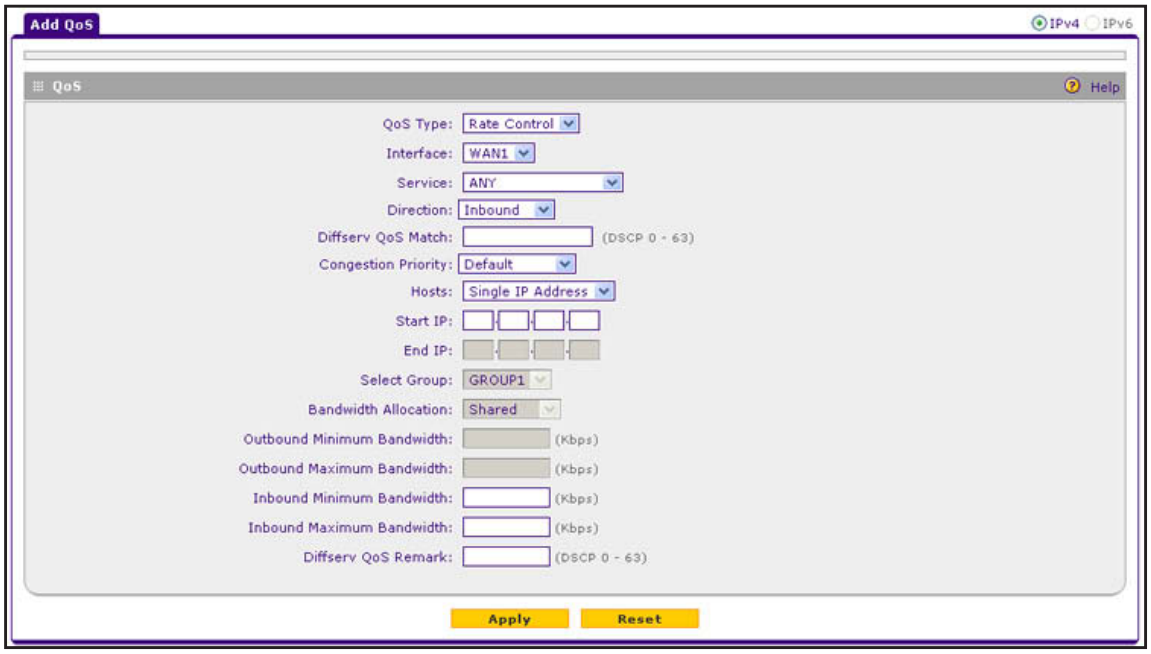

Figure 48.

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

Table 14. Add QoS screen settings for a rate control profile

Setting	Description
QoS Type	Rate Control (for Priority, see *Figure 49* on page 80 and *Table 15* on page 80).
Interface	From the drop-down list, select one of the WAN interfaces.
Service	From the drop-down list, select a service or application to be covered by this profile. If the service or application does not appear in the list, you need to define it using the Services screen (see *Add Customized Services* on page 177).
Direction	From the drop-down list, select the direction to which rate control is applied: • **Inbound Traffic**. Rate control is applied to inbound traffic only. • **Outbound Traffic**. Rate control is applied to outbound traffic only. • **Both**. Rate control is applied to both outbound and inbound traffic.

Table 14. Add QoS screen settings for a rate control profile (continued)

Setting	Description	
Diffserv QoS Match	Enter a DSCP value in the range of 0 through 63. Packets are classified against this value. Leave this field blank to disable packet matching.	
Congestion Priority	From the drop-down list, select the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall: • **Default**. Traffic is mapped based on the ToS field in the packet's IP header. • **High**. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4. • **Medium-high**. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3. • **Medium**. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2. • **Low**. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values.	
Hosts	From the drop-down list, select the IP address, range of IP addresses, or group to which the profile is applied: • **Single IP Address**. The profile is applied to a single IP address. Enter the address in the Start IP field. • **IP Address Range**. The profile is applied to an IP address range. Enter the start address of the range in the Start IP field and the end address of the range in the End IP field, and specify how the bandwidth is allocated by making a selection from the Bandwidth Allocation drop-down list. • **Group**. The profile is applied to a group. Select the group from the Select Group drop-down list, and specify how the bandwidth is allocated by making a selection from the Bandwidth Allocation drop-down list.	
	Start IP	The IP address for a single IP address or the start IP address for an IP address range.
	End IP	The end IP address for an IP address range.
	Select Group	From the drop-down list, select the LAN group to which the profile is applied. For information about LAN groups, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 96.
	Bandwidth Allocation	From the drop-down list, specify how the bandwidth is allocated: • **Shared**. The bandwidth is shared among all IP addresses in a range or all members of a group. • **Individual**. The bandwidth is allocated to each IP address in the range or each member of a group.
Outbound Minimum Bandwidth	Enter the outbound minimum bandwidth in Kbps that is allocated to the host.	
Outbound Maximum Bandwidth	Enter the outbound maximum bandwidth in Kbps that is allocated to the host.	
Inbound Minimum Bandwidth	Enter the inbound minimum bandwidth in Kbps that is allocated to the host.	

Table 14. Add QoS screen settings for a rate control profile (continued)

Setting	Description
Inbound Maximum Bandwidth	Enter the inbound maximum bandwidth in Kbps that is allocated to the host.
Diffserv QoS Remark	Enter a DSCP value in the range of 0 through 63. Packets are marked with this value. Leave this field blank to disable packet marking.

4. Click **Apply** to save your settings. The profile is added to the List of QoS Profiles table on the QoS screen.

➢ **To add a priority queue QoS profile:**

1. Select **Network Configuration > QoS**. The QoS screen displays.
2. Under the List of QoS Profiles table, click the **Add** table button. The Add QoS screen displays. The following figure shows settings for a priority QoS profile:

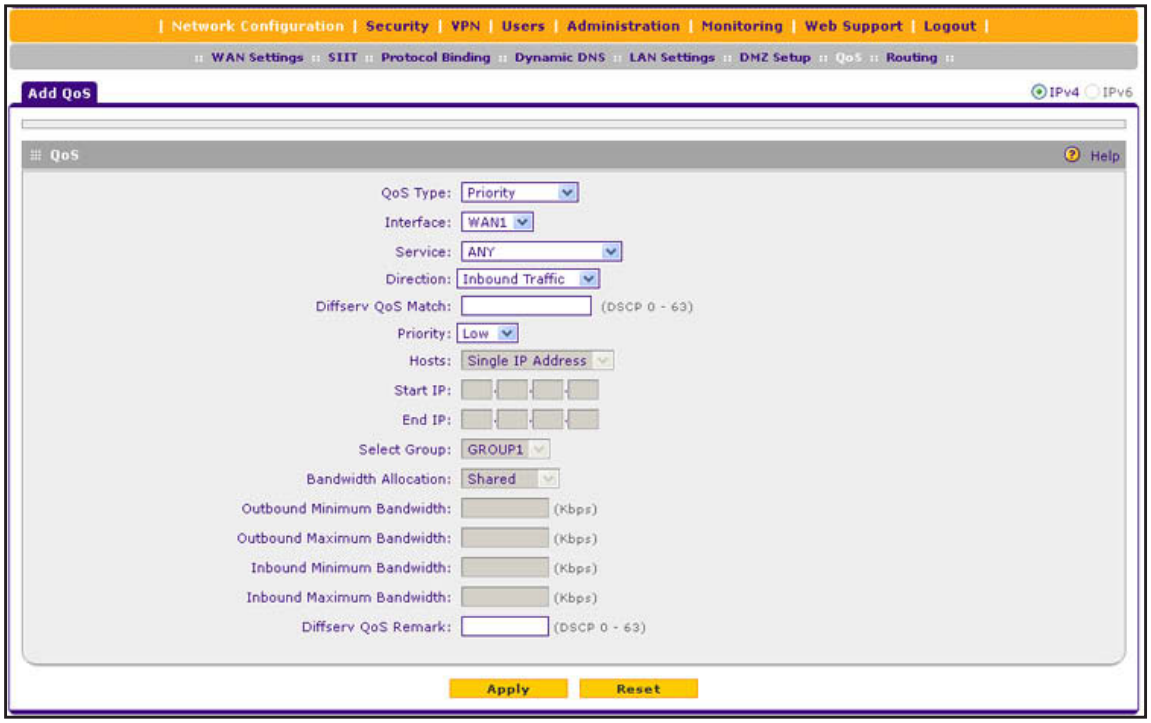

Figure 49.

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

Table 15. Add QoS screen settings for a priority profile

Setting	Description
QoS Type	Priority (for Rate Control, see *Figure 48* on page 78 and *Table 14* on page 78).
Interface	From the drop-down list, select one of the WAN interfaces.

Table 15. Add QoS screen settings for a priority profile (continued)

Setting	Description
Service	From the drop-down list, select a service or application to be covered by this profile. If the service or application does not appear in the list, you need to define it using the Services screen (see *Add Customized Services* on page 177).
Direction	From the drop-down list, select the direction to which the priority queue is applied: • **Outbound Traffic**. The priority queue is applied to outbound traffic only. • **Inbound Traffic**. The priority queue is applied to inbound traffic only.
Diffserv QoS Match	Enter a DSCP value in the range of 0 through 63. Packets are classified against this value. Leave this field blank to disable packet matching.
Priority	From the drop-down list, select the priority queue that determines the allocation of bandwidth: • **Low**. All services that are assigned a low-priority queue share 10 percent of interface bandwidth. • **High**. All services that are assigned a high-priority queue share 60 percent of interface bandwidth. **Note:** By default, all services are assigned the medium-priority queue in which they share 30 percent of the interface bandwidth.
Hosts	These settings do not apply to a priority profile.
Start IP	
End IP	
Select Group	
Bandwidth Allocation	
Outbound Minimum Bandwidth	
Outbound Maximum Bandwidth	
Inbound Minimum Bandwidth	
Inbound Maximum Bandwidth	
Diffserv QoS Remark	Enter a DSCP value in the range of 0 through 63. Packets are marked with this value. Leave this field blank to disable packet marking.

4. Click **Apply** to save your settings. The profile is added to the List of QoS Profiles table on the QoS screen.

➢ **To edit a QoS profile:**

1. In the List of QoS Profiles table, click the **Edit** table button to the right of the profile that you want to edit. The Edit QoS screen displays. This screen shows the same fields as the Add QoS screen (see the previous two figures).
2. Modify the settings as described in the previous two tables.
3. Click **Apply** to save your settings.

➢ **To delete a QoS profile:**

1. In the List of QoS Profiles table, select the check box to the left of the QoS profile that you want to delete, or click the **Select All** table button to select all profiles.
2. Click the **Delete** table button.

Additional WAN-Related Configuration Tasks

If you want the ability to manage the VPN firewall remotely, enable remote management (see *Configure Remote Management Access* on page 338). If you enable remote management, NETGEAR strongly recommends that you change your password (see *Change Passwords and Administrator and Guest Settings* on page 336).

As an option, you can also set up the traffic meter for each WAN interface (see *Configure and Enable the WAN Traffic Meter* on page 356).

Verify the Connection

Test the VPN firewall before deploying it in a live production environment. Verify that network traffic can pass through the VPN firewall:

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

What to Do Next

You have completed setting up the WAN connection for the VPN firewall. The following chapters and sections describe important tasks that you need to address before you deploy the VPN firewall in your network:

- *Chapter 3, LAN Configuration*
- *Configure Authentication Domains, Groups, and Users* on page 303
- *Manage Digital Certificates for VPN Connections* on page 320
- *Use the IPSec VPN Wizard for Client and Gateway Configurations* on page 203
- *Chapter 6, Virtual Private Networking Using SSL Connections*

LAN Configuration

3

This chapter describes how to configure the LAN features of your VPN firewall. The chapter contains the following sections:

- *Manage IPv4 Virtual LANs and DHCP Options*
- *Configure IPv4 Multihome LAN IP Addresses on the Default VLAN*
- *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)*
- *Manage the IPv6 LAN*
- *Configure IPv6 Multihome LAN IP Addresses on the Default VLAN*
- *Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic*
- *Manage Static IPv4 Routing*
- *Manage Static IPv6 Routing*

Manage IPv4 Virtual LANs and DHCP Options

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

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

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

VLANs have a number of advantages:

- It is easy to set up network segmentation. Users who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group’s traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Port-Based VLANs

The VPN firewall 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 VPN firewall are assigned to the default VLAN, or VLAN 1. Therefore, by default, all four LAN ports have the default PVID 1. However, you can assign another PVID to a LAN port by selecting a VLAN profile from the drop-down list on the LAN Setup screen.

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

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

Note the following about VLANs and PVIDs:

- One physical port is assigned to at least one VLAN.
- One physical port can be assigned to multiple VLANs.
- When one port is assigned to multiple VLANs, the port is used as a trunk port to connect to another switch or router.
- When a port receives an untagged packet, this packet is forwarded to a VLAN based on the PVID.
- When a port receives a tagged packet, this packet is forwarded to a VLAN based on the ID that is extracted from the tagged packet.

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

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

Packets coming from the IP phone to the VPN firewall LAN port are tagged. Packets passing through the IP phone from the connected device to the VPN firewall LAN port are untagged. When you assign the VPN firewall LAN port to a VLAN, packets entering and leaving the port are tagged with the VLAN ID. However, untagged packets entering the VPN firewall 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 is described in *Configure the IPv4 Internet Connection and WAN Settings* on page 29. For information about how to add and edit a VLAN profile, including its DHCP options, see *Configure a VLAN Profile* on page 88.

Assign and Manage VLAN Profiles

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

1. Select **Network Configuration > LAN Setting**. In the upper right of the screen, the IPv4 radio button is selected by default. The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings. (The following figure contains some VLAN profiles as an example.)

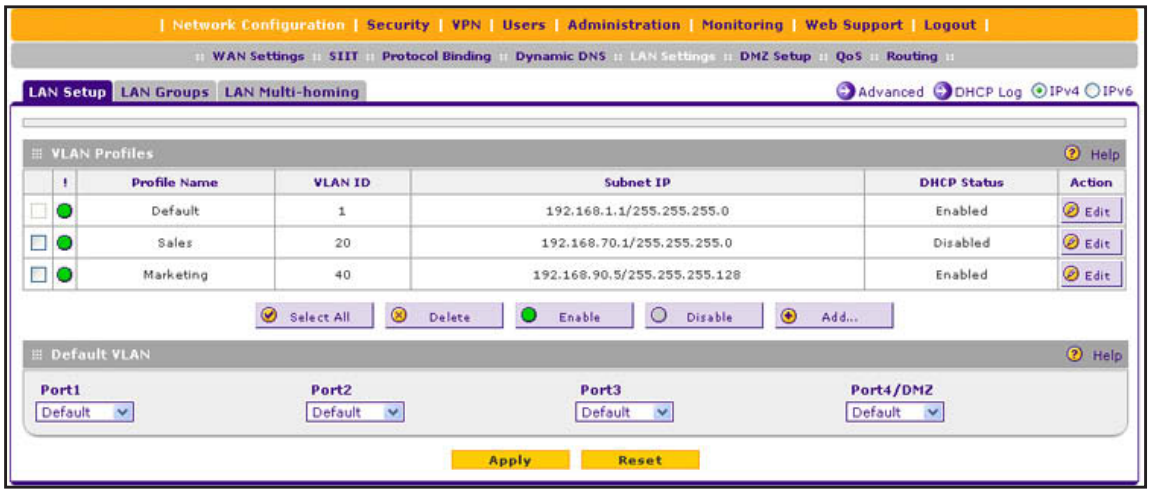

Figure 50.

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

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

2. Assign a VLAN profile to a LAN port by selecting a VLAN profile from the drop-down list. The enabled VLAN profiles are displayed in the drop-down lists.
3. Click **Apply** to save your settings.

VLAN DHCP Options

For each VLAN, you need to specify the Dynamic Host Configuration Protocol (DHCP) options (see *Configure a VLAN Profile* on page 88). The configuration of the DHCP options for the VPN firewall's default VLAN, or VLAN 1, is described in *Configure the IPv4 Internet Connection and WAN Settings* on page 29. 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 VPN firewall to assign IP, DNS server, WINS server, and default gateway addresses to all computers connected to the VPN firewall's LAN. The assigned default gateway address is the LAN address of the VPN firewall. IP addresses are assigned to the attached computers from a pool of addresses that you need to specify. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. When you create a VLAN, the DHCP server option is disabled by default.

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

The VPN firewall 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 VPN firewall's LAN IP address)
- Primary DNS server (the VPN firewall's LAN IP address)
- WINS server (if you entered a WINS server address in the DHCP Setup screen)
- Lease time (the date obtained and the duration of the lease)

DHCP Relay

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

DNS Proxy

When the DNS proxy option is enabled for a VLAN, the VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (as configured on the WAN IPv4 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 VPN

firewall'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.

LDAP Server

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

Configure a VLAN Profile

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

➢ **To add a VLAN profile:**

1. Select **Network Configuration > LAN Settings**. In the upper right of the screen, the IPv4 radio button is selected by default. The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings. (The following figure contains some VLAN profiles as an example.)

Note: For information about how to manage VLANs, see *Port-Based VLANs* on page 85. The following information describes how to configure a VLAN profile.

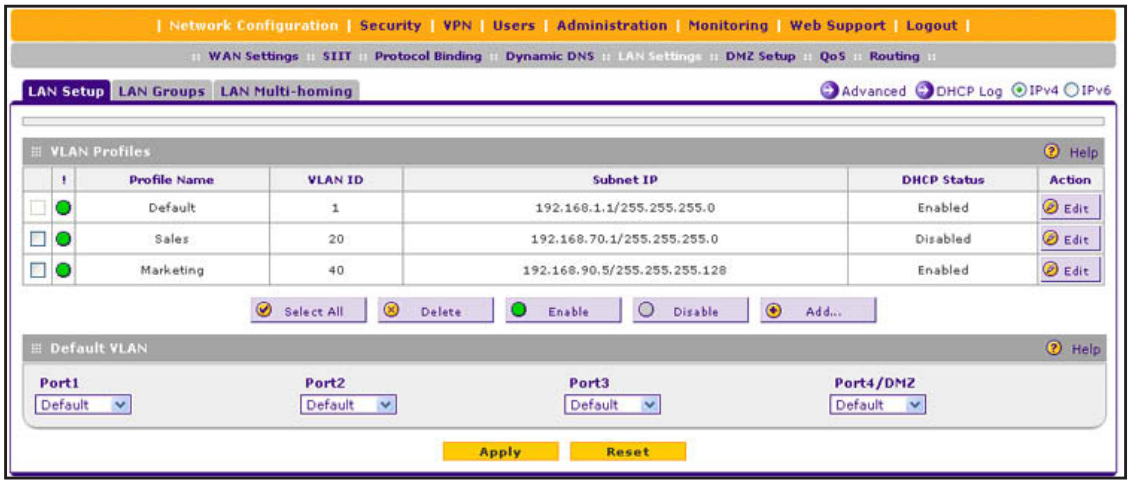

Figure 51.

2. Click the **Add** table button under the VLAN Profiles table. The Add VLAN Profile screen displays:

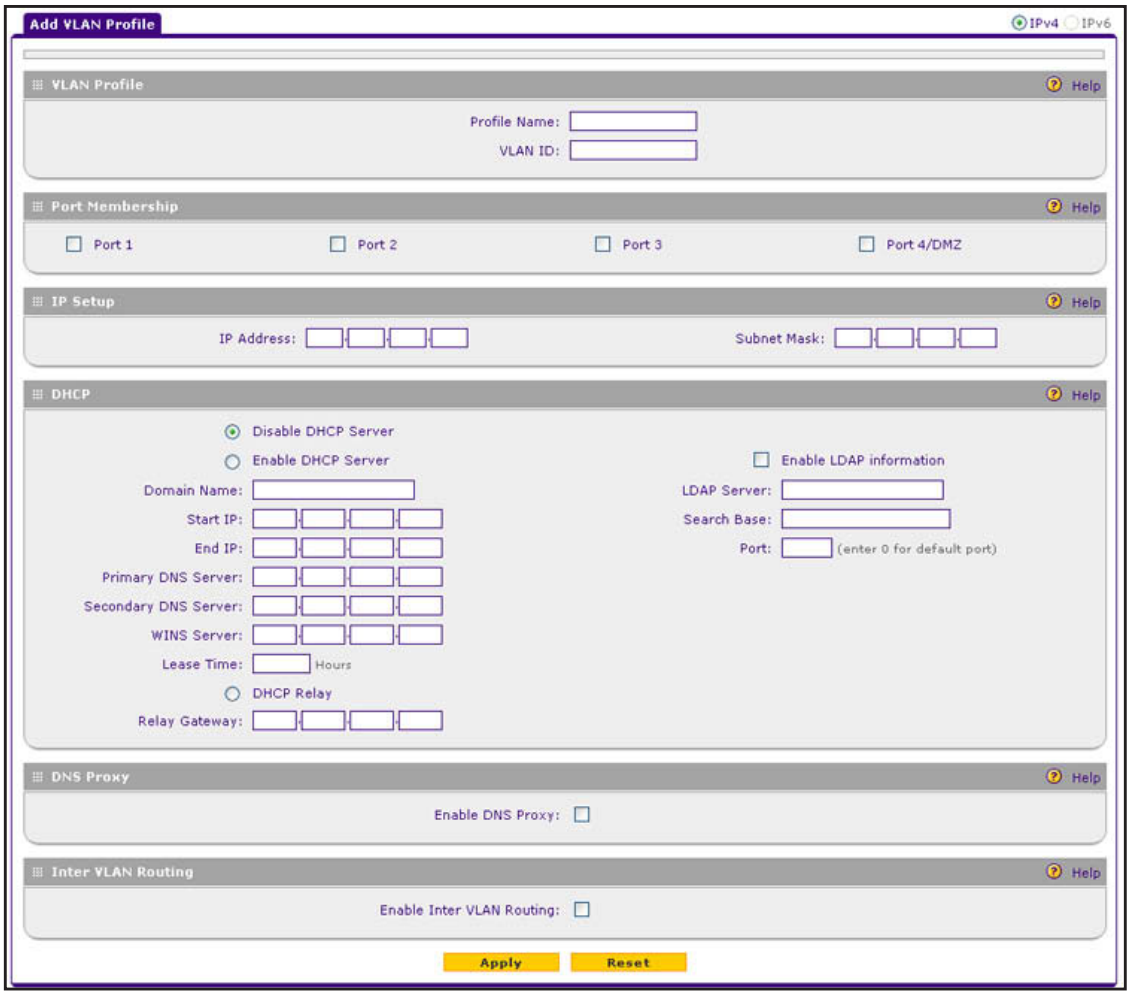

Figure 52.

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

Table 16. Add VLAN Profile screen settings

Setting	Description
VLAN Profile	
Profile Name	Enter a unique name for the VLAN profile.
VLAN ID	Enter a unique ID number for the VLAN profile. No two VLANs can have the same VLAN ID number. **Note:** You can enter VLAN IDs from 2 to 4089. VLAN ID 1 is reserved for the default VLAN; VLAN ID 4094 is reserved for the DMZ interface.

Table 16. Add VLAN Profile screen settings (continued)

Setting	Description
Port Membership	
Port 1, Port 2, Port 3, Port 4 / DMZ	Select one, several, or all port check boxes to make the ports members 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.
IP Setup	
IP Address	Enter the IP address of the VPN firewall (the factory default address is 192.168.1.1). **Note:** Ensure that the LAN port IP address and DMZ port IP address are in different subnets. **Note:** If you change the LAN IP address of the VLAN while being connected through the browser to the VLAN, you are disconnected. You then need to open a new connection to the new IP address and log in again. For example, if you change the default IP address 192.168.1.1 to 10.0.0.1, you now need to enter **https://10.0.0.1** in your browser to reconnect to the web management interface.
Subnet Mask	Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Based on the IP address that you assign, the VPN firewall automatically calculates the subnet mask. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the VPN firewall).
DHCP	
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you intend to manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. Except for the default VLAN for which the DHCP server is enabled, this is the default setting.

Table 16. Add VLAN Profile screen settings (continued)

Setting	Description	
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the VPN firewall to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the VLAN. (For the default VLAN, the DHCP server is enabled by default.) Enter the following settings:	
	Domain Name	This setting is optional. Enter the domain name of the VPN firewall.
	Start IP Address	Enter the start 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 end IP address. For the default VLAN, the default start IP address is 192.168.1.100.
	End IP Address	Enter the end 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 start IP address and this IP address. For the default VLAN, the default end IP address is 192.168.1.254. The start and end DHCP IP addresses should be in the same *network* as the LAN IP address of the VPN firewall (that is, the IP address in the IP Setup section as described earlier in this table).
	Primary DNS Server	This setting is optional. If an IP address is specified, the VPN firewall provides this address as the primary DNS server IP address. If no address is specified, the VPN firewall uses the VLAN IP address as the primary DNS server IP address.
	Secondary DNS Server	This setting is optional. If an IP address is specified, the VPN firewall provides this address as the secondary DNS server IP address.
	WINS Server	This setting is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.
DHCP Relay	To use the VPN firewall as a DHCP relay agent for a DHCP server somewhere else in your network, select the **DHCP Relay** radio button. Enter the following setting:	
	Relay Gateway	The IP address of the DHCP server for which the VPN firewall serves as a relay.

Table 16. Add VLAN Profile screen settings (continued)

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

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. For information about how to change these default traffic rules, see *Chapter 4, Firewall Protection*.

➢ **To edit a VLAN profile:**

1. On the LAN Setup screen for IPv4 (see *Figure 51* on page 88), click the **Edit** button in the Action column for the VLAN profile that you want to modify. The Edit VLAN Profile screen displays. This screen is identical to the Add VLAN Profile screen (see *Figure 52* on page 89).
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

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

1. On the LAN Setup screen for IPv4 (see *Figure 51* on page 88), select the check box to the left of each VLAN profile that you want to enable, disable, or delete, or click the **Select All** table button to select all profiles. (You cannot select the default VLAN profile.)
2. Click one of the following table buttons:
   - **Enable**. Enables the VLAN or VLANs. The ! status icon changes from a gray circle to a green circle, indicating that the selected VLAN or VLANs are enabled. (By default, when a VLAN is added to the table, it is automatically enabled.)
   - **Disable**. Disables the VLAN or VLANs. The ! status icon changes from a green circle to a gray circle, indicating that the selected VLAN or VLANs are disabled.
   - **Delete**. Deletes the VLAN or VLANs.

Configure VLAN MAC Addresses and LAN Advanced Settings

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

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

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

1. Select **Network Configuration > LAN Settings**. In the upper right of the screen, the IPv4 radio button is selected by default. The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings (see *Figure 51* on page 88).
2. Click the **Advanced** option arrow in the upper middle of the LAN Setup screen. The IPv4 LAN Advanced screen displays:

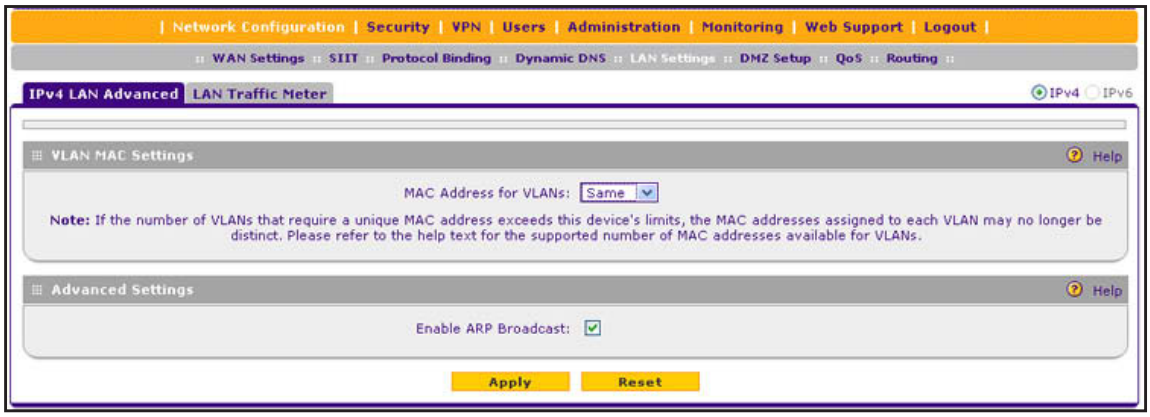

Figure 53.

3. From the MAC Address for VLANs drop-down list, select **Unique**. (The default is Same.)
4. As an option, you can disable the broadcast of ARP packets for the default VLAN by clearing the **Enable ARP Broadcast** check box. (The broadcast of ARP packets is enabled by default for the default VLAN.)
5. Click **Apply** to save your settings.

Note: If you attempt to configure more than 16 VLANs while the MAC address for VLANs is set to Unique on the IPv4 LAN Advanced screen, the MAC addresses that are assigned to each VLAN might no longer be distinct.

Note: For information about how to configure and enable the LAN traffic meter, see *Configure and Enable the LAN Traffic Meter* on page 359.

Configure IPv4 Multihome LAN IP Addresses on the Default VLAN

If you have computers using different IPv4 networks in the LAN (for example, 172.124.10.0 or 192.168.200.0), you can add aliases to the LAN ports and give computers on those networks access to the Internet, but you can do so only for the default VLAN. The IP address that is assigned as a secondary IP address needs to be unique and cannot be assigned to a VLAN.

Make sure 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 VPN firewall.

The following is an example of correctly configured IPv4 addresses:

- WAN IP address. 10.0.0.1 with subnet 255.0.0.0
- DMZ IP address. 176.16.2.1 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 IPv4 address:**

1. Select **Network Configuration > LAN Settings > LAN Multi-homing**. In the upper right of the screen, the IPv4 radio button is selected by default. The LAN Multi-homing screen displays the IPv4 settings. (The following figure contains one example.)

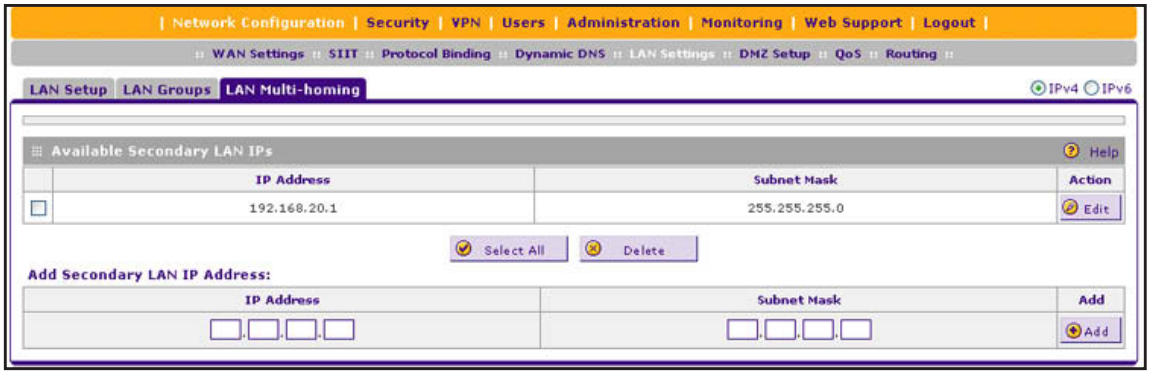

Figure 54.

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

2. In the Add Secondary LAN IP Address section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the LAN ports.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.
3. Click the **Add** table button in the rightmost column to add the secondary IP address to the Available Secondary LAN IPs table.

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

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

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

1. On the LAN Multi-homing screen for IPv4 (see the previous figure), click the **Edit** button in the Action column for the secondary IP address that you want to modify. The Edit LAN Multi-homing screen displays.

2. Modify the IP address or subnet mask, or both.
3. Click **Apply** to save your settings.

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

1. On the LAN Multi-homing screen for IPv4 (see the previous figure), select the check box to the left of each secondary IP address that you want to delete, or click the **Select All** table button to select secondary IP addresses.
2. Click the **Delete** table button.

Manage IPv4 Groups and Hosts (IPv4 LAN Groups)

- *Manage the Network Database*
- *Change Group Names in the Network Database*
- *Set Up DHCP Address Reservation*

The Known PCs and Devices table on the LAN Groups (IPv4) screen (see *Figure 55* on page 97) contains a list of all known computers and network devices that are assigned dynamic IP addresses by the VPN firewall, have been discovered by other means, or were entered manually. 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 computers 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 VPN firewall receives a reply to an ARP request, it might not be able to determine the device name if the software firewall of the device blocks the name.

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

These are some advantages of the network database:

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

- There is no need to reserve an IP address for a computer in the DHCP server. All IP address assignments made by the DHCP server are maintained until the computer 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 computer. Because the IP address allocated by the DHCP server never changes, you do not need to assign a fixed IP address to a computer to ensure that it always has the same IP address.
- A computer is identified by its MAC address—not its IP address. The network database uses the MAC address to identify each computer or device. Therefore, changing a computer's IP address does not affect any restrictions applied to that computer.
- Control over computers can be assigned to groups and individuals:
  - You can assign computers to groups (see *Manage the Network Database* on this page) and apply restrictions (outbound rules and inbound rules) to each group (see *Overview of Rules to Block or Allow Specific Kinds of Traffic* on page 136).
  - You can select groups that are allowed access to URLs that you have blocked for other groups, or the other way around, block access to URLs that you have allowed access to for groups (see *Configure Content Filtering* on page 186).
  - If necessary, you can also create firewall rules to apply to a single computer (see *Enable Source MAC Filtering* on page 190). Because the MAC address is used to identify each computer, users cannot avoid these restrictions by changing their IP address.

Manage the Network Database

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

To view the network database, select **Network Configuration > LAN Settings > LAN Groups**. The LAN Groups screen displays. (The following figure shows some manually added devices in the Known PCs and Devices table as an example.)

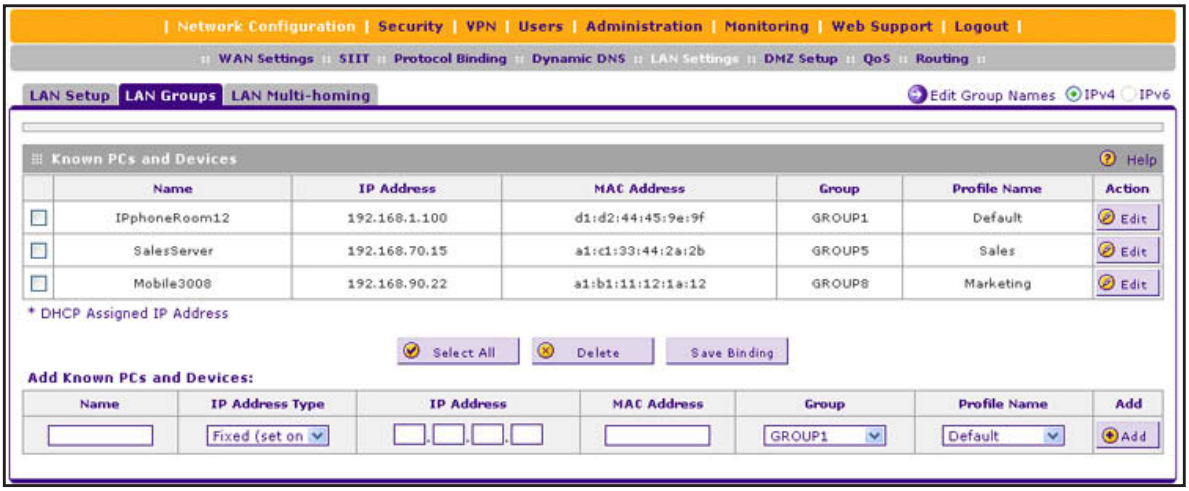

Figure 55.

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

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

Add Computers or Devices to the Network Database

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

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

Table 17. Add Known PCs and Devices section settings

Setting	Description
Name	Enter the name of the computer or device.
IP Address Type	From the drop-down list, select how the computer or device receives its IP address: • **Fixed (set on PC)**. The IP address is statically assigned on the computer or device. • **Reserved (DHCP Client)**. The DHCP server of the VPN firewall always assigns the specified IP address to this client during the DHCP negotiation (see also *Set Up DHCP Address Reservation* on page 101). **Note:** For both types of IP addresses, the VPN firewall reserves the IP address for the associated MAC address.

Table 17. Add Known PCs and Devices section settings (continued)

Setting	Description
IP Address	Enter the IP address that this computer or device is assigned to: • If the IP address type is Fixed (set on PC), the IP address needs to be outside of the address range that is allocated to the DHCP server pool to prevent the IP address from also being allocated by the DHCP server. • If the IP address type is Reserved (DHCP Client), the IP address can be inside or outside the address range that is allocated to the DHCP server pool. **Note:** Make sure that the IP address is in the IP subnet for the VLAN profile that you select from the Profile Name drop-down list.
MAC Address	Enter the MAC address of the computer's or device's network interface. The MAC address format is six colon-separated pairs of hexadecimal characters (0–9 and a–f), such as 01:23:d2:6f:89:ab.
Group	From the drop-down list, select the group to which the computer or device is assigned. (Group 1 is the default group.)
Profile Name	From the drop-down list, select the name of the VLAN profile to which the computer or device is assigned.

2. Click the **Add** table button to add the computer or device to the Known PCs and Devices table.
3. As an optional step: To save the binding between the IP address and MAC address for the entry that you just added to the Known PCs and Devices table, select the check box for the table entry, and click the **Save Binding** button.

Note: The saved binding is also displayed on the IP/MAC Binding screen (see *Figure 116* on page 193).

Edit Computers or Devices in the Network Database

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

1. In the Known PCs and Devices table of the LAN Groups screen (see *Figure 55* on page 97), click the **Edit** table button of a table entry. The Edit LAN Groups screen displays (see the following figure, which contains an example).

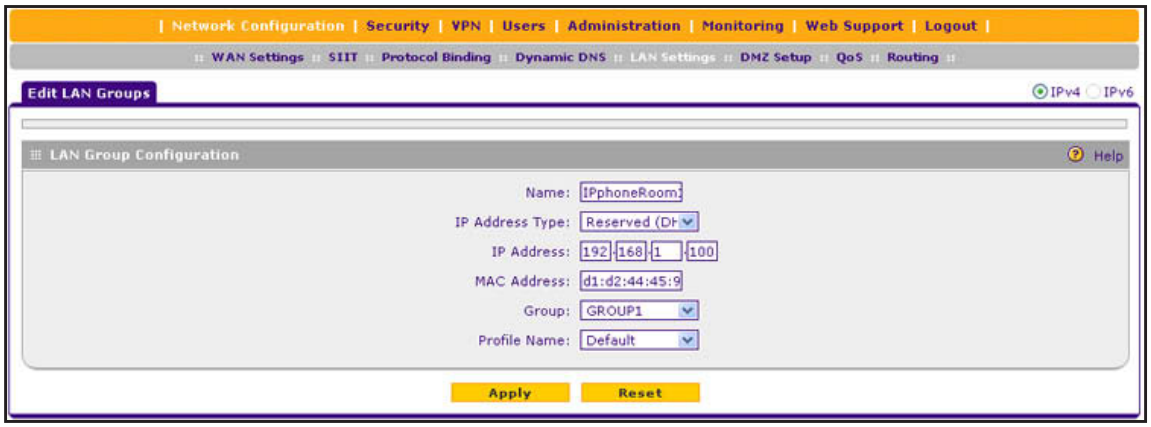

Figure 56.

2. Modify the settings as described in *Table 17* on page 98.
3. Click **Apply** to save your settings in the Known PCs and Devices table.

Deleting Computers or Devices from the Network Database

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

1. On the LAN Groups screen (see *Figure 55* on page 97), select the check box to the left of each computer or device that you want to delete, or click the **Select All** table button to select all computers and devices.
2. Click the **Delete** table button.

Note: If you delete a saved binding between an IP and MAC address on the LAN Groups screen, make sure that you also delete the binding on the IP/MAC Binding screen (see *Figure 116* on page 193).

Change Group Names in the Network Database

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

➢ **To edit the name of one of the eight available groups:**

1. Select **Network Configuration > LAN Settings > LAN Groups**. The LAN Groups screen displays (see *Figure 55* on page 97, which shows some examples in the Known PCs and Devices table).
2. Click the **Edit Group Names** option arrow to the right of the LAN submenu tabs. The Network Database Group Names screen displays. (The following figure shows some examples.)

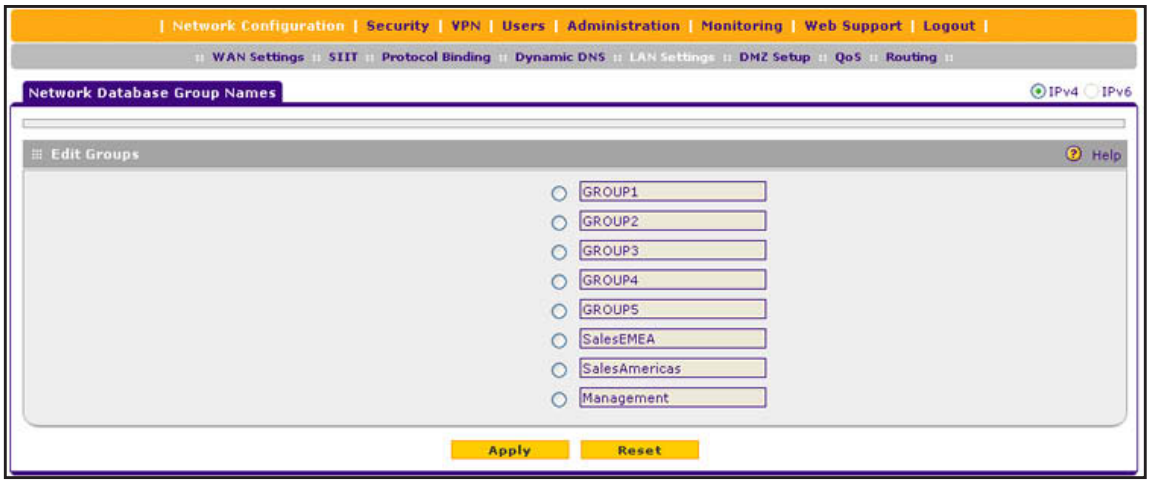

Figure 57.

3. Select the radio button next to the group name that you want to change.
4. Type a new name in the field. The maximum number of characters is 15. Do not use a double quote ("), single quote('), or space in the name.
5. Click **Apply** to save your settings.

Note: You can change only one group name at a time.

Set Up DHCP Address Reservation

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

To reserve and bind an IP address to a MAC address, select **Reserved (DHCP Client)** from the IP Address Type drop-down list on the LAN Groups screen and save the binding by clicking the Save Binding button on the same screen. For detailed steps, see *Add Computers or Devices to the Network Database* on page 98.

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

Note: The saved binding is also displayed on the IP/MAC Binding screen (see *Figure 116* on page 193).

Manage the IPv6 LAN

- *DHCPv6 Server Options*
- *Configure the IPv6 LAN*
- *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN*

An IPv6 LAN typically functions with site-local and link-local unicast addresses. Each physical interface requires an IPv6 link-local address that is automatically derived from the MAC addresses of the IPv4 interface and that is used for address configuration and neighbor discovery. (Normally, you would not manually configure a link-local address.)

Traffic with site-local or link-local addresses is never forwarded by the VPN firewall (or by any other router), that is, the traffic remains in the LAN subnet and is processed over the default VLAN only. A site-local address always starts with fec0 (hexadecimal); a link-local unicast address always starts with FE80 (hexadecimal). To forward traffic from sources with a site local or link-local unicast address in the LAN, a DHCP server is required. For more information about link-local unicast addresses, see *Configure ISATAP Automatic Tunneling* on page 65.

Because each interface is automatically assigned a link-local IP address, it is not useful to assign another link-local IP address as the default IPv6 LAN address. The default IPv6 LAN address is a site-local address. You can change this address to any other IPv6 address for LAN use.

Note: Site-local addresses, that is, addresses that start with fec0, have been depreciated. However, NETGEAR has implemented a site-local address as a *temporary* default IPv6 LAN address that you can replace with another LAN address. The firewall restricts external communication of this default site-local address.

DHCPv6 Server Options

The IPv6 clients in the LAN can autoconfigure their own IPv6 address or obtain an IPv6 address through a DHCPv6 server. For the LAN, there are three DHCPv6 options:

Stateless DHCPv6 Server

The IPv6 clients in the LAN generate their own IP address by using a combination of locally available information and router advertisements, but receive DNS server information from the DHCPv6 server. For stateless DHCPv6, you need to configure the RADVD and advertisement prefixes (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 109).

Stateless DHCPv6 Server With Prefix Delegation

As an option for a stateless DHCPv6 server, you can enable prefix delegation. The ISP's *stateful* DHCPv6 server assigns a prefix that is used by the VPN firewall's *stateless* DHCPv6 server to assign to its IPv6 LAN clients.

Prefix delegation functions in the following way:

1. The VPN firewall's DHCPv6 client requests prefix delegation from the ISP.

   You need to select the Prefix Delegation check box on the ISP IPv6 WAN Settings screen (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 55).

2. The ISP allocates a prefix to the VPN firewall.

   This prefix is automatically added to the List of Prefixes to Advertise table on the LAN RADVD screen for IPv6 (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 109).

3. The stateless DHCPv6 server allocates the prefix to the IPv6 LAN clients through the RADVD. When prefix delegation is enabled, the RADVD advertises the following prefixes:
   - The prefix that was added through prefix delegation.
   - Prefixes that you manually added to the List of Prefixes to Advertise table on the RADVD screen.

   You need to perform the following tasks:

   - Select the Prefix Delegation check box on the LAN Setup screen for IPv6 (see *Configure the IPv6 LAN* on page 104).
   - Configure the RADVD (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 109).
   - Optionally, manually add prefixes to the List of Prefixes for Prefix Delegation table on the LAN Setup screen for IPv6 (see *IPv6 LAN Prefixes for Prefix Delegation* on page 107).
   - Optionally, manually add prefixes to List of Prefixes to Advertise table on the RADVD screen (see *Advertisement Prefixes for the LAN* on page 111).

Stateful DHCPv6 Server

The IPv6 clients in the LAN obtain an interface IP address, configuration information such as DNS server information, and other parameters from the DHCPv6 server. The IP address is a dynamic address. For stateful DHCPv6, you need to configure IPv6 address pools (see *IPv6 LAN Address Pools* on page 106).

Configure the IPv6 LAN

➢ **To configure the IPv6 LAN settings:**

1. Select **Network Configuration > LAN Settings**.
2. In the upper right of the screen, select the **IPv6** radio button. The LAN Setup screen displays the IPv6 settings. (The following figure contains some examples.)

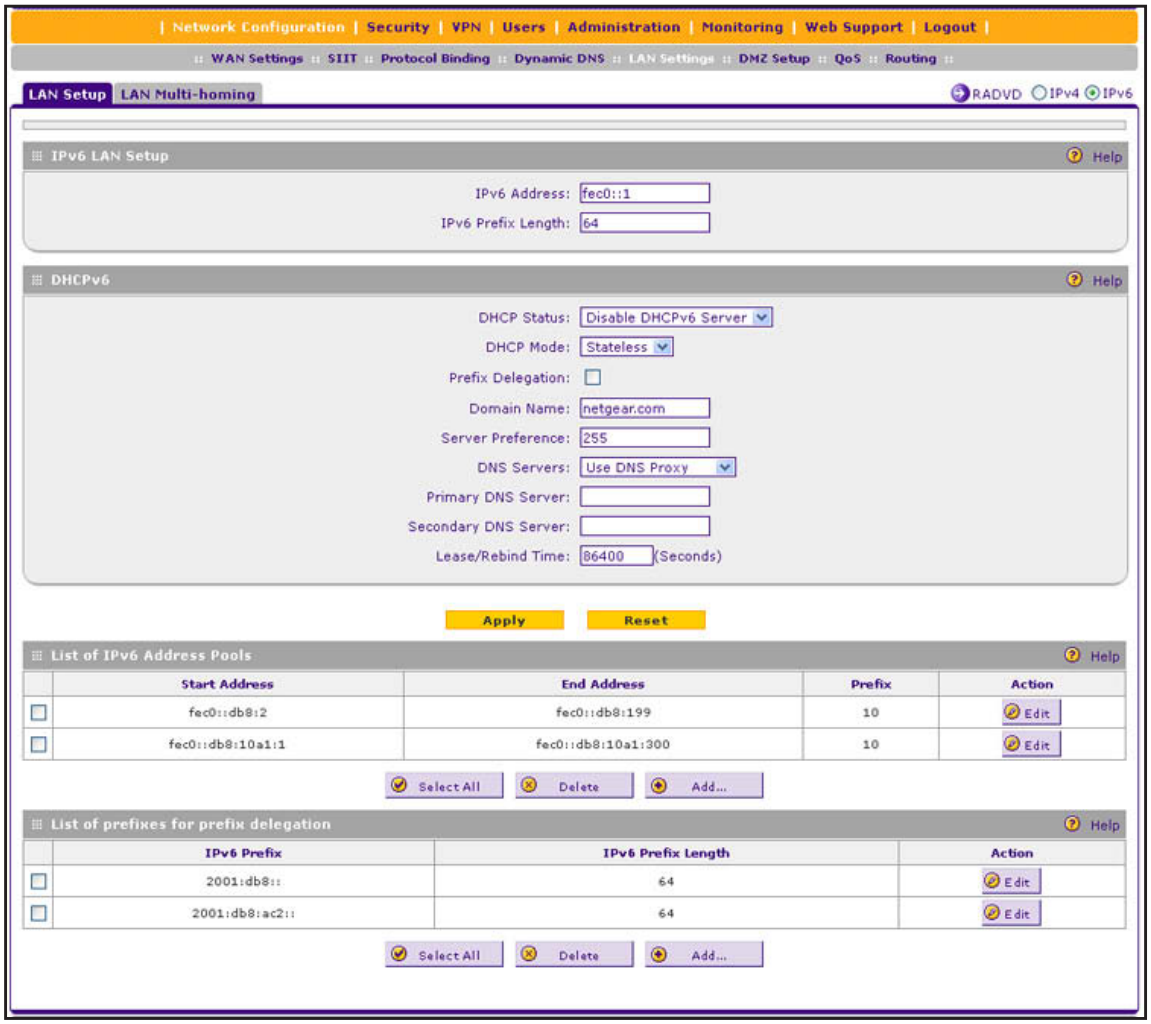

Figure 58.

3. Enter the settings as described in the following table. The IPv6 address pools and prefixes for prefix delegation are described in the sections following the table.

Table 18. LAN Setup screen settings for IPv6

Setting	Description	
IPv6 LAN Setup		
IPv6 Address	Enter the LAN IPv6 address. The default address is fec0::1.(For more information, see the introduction to this section, *Manage the IPv6 LAN*.)	
IPv6 Prefix Length	Enter the IPv6 prefix length, for example, 10 or 64. The default prefix length is 64.	
DHCPv6		
DHCP Status	Specify the status of the DHCPv6 server: • **Disable DHCPv6 Server**. This is the default setting, and the DHCPv6 fields are masked out. • **Enable the DHCPv6 Server**. If you enable the server, you need to complete the DHCPv6 fields.	
	DHCP Mode	Select one of the DHCPv6 modes from the drop-down list: • **Stateless**. The IPv6 clients generate their own IP address by using a combination of locally available information and router advertisements, but receive DNS server information from the DHCPv6 server. For stateless DHCPv6, you need to configure the RADVD and advertisement prefixes (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 109). As an option, you can enable prefix delegation (see the explanation further down in this table). • **Stateful**. The IPv6 clients obtain an interface IP address, configuration information such as DNS server information, and other parameters from the DHCPv6 server. The IP address is a dynamic address. You need to add IPv6 address pools to the List of IPv6 Address Pools table on the LAN Setup screen (see *IPv6 LAN Address Pools* on page 106).
	Prefix Delegation	If you have selected the *stateless* DHCPv6 mode, you can select the Prefix Delegation check box: • **Prefix delegation check box is selected**. The stateless DHCPv6 server assigns prefixes to its IPv6 LAN clients. Make sure that the Prefix Delegation check box on the WAN IPv6 ISP Settings screen is also selected (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 55) to enable the VPN firewall to acquire a prefix from the ISP through prefix delegation. In this configuration, a prefix is automatically added to the List of Prefixes to Advertise table on the LAN RADVD screen for IPv6 (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 109). • **Prefix delegation check box is cleared**. Prefix delegation is disabled in the LAN. This is the default setting.
	Domain Name	Enter the domain name of the DHCP server.

Table 18. LAN Setup screen settings for IPv6 (continued)

Setting	Description		
DHCP Status (continued)	Server Preference	Enter the DHCP server preference value. The possible values are 0–255, with 255 as the default setting. This is an optional setting that specifies the server's preference value in a server advertise message. The client selects the server with the highest preference value as the preferred server.	
	DNS Servers	Select one of the DNS server options from the drop-down lists: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers that you configured on the WAN IPv6 ISP Settings screen (see *Configure a Static IPv6 Internet Connection* on page 58). • **Use DNS from ISP**. The VPN firewall uses the ISP's DNS servers that you configured on the WAN IPv6 ISP Settings screen (see *Configure a Static IPv6 Internet Connection* on page 58). • **Use below**. When you select this option, the DNS server fields become available for you to enter IP addresses.	
		Primary DNS Server	Enter the IP address of the primary DNS server for the LAN.
		Secondary DNS Server	Enter the IP address of the secondary DNS server for the LAN.
	Lease/Rebind Time	Enter the period after which the DHCP lease is renewed with the original DHCP server or rebound with another DHCP server to extend the existing DHCP lease. The default period is 86400 seconds (24 hours).	

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

IPv6 LAN Address Pools

If you configure a *stateful* DHCPv6 server for the LAN, you need to add local DHCP IPv6 address pools so the DHCPv6 server can control the allocation of IPv6 addresses in the LAN.

➢ **To add an IPv6 LAN address pool:**

1. On the LAN Setup screen for IPv6, under the List of IPv6 Address Pools table, click **Add**. The LAN IPv6 Config screen displays:

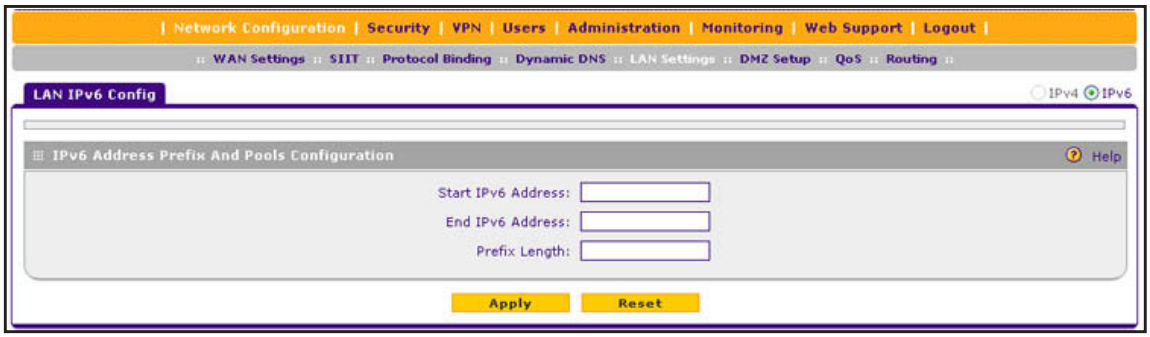

Figure 59.

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

Table 19. LAN IPv6 Config screen settings

Setting	Description
Start IPv6 Address	Enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCPv6 client joining the LAN is assigned an IP address between this address and the end IP address.
End IPv6 Address	Enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCPv6 client joining the LAN is assigned an IP address between the start IP address and this IP address.
Prefix Length	Enter the IPv6 prefix length, for example, 10 or 64.

3. Click **Apply** to save your changes and add the new IPv6 address pool to the List of IPv6 Address Pools table on the LAN Setup screen for IPv6.

- **To edit an IPv6 LAN address pool:**

1. On the LAN Setup screen for IPv6 (see *Figure 58* on page 104), click the **Edit** button in the Action column for the address pool that you want to modify. The LAN IPv6 Config screen displays.
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

- **To delete one or more IPv6 LAN address pools:**

1. On the LAN Setup screen for IPv6 (see *Figure 58* on page 104), select the check box to the left of each address pool that you want to delete, or click the **Select All** table button to select all address pools.
2. Click the **Delete** table button.

IPv6 LAN Prefixes for Prefix Delegation

If you configure a *stateless* DHCPv6 server for the LAN and select the Prefix Delegation check box (both on the ISP IPv6 WAN Settings screen and on the LAN Setup screen for IPv6, a prefix delegation pool is automatically added to the List of Prefixes for Prefix Delegation table. You can also manually add prefixes to the List of Prefixes for Prefix

Delegation table to enable the DHCPv6 server to assign these prefixes to its IPv6 LAN clients.

➢ **To add an IPv6 prefix:**

1. On the LAN Setup screen for IPv6, under the List of Prefixes for Prefix Delegation table, click **Add**. The Add Prefix Delegation Prefixes screen displays:

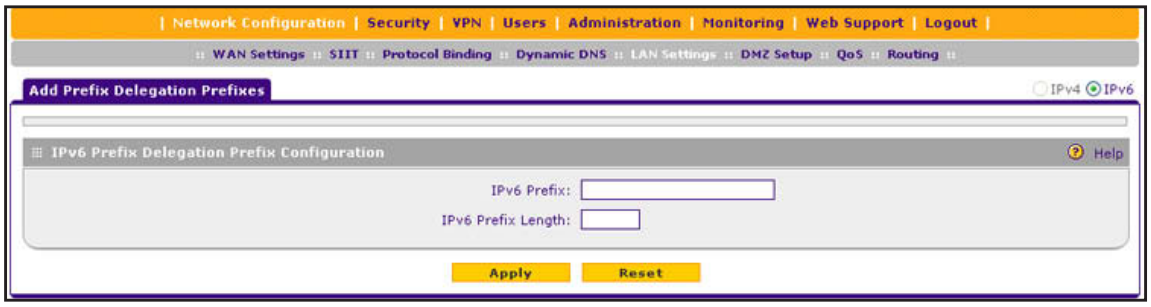

Figure 60.

2. Enter the following settings:
   - **IPv6 Prefix**. Enter a prefix, for example, 2001:db8::.
   - **IPv6 Prefix Length**. Enter the IPv6 prefix length, for example, 64.
3. Click **Apply** to save your changes and add the new prefix to the List of Prefixes for Prefix Delegation table on the LAN Setup screen for IPv6.

➢ **To edit a prefix:**

1. On the LAN Setup screen for IPv6 (see *Figure 58* on page 104), click the **Edit** button in the Action column for the prefix that you want to modify. The Edit Prefix Delegation Prefixes screen displays.
2. Modify the settings as described in *Step 2* of the previous procedure.
3. Click **Apply** to save your settings.

➢ **To delete one or more prefixes:**

1. On the LAN Setup screen for IPv6 (see *Figure 58* on page 104), select the check box to the left of each prefix that you want to delete, or click the **Select All** table button to select all prefixes.
2. Click the **Delete** table button.

Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN

Note: If you do not configure stateful DHCPv6 for the LAN but use stateless DHCPv6, you need to configure the Router Advertisement Deamon (RADVD) and advertisement prefixes.

The RADVD is an application that uses the Neighbor Discovery Protocol (NDP) to collect link-local advertisements of IPv6 addresses and IPv6 prefixes in the LAN. The RADVD then distributes this information in the LAN, which allows IPv6 clients to configure their own IPv6 address.

Hosts and routers in the LAN use NDP to determine the link-layer addresses and related information of neighbors in the LAN that can forward packets on their behalf. The VPN firewall periodically distributes router advertisements (RAs) throughout the LAN to provide such information to the hosts and routers in the LAN. RAs include IPv6 addresses, types of prefixes, prefix addresses, prefix lifetimes, the maximum transmission unit (MTU), and so on. In addition to configuring the RADVD, you also need to configure the prefixes that are advertised in the LAN RAs.

The following table provides an overview of how information is obtained in the LAN when you have configured a stateless DHCPv6 server and the RADVD:

Table 20. DHCPv6 and RADVD interaction in the LAN

Flags in the RADVD	DHCPv6 Server Provides	RADVD Provides
Managed RA flag is set	• IP address assignment • DNS server and other configuration information	• IP address assignment • Prefix • Prefix length • Gateway address
Other RA flag is set	DNS server and other configuration information	• IP address assignment • Prefix • Prefix length • Gateway address

When the Managed flag is set in the RADVD, the DHCPv6 server can assign IP addresses, and the RADVD also assigns IP addresses in the sense that it provides information that allows IPv6 clients to configure their own IPv6 address.

When the Other flag is set, the DHCPv6 server does not assign IP addresses but provides DNS server and other configuration information only.

➢ **To configure the Router Advertisement Daemon for the LAN:**

1. Select **Network Configuration > LAN Settings**.
2. In the upper right of the screen, select the **IPv6** radio button. The LAN Setup screen displays the IPv6 settings (see *Figure 58* on page 104.)
3. To the right of the LAN Setup tab, click the **RADVD** option arrow. The RADVD screen for the LAN displays. (The following figure contains some examples.)

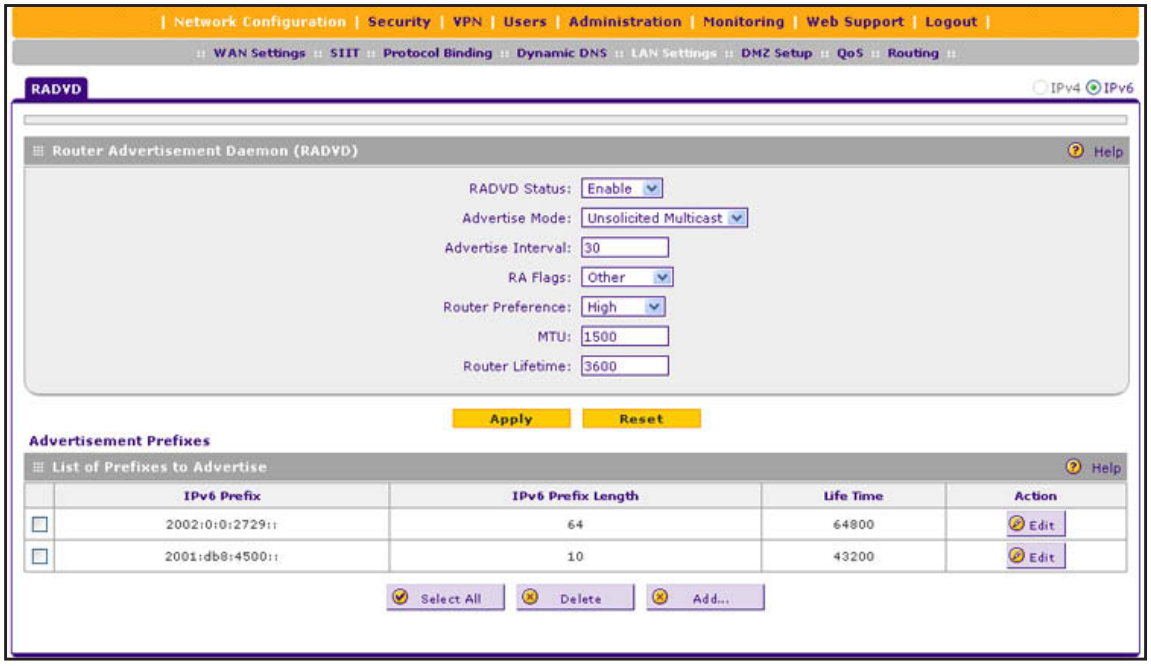

Figure 61.

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

Table 21. RADVD screen settings for the LAN

Setting	Description
RADVD Status	Specify the RADVD status by making a selection from the drop-down list: • **Enable**. The RADVD is enabled, and the RADVD fields become available for you to configure. • **Disable**. The RADVD is disabled, and the RADVD fields are masked out. This is the default setting.
Advertise Mode	Specify the advertisement mode by making a selection from the drop-down list: • **Unsolicited Multicast**. The VPN firewall advertises unsolicited multicast packets at a rate that is specified by the advertisement interval. • **Unicast only**. The VPN firewall responds to unicast packet requests only. No unsolicited packets are advertised. Select this option for nonbroadcast multiple access (NBMA) links such as ISATAP.
Advertise Interval	Enter the advertisement interval of unsolicited multicast packets in seconds. The minimum value is 10 seconds; the maximum value is 1800 seconds.

Table 21. RADVD screen settings for the LAN (continued)

Setting	Description
RA Flags	Specify what type of information the DHCPv6 server provides in the LAN by making a selection from the drop-down list: • **Managed**. The DHCPv6 server is used for autoconfiguration of the IP address. • **Other**. The DHCPv6 server is not used for autoconfiguration of the IP address, but other configuration information such as DNS information is available through the DHCPv6 server. **Note:** Irrespective of the RA flag settings, the RADVD provides information about the prefix, prefix length, and gateway addresses and is also used for autoconfiguration of the IP address.
Router Preference	Specify the VPN firewall's preference in relation to other hosts and routers in the LAN by making a selection from the drop-down list: • **Low**. The VPN firewall is treated as a nonpreferred router in the LAN. • **Medium**. The VPN firewall is treated as a neutral router in the LAN. • **High**. The VPN firewall is treated as a preferred router in the LAN.
MTU	The maximum transmission unit (MTU) size for a packet in one transmission over a link. The default setting is 1500.
Router Lifetime	The router lifetime specifies how long the default route that was created as a result of the router advertisement should remain valid. Enter the router lifetime in seconds. This is the period that the advertised prefixes are valid for route determination. The default period is 3600 seconds (one hour). The minimum value is 30 seconds; the maximum value is 9000 seconds.

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

Advertisement Prefixes for the LAN

You need to configure the prefixes that are advertised in the LAN RAs. For a 6to4 address, you need to specify only the site level aggregation identifier (SLA ID) and the prefix lifetime. For a global, local, or ISATAP address, you need to specify the prefix, prefix length, and prefix lifetime.

➢ **To add an advertisement prefix for the LAN:**

1. On the RADVD screen for the LAN, under the List of Prefixes to Advertise table, click **Add**. The Add Advertise Prefixes screen displays:

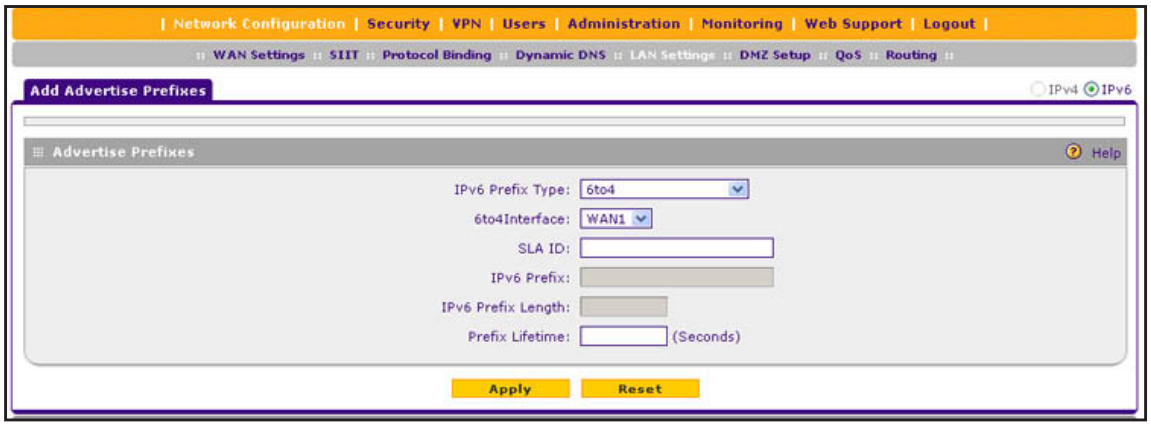

Figure 62.

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

Table 22. Add Advertise Prefixes screen settings for the LAN

Setting	Description
IPv6 Prefix Type	Specify the IPv6 prefix type by making a selection from the drop-down list: • **6to4**. The prefix is for a 6to4 address. You need to select a WAN interface from the 6to4Interface drop-down list, and complete the SLA ID field and Prefix Lifetime field. The other fields are masked out. • **Global/Local/ISATAP**. The prefix is for a global, local, or ISATAP address. This needs to be a global prefix or a site-local prefix; it cannot be a link-local prefix. You need to complete the IPv6 Prefix field, IPv6 Prefix Length field, and Prefix Lifetime field. The 6to4Interface drop-down list and SLA ID field are masked out.
6to4Interface	Select a WAN interface from the drop-down list.
SLA ID	Enter the site level aggregation identifier (SLA ID) for the 6to4 address prefix that should be included in the advertisement.
IPv6 Prefix	Enter the IPv6 prefix for the VPN firewall's LAN that should be included in the advertisement.
IPv6 Prefix Length	Enter the IPv6 prefix length (typically 64) that should be included in the advertisement.
Prefix Lifetime	The prefix lifetime specifies how long the IP address that was created as a result of the router advertisement should remain valid. Enter the prefix lifetime in seconds that should be included in the advertisement. The minimum period is 0 seconds; the maximum period is 65536 seconds.

3. Click **Apply** to save your changes and add the new IPv6 address pool to the List of Prefixes to Advertise table on the RADVD screen for the LAN.

➢ **To edit an advertisement prefix:**

1. On the RADVD screen for the LAN (see *Figure 61* on page 110), click the **Edit** button in the Action column for the advertisement prefix that you want to modify. The Add Advertisement Prefix screen displays.
2. Modify the settings as described in the previous table.

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

➢ **To delete one or more advertisement prefixes:**

1. On the RADVD screen for the LAN (see *Figure 61* on page 110), select the check box to the left of each advertisement prefix that you want to delete, or click the **Select All** table button to select all advertisement prefixes.
2. Click the **Delete** table button.

Configure IPv6 Multihome LAN IP Addresses on the Default VLAN

If you have computers using different IPv6 networks in the LAN (for example, fec0::2 or fec0::1000:10), you can add aliases to the LAN ports and give computers on those networks access to the Internet, but you can do so only for the default VLAN. The IP address that is assigned as a secondary IP address needs to be unique and cannot be assigned to a VLAN.

Make sure 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 VPN firewall. The following is an example of correctly configured IPv6 addresses:

- WAN IP address. 2000::e246:9aff:fe1d:1a9c with a prefix length of 64
- DMZ IP address. 176::e246:9aff:fe1d:a1bc with a prefix length of 64
- Primary LAN IP address. fec0::1 with a prefix length of 10
- Secondary LAN IP address. 2001:db8:3000::2192 with a prefix length of 10.

➢ **To add a secondary LAN IPv6 address:**

1. Select **Network Configuration > LAN Settings > LAN Multi-homing**.
2. In the upper right of the screen, select the **IPv6** radio button. The LAN Multi-homing screen displays the IPv6 settings. (The following figure contains one example.)

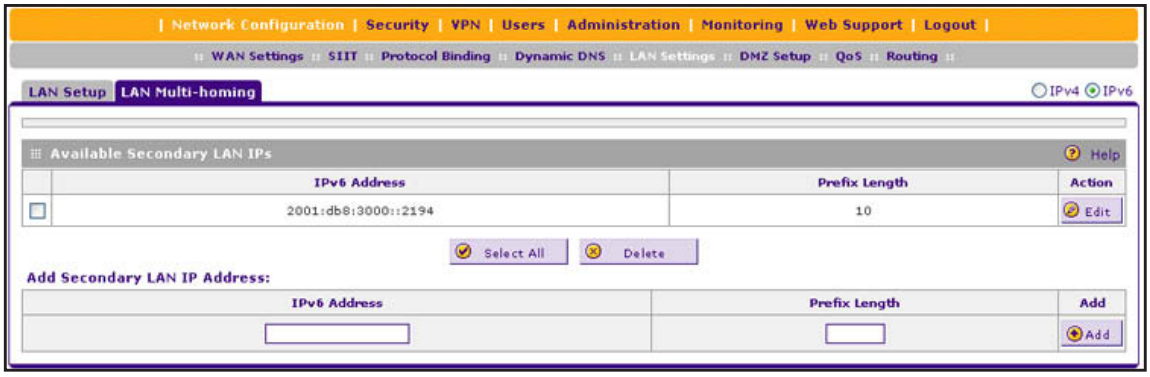

Figure 63.

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

3. In the Add Secondary LAN IP Address section of the screen, enter the following settings:
   - **IPv6 Address**. Enter the secondary address that you want to assign to the LAN ports.
   - **Prefix Length**. Enter the prefix length 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 2* and *Step 3* for each secondary IP address that you want to add to the Available Secondary LAN IPs table.

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

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

1. On the LAN Multi-homing screen for IPv6 (see the previous figure), click the **Edit** button in the Action column for the secondary IP address that you want to modify. The Edit LAN Multi-homing screen displays.
2. Modify the IP address or prefix length, or both.
3. Click **Apply** to save your settings.

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

1. On the LAN Multi-homing screen for IPv6 (see the previous figure), select the check box to the left of each secondary IP address that you want to delete, or click the **Select All** table button to select secondary IP addresses.
2. Click the **Delete** table button.

Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic

- *DMZ Port for IPv4 Traffic*
- *DMZ Port for IPv6 Traffic*
- *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the DMZ*

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions than the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. The rightmost LAN port on the VPN firewall 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 VPN firewall is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, local computers can run the application correctly if those computers are used on the DMZ port.

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

Note: For information about how to define the DMZ WAN rules and LAN DMZ rules, see *Configure DMZ WAN Rules* on page 152 and *Configure LAN DMZ Rules* on page 158, respectively.

Note: When you enable the DMZ port for IPv4 traffic, IPv6 traffic, or both, the DMZ LED next to LAN port 4 (see *Front Panel* on page 17) lights green to indicate that the DMZ port is enabled.

DMZ Port for IPv4 Traffic

The DMZ Setup (IPv4) screen lets you set up the DMZ port for IPv4 traffic. You can enable or disable the hardware DMZ port (LAN port 4; see *Front Panel* on page 17) and configure an IPv4 address and subnet mask for the DMZ port.

➢ **To enable and configure the DMZ port for IPv4 traffic:**

1. Select **Network Configuration > DMZ Setup**. In the upper right of the screen, the IPv4 radio button is selected by default. The DMZ Setup screen displays the IPv4 settings:

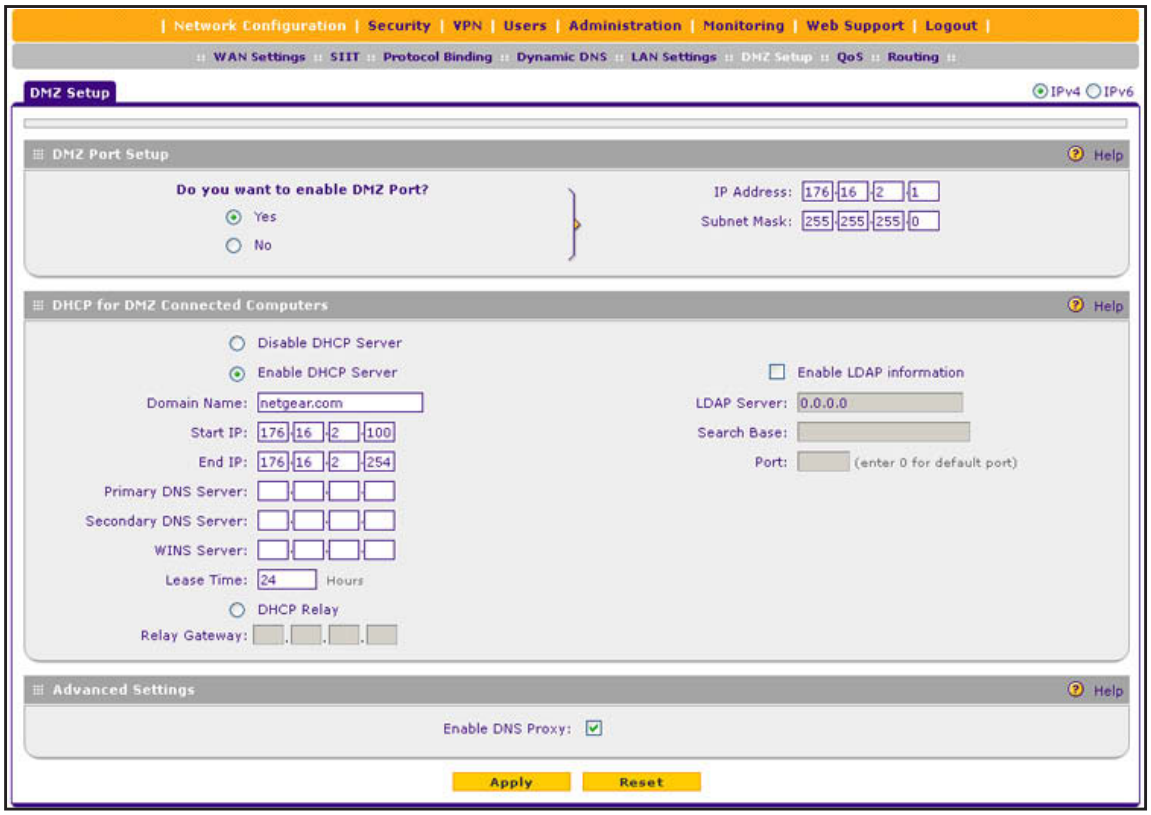

Figure 64.

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

Table 23. DMZ Setup screen settings for IPv4

Setting	Description	
DMZ Port Setup		
Do you want to enable DMZ Port?	Select one of the following radio buttons: • **Yes**. Enables you to configure the DMZ port settings. Fill in the IP Address and Subnet Mask fields. • **No**. Allows you to disable the DMZ port after you have configured it.	
	IP Address	Enter the IP address of the DMZ port. Make sure that the DMZ port IP address and LAN port IP address are in different subnets (for example, an address outside the LAN DHCP address pool, such as 192.168.1.101 when the LAN DHCP pool is 192.168.1.2–192.168.1.100). The default IP address for the DMZ port 176.16.2.1.
	Subnet Mask	Enter the IP subnet mask of the DMZ port. The subnet mask specifies the network number portion of an IP address. The subnet mask for the DMZ port is 255.255.255.0.

Table 23. DMZ Setup screen settings for IPv4 (continued)

Setting	Description	
DHCP for DMZ Connected Computers		
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you intend to 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 VPN firewall to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the VLAN. Enter the following settings:	
	Domain Name	This setting is optional. Enter the domain name of the VPN firewall.
	Start IP Address	Enter the start 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 end IP address. The default IP address 176.16.2.100.
	End IP Address	Enter the end 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 start IP address and this IP address. The default IP address 176.16.2.254. **Note:** The start and end DHCP IP addresses should be in the same network as the LAN TCP/IP address of the VPN firewall (that is, the IP address in the DMZ Port Setup section as described earlier in this table).
	Primary DNS Server	This setting is optional. If an IP address is specified, the VPN firewall provides this address as the primary DNS server IP address. If no address is specified, the VPN firewall provides its own LAN IP address as the primary DNS server IP address.
	Secondary DNS Server	This setting is optional. If an IP address is specified, the VPN firewall provides this address as the secondary DNS server IP address.
	WINS Server	This setting is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.
DHCP Relay	To use the VPN firewall as a DHCP relay agent for a DHCP server somewhere else in your network, select the **DHCP Relay** radio button. Enter the following setting:	
	Relay Gateway	The IP address of the DHCP server for which the VPN firewall serves as a relay.

Table 23. DMZ Setup screen settings for IPv4 (continued)

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

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

DMZ Port for IPv6 Traffic

The DMZ Setup (IPv6) screen lets you set up the DMZ port for IPv6 traffic. You can enable or disable the hardware DMZ port (LAN port 4; see *Front Panel* on page 17) for IPv6 traffic and configure an IPv6 address and prefix length for the DMZ port.

The IPv6 clients in the DMZ can autoconfigure their own IPv6 address or obtain an IPv6 address through a DHCPv6 server.

For the DMZ, there are two DHCPv6 server options:

- **Stateless DHCPv6 server**. The IPv6 clients in the DMZ generate their own IP address by using a combination of locally available information and router advertisements, but receive DNS server information from the DHCPv6 server. For stateless DHCPv6, you need to configure the RADVD and advertisement prefixes (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the DMZ* on page 122).
- **Stateful DHCPv6 server**. The IPv6 clients in the DMZ obtain an interface IP address, configuration information such as DNS server information, and other parameters from the DHCPv6 server. The IP address is a dynamic address. For stateful DHCPv6, you need to configure IPv6 address pools (see *IPv6 DMZ Address Pools* on page 121).

➢ **To enable and configure the DMZ port for IPv6 traffic:**

1. Select **Network Configuration > DMZ Setup**.
2. In the upper right of the screen, select the **IPv6** radio button. The DMZ Setup screen displays the IPv6 settings:

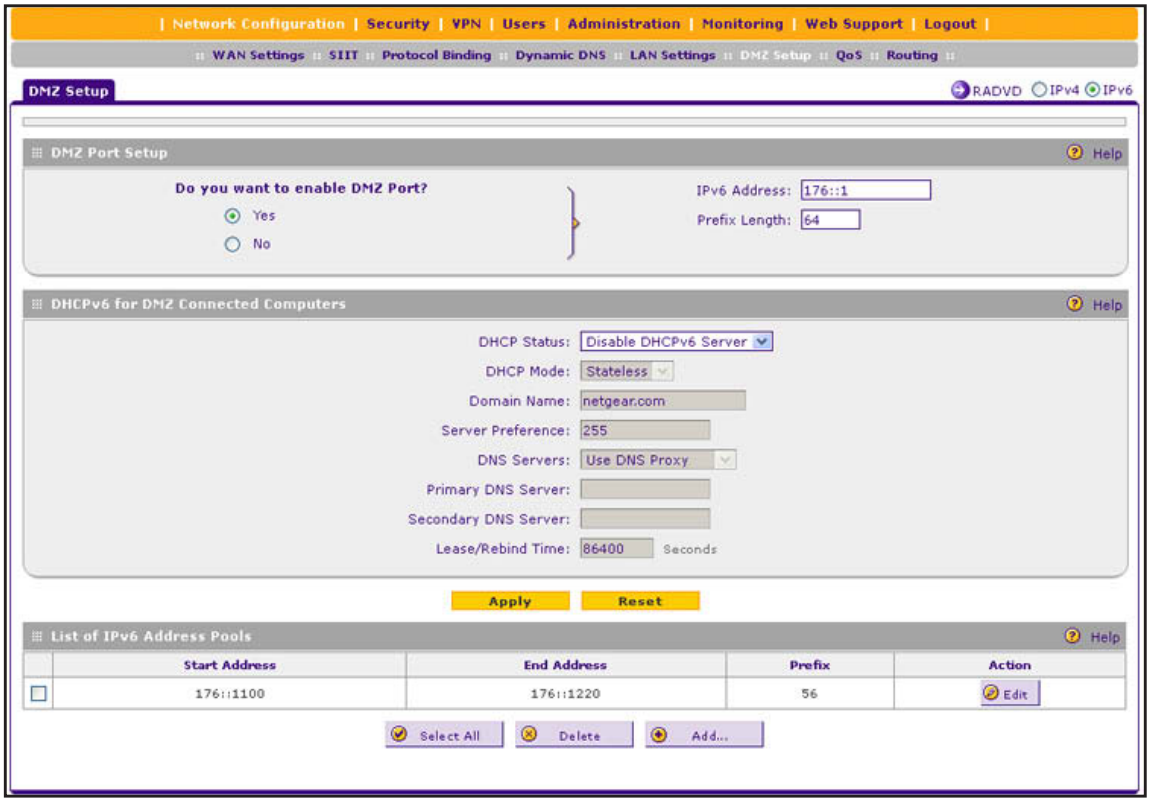

Figure 65.

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

Table 24. DMZ Setup screen settings for IPv6

Setting	Description	
DMZ Port Setup		
Do you want to enable DMZ Port?	Select one of the following radio buttons: • **Yes**. Enables you to configure the DMZ port settings. Fill in the IP Address and Subnet Mask fields. • **No**. Allows you to disable the DMZ port after you have configured it.	
	IPv6 Address	Enter the IP address of the DMZ port. Make sure that the DMZ port IP address, LAN port IP address, and WAN port IP address are in different subnets. The default IP address for the DMZ port is 176::1.
	Prefix Length	Enter the IPv6 prefix length, for example, 10 or 64. The default prefix length for the DMZ port is 64.
DHCPv6 for DMZ Connected Computers		
DHCP Status	Specify the status of the DHCPv6 server: • **Disable DHCPv6 Server**. This is the default setting, and the DHCPv6 fields are masked out. • **Enable the DHCPv6 Server**. If you enable the server, you need to complete the DHCPv6 fields.	
	DHCP Mode	Select one of the DHCPv6 modes from the drop-down list: • **Stateless**. The IPv6 clients generate their own IP address by using a combination of locally available information and router advertisements, but receive DNS server information from the DHCPv6 server. For stateless DHCPv6, you need to configure the RADVD and advertisement prefixes (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the DMZ* on page 122). • **Stateful**. The IPv6 clients obtain an interface IP address, configuration information such as DNS server information, and other parameters from the DHCPv6 server. The IP address is a dynamic address. (see *IPv6 DMZ Address Pools* on page 121).
	Domain Name	Enter the domain name of the DHCP server.
	Server Preference	Enter the DHCP server preference value. The possible values are 0–255, with 255 as the default setting. This is an optional setting that specifies the server's preference value in a server advertise message. The client selects the server with the highest preference value as the preferred server.

Table 24. DMZ Setup screen settings for IPv6 (continued)

Setting	Description		
DHCP Status (continued)	DNS Server	Select one of the DNS server options from the drop-down lists: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers that you configured on the WAN IPv6 ISP Settings screen (see *Configure a Static IPv6 Internet Connection* on page 58). • **Use DNS from ISP**. The VPN firewall uses the ISP's DNS servers that you configured on the WAN ISP IPv6 Settings screen (see *Configure a Static IPv6 Internet Connection* on page 58). • **Use below**. When you select this option, the DNS server fields become available for you to enter IP addresses.	
		Primary DNS Server	Enter the IP address of the primary DNS server for the DMZ.
		Secondary DNS Server	Enter the IP address of the secondary DNS server for the DMZ.
	Lease/Rebind Time	Enter the period after which the DHCP lease is renewed with the original DHCP server or rebound with another DHCP server to extend the existing DHCP lease. The default period is 86400 seconds (24 hours).	

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

IPv6 DMZ Address Pools

If you configure a stateful DHCPv6 server for the DMZ, you need to add local DHCP IPv6 address pools so the DHCPv6 server can control the allocation of IPv6 addresses in the DMZ.

➢ **To add an IPv6 DMZ address pool:**

1. On the DMZ Setup screen for IPv6 (see *Figure 65* on page 119), under the List of IPv6 Address Pools table, click **Add**. The DMZ IPv6 Config screen displays:

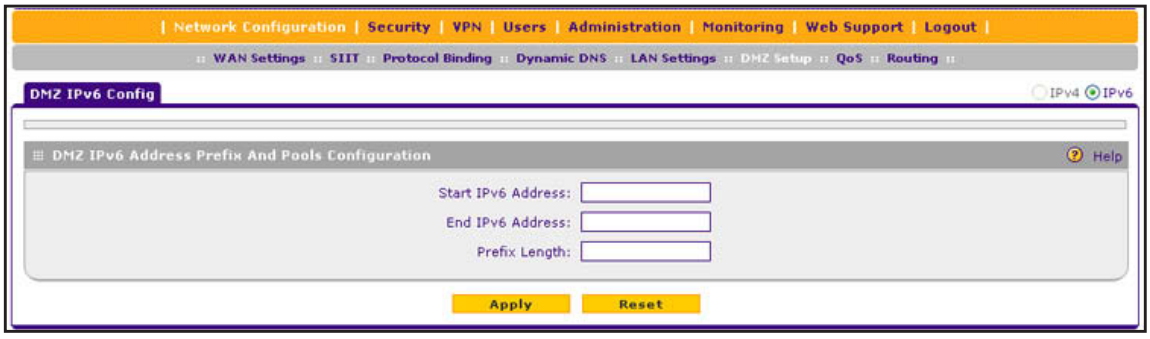

Figure 66.

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

Table 25. DMZ IPv6 Config screen settings

Setting	Description
Start IPv6 Address	Enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCPv6 client joining the DMZ is assigned an IP address between this address and the end IP address.
End IPv6 Address	Enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCPv6 client joining the DMZ is assigned an IP address between the start IP address and this IP address.
Prefix Length	Enter the IPv6 prefix length, for example, 10 or 64.

3. Click **Apply** to save your changes and add the new IPv6 address pool to the List of IPv6 Address Pools table on the DMZ Setup (IPv6) screen.

- **To edit an IPv6 DMZ address pool:**

1. On the DMZ Setup screen for IPv6 (see *Figure 65* on page 119), click the **Edit** button in the Action column for the address pool that you want to modify. The DMZ IPv6 Config screen displays.
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

- **To delete one or more IPv6 DMZ address pools:**

1. On the DMZ Setup screen for IPv6 (see *Figure 65* on page 119), select the check box to the left of each address pool that you want to delete, or click the **Select All** table button to select all address pools.
2. Click the **Delete** table button.

Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the DMZ

Note: If you do not configure stateful DHCPv6 for the DMZ but use stateless DHCPv6, you need to configure the Router Advertisement Deamon (RADVD) and advertisement prefixes.

The RADVD is an application that uses the Neighbor Discovery Protocol (NDP) to collect link-local advertisements of IPv6 addresses and IPv6 prefixes in the DMZ. The RADVD then distributes this information in the DMZ, which allows IPv6 clients to configure their own IPv6 address.

Hosts and routers in the LAN use NDP to determine the link-layer addresses and related information of neighbors in the LAN that can forward packets on their behalf. The VPN firewall periodically distributes router advertisements (RAs) throughout the DMZ to provide such information to the hosts and routers in the DMZ. RAs include IPv6 addresses, types of prefixes, prefix addresses, prefix lifetimes, the maximum transmission unit (MTU), and so on. In addition to configuring the RADVD, you also need to configure the prefixes that are advertised in the DMZ RAs.

The following table provides an overview of how information is obtained in the DMZ when you have configured a stateless DHCPv6 server and the RADVD:

Table 26. DHCPv6 and RADVD interaction in the DMZ

Flags in the RADVD	DHCPv6 Server Provides	RADVD Provides
Managed RA flag is set	• IP address assignment • DNS server and other configuration information	• IP address assignment • Prefix • Prefix length • Gateway address
Other RA flag is set	DNS server and other configuration information	• IP address assignment • Prefix • Prefix length • Gateway address

When the Managed flag is set in the RADVD, the DHCPv6 server can assign IP addresses, and the RADVD also assigns IP addresses in the sense that it provides information that allows IPv6 clients to configure their own IPv6 address.

When the Other flag is set, the DHCPv6 server does not assign IP addresses but provides DNS server and other configuration information only.

➢ **To configure the Router Advertisement Daemon for the DMZ:**

1. Select **Network Configuration > DMZ Setup**.
2. In the upper right of the screen, select the **IPv6** radio button. The DMZ Setup screen displays the IPv6 settings (see *Figure 65* on page 119).
3. Click the **RADVD** option arrow to the right of the DMZ Setup tab. The RADVD screen for the DMZ displays. (The following figure contains some examples.)

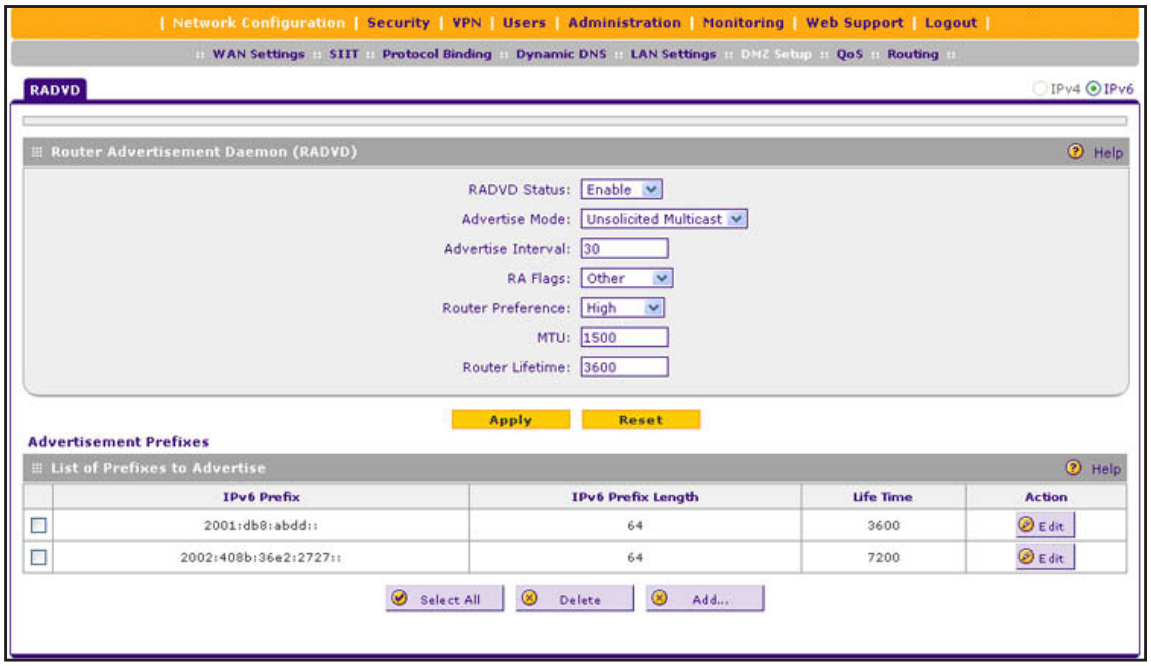

Figure 67.

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

Table 27. RADVD screen settings for the DMZ

Setting	Description
RADVD Status	Specify the RADVD status by making a selection from the drop-down list: • **Enable**. The RADVD is enabled, and the RADVD fields become available for you to configure. • **Disable**. The RADVD is disabled, and the RADVD fields are masked out. This is the default setting.
Advertise Mode	Specify the advertisement mode by making a selection from the drop-down list: • **Unsolicited Multicast**. The VPN firewall advertises unsolicited multicast packets at a rate that is specified by the advertisement interval. • **Unicast only**. The VPN firewall responds to unicast packet requests only. No unsolicited packets are advertised. Select this option for nonbroadcast multiple access (NBMA) links such as ISATAP.
Advertise Interval	Enter the advertisement interval of unsolicited multicast packets in seconds. The minimum value is 10 seconds; the maximum value is 1800 seconds.

Table 27. RADVD screen settings for the DMZ (continued)

Setting	Description
RA Flags	Specify what type of information the DHCPv6 server provides in the DMZ by making a selection from the drop-down list: • **Managed**. The DHCPv6 server is used for autoconfiguration of the IP address. • **Other**. The DHCPv6 server is not used for autoconfiguration of the IP address, but other configuration information such as DNS information is available through the DHCPv6 server. **Note:** Irrespective of the RA flag settings, the RADVD provides information about the prefix, prefix length, and gateway addresses and is also used for autoconfiguration of the IP address.
Router Preference	Specify the VPN firewall's preference in relation to other hosts and routers in the DMZ by making a selection from the drop-down list: • **Low**. The VPN firewall is treated as a nonpreferred router in the DMZ. • **Medium**. The VPN firewall is treated as a neutral router in the DMZ. • **High**. The VPN firewall is treated as a preferred router in the DMZ.
MTU	The maximum transmission unit (MTU) size for a packet in one transmission over a link. The default setting is 1500.
Router Lifetime	The router lifetime specifies how long the default route that was created as a result of the router advertisement should remain valid. Enter the router lifetime in seconds. This is the period that the advertised prefixes are valid for route determination. The default period is 3600 seconds (one hour). The minimum value is 30 seconds; the maximum value is 9000 seconds.

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

Advertisement Prefixes for the DMZ

You need to configure the prefixes that are advertised in the DMZ RAs. For a 6to4 address, you need to specify only the site level aggregation identifier (SLA ID) and the prefix lifetime. For a global, local, or ISATAP address, you need to specify the prefix, prefix length, and prefix lifetime.

➢ **To add an advertisement prefix for the DMZ:**

1. On the RADVD screen for the DMZ, under the List of Prefixes to Advertise table, click **Add**. The Add Advertisement Prefix screen displays:

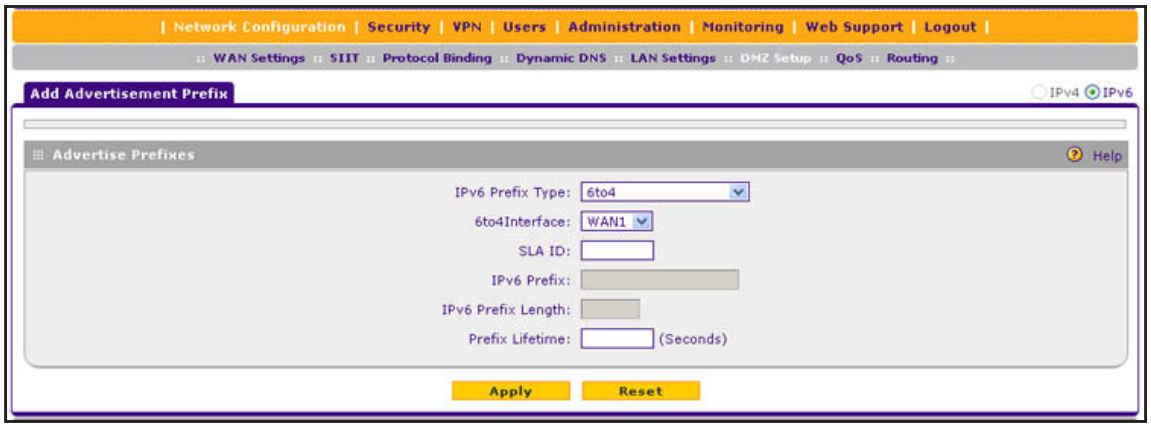

Figure 68.

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

Table 28. Add Advertisement Prefix screen settings for the DMZ

Setting	Description
IPv6 Prefix Type	Specify the IPv6 prefix type by making a selection from the drop-down list: • **6to4**. The prefix is for a 6to4 address. You need to select a WAN interface from the 6to4Interface drop-down list, and complete the SLA ID field and Prefix Lifetime field. The other fields are masked out. • **Global/Local/ISATAP**. The prefix is for a global, local, or ISATAP address. This needs to be a global prefix or a site-local prefix; it cannot be a link-local prefix. You need to complete the IPv6 Prefix field, IPv6 Prefix Length field, and Prefix Lifetime field. The 6to4Interface drop-down list and SLA ID field are masked out.
6to4Interface	Select a WAN interface from the drop-down list.
SLA ID	Enter the site level aggregation identifier (SLA ID) for the 6to4 address prefix that should be included in the advertisement.
IPv6 Prefix	Enter the IPv6 prefix for the VPN firewall's DMZ that should be included in the advertisement.
IPv6 Prefix Length	Enter the IPv6 prefix length (typically 64) that should be included in the advertisement.
Prefix Lifetime	The prefix lifetime specifies how long the IP address that was created as a result of the router advertisement should remain valid. Enter the prefix lifetime in seconds that should be included in the advertisement. The minimum period is 0 seconds; the maximum period is 65536 seconds.

3. Click **Apply** to save your changes and add the new IPv6 address pool to the List of Prefixes to Advertise table on the RADVD screen for the DMZ.

➢ **To edit an advertisement prefix:**

1. On the RADVD screen for the DMZ (see *Figure 67* on page 124), click the **Edit** button in the Action column for the advertisement prefix that you want to modify. The Add Advertisement Prefix screen displays.
2. Modify the settings as described in the previous table.

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

➢ **To delete one or more advertisement prefixes:**

1. On the RADVD screen for the DMZ screen (see *Figure 67* on page 124), select the check box to the left of each advertisement prefix that you want to delete, or click the **Select All** table button to select all advertisement prefixes.
2. Click the **Delete** table button.

Manage Static IPv4 Routing

- *Configure Static IPv4 Routes*
- *Configure the Routing Information Protocol*
- *IPv4 Static Route Example*

Static routes provide additional routing information to your VPN firewall. Under normal circumstances, the VPN firewall 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 on your network.

Note: The VPN firewall automatically sets up routes between VLANs and secondary IPv4 addresses that you have configured on the LAN Multi-homing (IPv4) screen (see *Configure IPv4 Multihome LAN IP Addresses on the Default VLAN* on page 94). Therefore, you do not need to manually add an IPv4 static route between a VLAN and a secondary IPv4 address.

Configure Static IPv4 Routes

➢ **To add an IPv4 static route to the Static Route table:**

1. Select **Network Configuration > Routing**. In the upper right of the screen, the IPv4 radio button is selected by default. The Static Routing screen displays the IPv4 settings. (The following figure contains one example.)

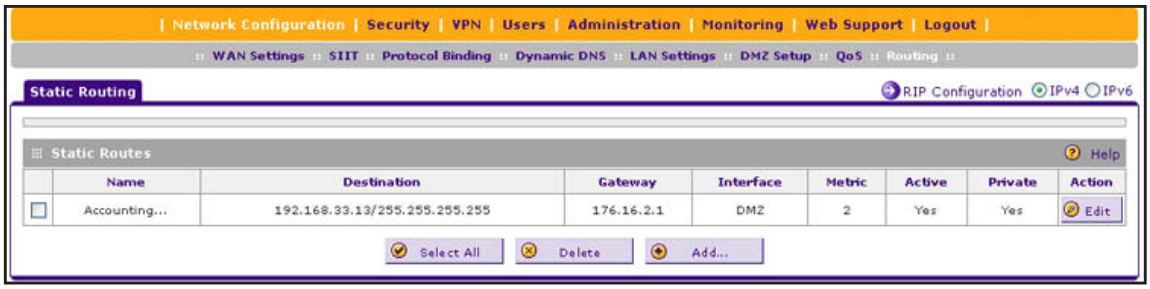

Figure 69.

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

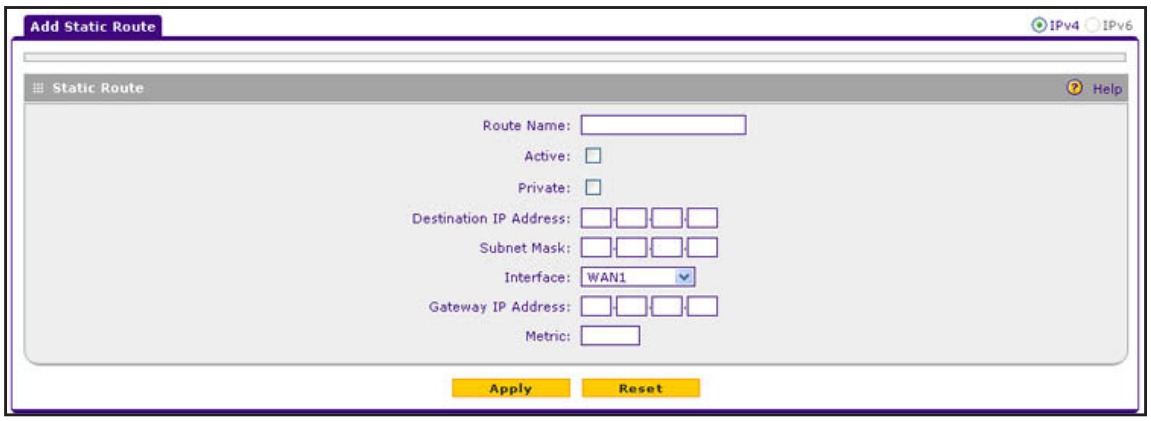

Figure 70.

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

Table 29. Add Static Route screen settings for IPv4

Setting	Description
Route Name	The route name for the static route (for purposes of identification and management).
Active	To make the static route effective, select the **Active** check box. **Note:** A route can be added to the table and made inactive if not needed. This allows you to use routes as needed without deleting and re-adding the entry. An inactive route is not advertised if RIP is enabled.
Private	If you want to limit access to the LAN only, select the **Private** check box. Doing so prevents the static route from being advertised in RIP.
Destination IP Address	The destination IP address of the host or network to which the route leads.
Subnet Mask	The IP subnet mask of the host or network to which the route leads. If the destination is a single host, enter **255.255.255.255**.
Interface	From the drop-down list, select the physical or virtual network interface (the WAN1, WAN2, WAN3, or WAN4 interface, a VLAN, or the DMZ interface) through which the route is accessible.
Gateway IP Address	The gateway IP address through which the destination host or network can be reached.
Metric	The priority of the route. Select a value between 2 and 15. If multiple routes to the same destination exist, the route with the lowest metric is used.

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

➢ **To edit an IPv4 static route:**

1. On the Static Routing screen for IPv4 (see *Figure 69* on page 127), click the **Edit** button in the Action column for the route that you want to modify. The Edit Static Route screen

displays. This screen is identical to the Add Static Route screen (see the previous figure).

2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more routes:**

1. On the Static Routing screen for IPv4 (see *Figure 69* on page 127), select the check box to the left of each route that you want to delete, or click the **Select All** table button to select all routes.
2. Click the **Delete** table button.

Configure the Routing Information Protocol

Routing Information Protocol (RIP), RFC 2453, is an Interior Gateway Protocol (IGP) that is commonly used in internal IPv4 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. RIP does not apply to IPv6.

➢ **To enable and configure RIP:**

1. Select **Network Configuration > Routing**. In the upper right of the screen, the IPv4 radio button is selected by default. The Static Routing screen displays the IPv4 settings (see *Figure 69* on page 127).
2. Click the **RIP Configuration** option arrow to the right of the Static Routing submenu tab. The RIP Configuration screen displays. (The following figure contains some examples.)

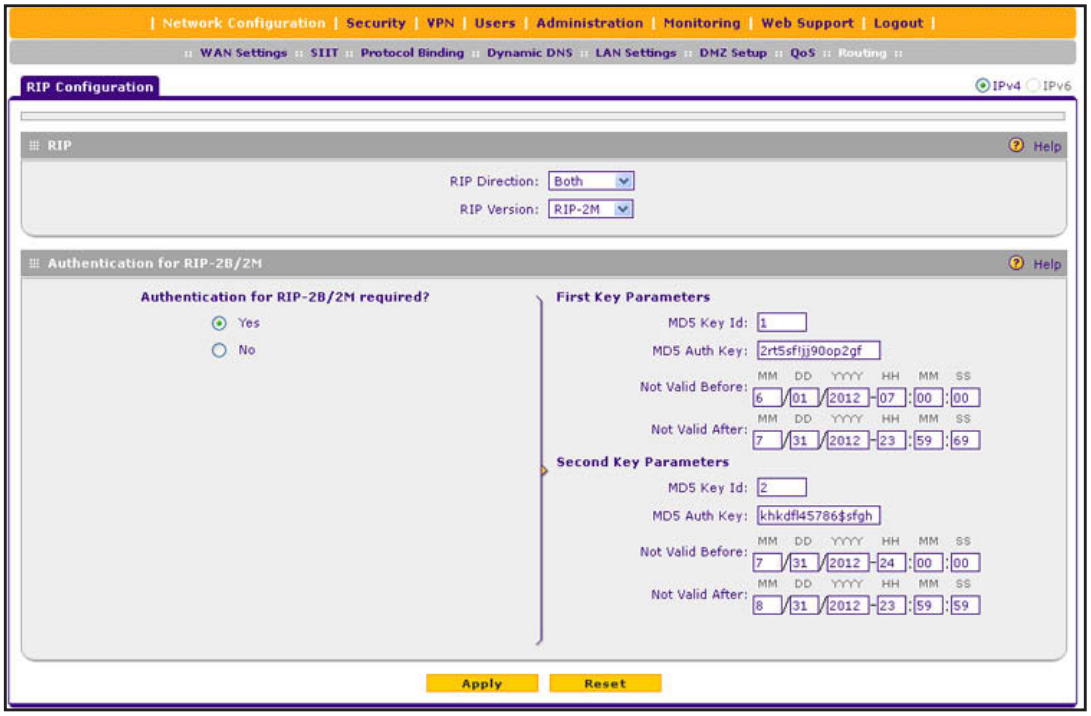

Figure 71.

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

Table 30. RIP Configuration screen settings

Setting	Description	
RIP		
RIP Direction	From the RIP Direction drop-down list, select the direction in which the VPN firewall sends and receives RIP packets: • **None**. The VPN firewall neither advertises its route table, nor accepts any RIP packets from other routers. This effectively disables RIP, and is the default setting. • **In Only**. The VPN firewall accepts RIP information from other routers but does not advertise its routing table. • **Out Only**. The VPN firewall advertises its routing table but does not accept RIP information from other routers. • **Both**. The VPN firewall advertises its routing table and also processes RIP information received from other routers.	
RIP Version	By default, the RIP version is set to Disabled. From the RIP Version drop-down list, select the version: • **RIP-1**. Classful routing that does not include subnet information. This is the most commonly supported version. • **RIP-2**. Routing that supports subnet information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format: - **RIP-2B**. Sends the routing data in RIP-2 format and uses subnet broadcasting. - **RIP-2M**. Sends the routing data in RIP-2 format and uses multicasting.	
Authentication for RIP-2B/2M		
Authentication for RIP-2B/2M required?	Authentication for RP-2B or RIP-2M is disabled by default, that is, the No radio button is selected. To enable authentication for RP-2B or RIP-2M, select the **Yes** radio button, and enter the settings for the following fields.	
	First Key Parameters	
	MD5 Key Id	The identifier for the key that is used for authentication.
	MD5 Auth Key	The password that is used for MD5 authentication.
	Not Valid Before	The beginning of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. Before this date and time, the MD5 key is not valid.
	Not Valid After	The end of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. After this date and time, the MD5 key is no longer valid.
	Second Key Parameters	
	MD5 Key Id	The identifier for the key that is used for authentication.
	MD5 Auth Key	The password that is used for MD5 authentication.

Table 30. RIP Configuration screen settings (continued)

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

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

IPv4 Static Route Example

In this example, we assume the following:

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

When you first configured the VPN firewall, 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 VPN firewall forwards your request to the ISP. In turn, the ISP forwards your request to the remote network, where the request is likely to be denied by the remote network's firewall.

In this case, you need to define a static route, informing the VPN firewall 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 VPN firewall needs to be defined as follows:

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

Manage Static IPv6 Routing

NETGEAR's implementation of IPv6 does not support RIP next generation (RIPng) to exchange routing information, and dynamic changes to IPv6 routes are not possible. To enable routers to exchange information over a static IPv6 route, you need to manually configure the static route information on each router.

➢ **To add an IPv6 static route to the Static Route table:**

1. Select **Network Configuration > Routing**.
2. In the upper right of the screen, select the **IPv6** radio button. The Static Routing screen displays the IPv6 settings:

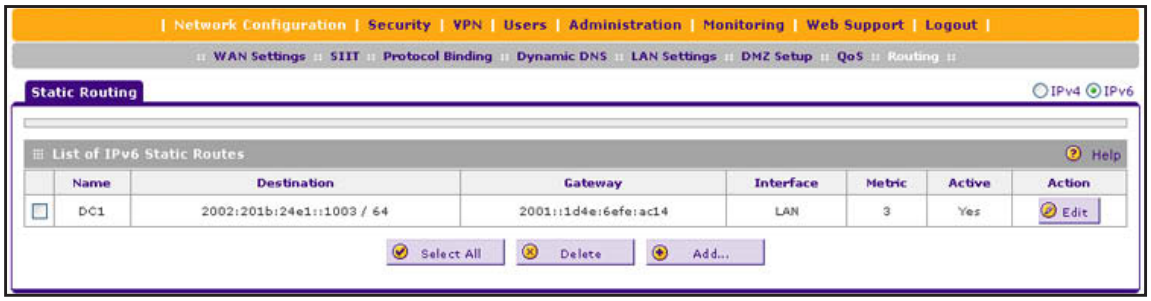

Figure 72.

3. Click the **Add** table button under the Static Routes table. The Add IPv6 Static Routing screen displays:

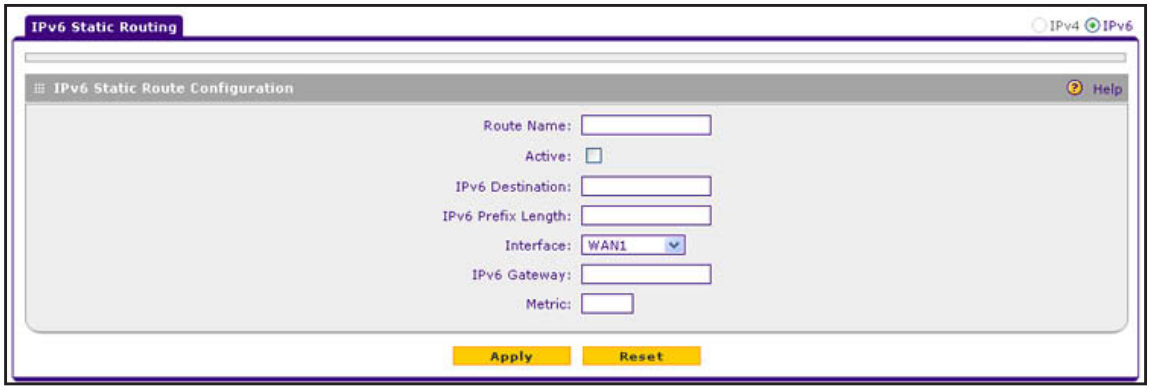

Figure 73.

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

Table 31. Add IPv6 Static Routing screen settings

Setting	Description
Route Name	The route name for the static route (for purposes of identification and management).
Active	To make the static route effective, select the **Active** check box. **Note:** A route can be added to the table and made inactive if not needed. This allows you to use routes as needed without deleting and re-adding the entry.
IPv6 Destination	The destination IPv6 address of the host or network to which the route leads.
IPv6 Prefix Length	The destination IPv6 prefix length of the host or network to which the route leads.
Interface	From the drop-down list, select the physical or virtual network interface (the WAN1, WAN2, WAN3, or WAN4 interface, a sit0 Tunnel, LAN interface, or DMZ interface) through which the route is accessible.
IPv6 Gateway	The gateway IPv6 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.

5. Click **Apply** to save your settings. The new static route is added to the List of IPv6 Static Routes table.

➢ **To edit an IPv6 static route:**

1. On the Static Routing screen for IPv6 (see *Figure 72* on page 132), click the **Edit** button in the Action column for the route that you want to modify. The Edit IPv6 Static Routing screen displays. This screen is identical to the Add IPv6 Static Routing screen.
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more routes:**

1. On the Static Routing screen for IPv6 (see *Figure 72* on page 132), select the check box to the left of each route that you want to delete, or click the **Select All** table button to select all routes.
2. Click the **Delete** table button.

Firewall Protection

4

This chapter describes how to use the firewall features of the VPN firewall to protect your network. The 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. For information about how to set up LAN groups, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 96.

For IPv4, 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 Internet, DMZ, and LAN. Unlike simple NAT routers, a firewall uses a process called stateful packet inspection to protect your network from attacks and intrusions. NAT performs a 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.

For IPv6, which in itself provides stronger security than IPv4, a firewall in particular controls the exchange of traffic between the Internet, DMZ, and LAN.

Administrator Tips

Consider the following operational items:

1. As an option, you can enable remote management if you have to manage distant sites from a central location (see *Configure Authentication Domains, Groups, and Users* on page 303 and *Configure Remote Management Access* on page 338).
2. Although rules are the basic way of managing the traffic through your system (see *Overview of Rules to Block or Allow Specific Kinds of Traffic* on page 136), you can further refine your control using the following features and capabilities of the VPN firewall:
   - Groups and hosts (see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 96)
   - Services (see *Outbound Rules (Service Blocking)* on page 137 and *Inbound Rules (Port Forwarding)* on page 140)
   - Schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 189)
   - Allowing or blocking sites (see *Configure Content Filtering* on page 186)
   - Source MAC filtering (see *Enable Source MAC Filtering* on page 190)
   - Port triggering (see *Configure Port Triggering* on page 197)
3. Some firewall settings might affect the performance of the VPN firewall. For more information, see *Performance Management* on page 329.
4. The firewall logs can be configured to log and then email denial of access, general attack, and other information to a specified email address. For information about how to configure logging and notifications, see *Configure Logging, Alerts, and Event Notifications* on page 362.

Overview of 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 600 firewall rules on the VPN firewall (see the following table). 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 VPN firewall 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 VPN firewall can be applied to LAN WAN traffic, DMZ WAN traffic, and LAN DMZ traffic.

Table 32. Number of supported firewall rule configurations

Traffic Rule	Maximum Number of Outbound Rules	Maximum Number of Inbound Rules	Maximum Number of Combined Supported Rules
LAN WAN	300	300	600
DMZ WAN	50	50	100
LAN DMZ	50	50	100
Total Rules	400	400	800

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

- **Outbound rules (service blocking)**. Outbound traffic is allowed unless you configure the firewall to block specific or all outbound traffic.
- **Inbound rules (port forwarding)**. Inbound traffic is blocked unless the traffic is in response to a request from the LAN side. You can configure the firewall to allow specific or all inbound traffic.
- **Customized services**. You can add additional services to the list of services in the factory defaults list. You can then define rules for these added services to either allow or block that traffic (see *Add Customized Services* on page 177).
- **Quality of Service (QoS) priorities**. Each service has its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change the QoS priority, which changes the traffic mix through the system (see *Create Quality of Service Profiles for IPv4 Firewall Rules* on page 184 and *Quality of Service Priorities for IPv6 Firewall Rules* on page 186).

- **Bandwidth profiles**. After you have a configured a bandwidth profile (see *Create Bandwidth Profiles* on page 181), you can assign it to a rule.

Outbound Rules (Service Blocking)

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

> **Note:** See *Enable Source MAC Filtering* on page 190 for yet another way to block outbound traffic from selected computers that would otherwise be allowed by the firewall.

The following table describes the fields that define the rules for outbound traffic and that are common to most Outbound Service screens (see *Figure 77* on page 148, *Figure 83* on page 154, and *Figure 89* on page 160).

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

- *Configure LAN WAN Rules*
- *Configure DMZ WAN Rules*
- *Configure LAN DMZ Rules*

Table 33. Outbound rules overview

Setting	Description	Outbound Rules
Service	The service or application to be covered by this rule. If the service or application does not display in the list, you need to define it using the Services screen (see *Add Customized Services* on page 177).	All rules
Action	The action for outgoing connections covered by this rule: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any outbound traffic that is not blocked by rules you create is allowed by the default rule. **Note:** ALLOW rules are useful only if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is blocked by another rule.	All rules

Table 33. Outbound rules overview (continued)

Setting	Description	Outbound Rules
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This drop-down list is activated only when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action. • Use the Schedule screen to configure the time schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 189).	All rules when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action
LAN Users	The settings that determine which computers on your network are affected by this rule. The options are: • **Any**. All computers and devices on your LAN. • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices. • **Group**. Select the LAN group to which the rule applies. Use the LAN Groups screen to assign computers to groups (see *Manage the Network Database* on page 97). Groups apply only to IPv4 rules. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 179.	LAN WAN rules LAN DMZ 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 addresses are covered by this rule. • **Single address**. Enter the required address in the Start field. • **Address range**. Enter the required addresses the Start and Finish fields. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 179.	LAN WAN rules DMZ WAN rules
DMZ Users	The settings that determine which DMZ computers on the DMZ network are affected by this rule. The options are: • **Any**. All computers and devices on your DMZ network. • **Single address**. Enter the required address in the Start field to apply the rule to a single computer 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.	DMZ WAN rules LAN DMZ rules

Table 33. Outbound rules overview (continued)

Setting	Description	Outbound Rules
QoS Profile or QoS Priority	The priority assigned to IP packets of this service. The priorities are defined by *Type of Service 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 VPN firewall marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Create Quality of Service Profiles for IPv4 Firewall Rules* on page 184 and *Quality of Service Priorities for IPv6 Firewall Rules* on page 186. **Note:** There are no default QoS profiles on the VPN firewall. After you have created a QoS profile, it can become active only when you apply it to a nonblocking inbound or outbound firewall rule. **Note:** QoS profiles and QoS priorities do not apply to LAN DMZ rules.	QoS Profile: • IPv4 LAN WAN rules • IPv4 DMZ WAN rules Qos Priority: • IPv6 LAN WAN rules • IPv6 DMZ WAN rules
Bandwidth Profile	Bandwidth limiting determines how the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Create Bandwidth Profiles* on page 181. For outbound traffic, you can configure bandwidth limiting only on the WAN interface for a LAN WAN rule. **Note:** Bandwidth limiting does not apply to the DMZ interface.	IPv4 LAN WAN rules
Log	The setting that determines whether packets covered by this rule are logged. The options are: • **Always**. Always log traffic that matches this rule. This is useful when you are debugging your rules. • **Never**. Never log traffic that matches this rule.	All rules
NAT IP	The setting that specifies whether the source address of the outgoing packets on the WAN is autodetected, is assigned the address of the WAN interface, or is a different IP address. You can specify these settings only for outbound traffic of the WAN interface. The options are: • **Auto**. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules. • **WAN Interface Address**. All the outgoing packets on the WAN are assigned to the address of the specified WAN interface. • **Single Address**. All the outgoing packets on the WAN are assigned to the specified IP address, for example, a secondary WAN address that you have configured. **Note:** The NAT IP drop-down list is available only when the WAN mode is NAT. If you select Single Address, the IP address specified should fall under the WAN subnet.	IPv4 LAN WAN rules IPv4 DMZ WAN rules

Inbound Rules (Port Forwarding)

If you have enabled Network Address Translation (NAT), your network presents *one* IP address only to the Internet, and outside users cannot directly access any of your local computers (LAN users). (For information about configuring NAT, see *Network Address Translation* on page 29.) 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.

WARNING:

Allowing inbound services opens security holes in your network. Only enable those ports that are necessary for your network.

Whether or not DHCP is enabled, how the computer 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 Dynamic DNS so that external users can always find your network (see *Configure Dynamic DNS* on page 49).
- If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved (DHCP Client) feature in the LAN Groups screen to keep the computer's IP address constant (see *Set Up DHCP Address Reservation* on page 101).
- Local computers need to access the local server using the computers' local LAN address. Attempts by local computers to access the server using the external WAN IP address will fail.

Note: See *Configure Port Triggering* on page 197 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

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

Note: When the Block TCP Flood and Block UDP Flood check boxes are selected on the Attack Checks screen (which they are by default; see *Attack Checks* on page 170), multiple concurrent connections of the same application from one host or IP address (such as multiple DNS queries from one computer) trigger the VPN firewall's DoS protection.

The following table describes the fields that define the rules for inbound traffic and that are common to most Inbound Service screens (see *Figure 79* on page 150, *Figure 85* on page 156, and *Figure 91* on page 162).

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

- *Configure LAN WAN Rules*
- *Configure DMZ WAN Rules*
- *Configure LAN DMZ Rules*

Table 34. Inbound rules overview

Setting	Description	Inbound Rules
Service	The service or application to be covered by this rule. If the service or application does not display in the list, you need to define it using the Services screen (see *Add Customized Services* on page 177).	All rules
Action	The action for outgoing connections covered by this rule: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any inbound traffic that is not blocked by rules you create is allowed by the default rule.	All rules
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This drop-down list is activated only when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action. • Use the Schedule screen to configure the time schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 189).	All rules when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action

Table 34. Inbound rules overview (continued)

Setting	Description	Inbound Rules
Send to LAN Server	The LAN server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.) The options are: • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices.	IPv4 LAN WAN rules
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.)	IPv4 DMZ WAN rules
Translate to Port Number	If the LAN server or DMZ server that is hosting the service is using a port other than the default port for the service, you can select this setting and specify a port number. If the service is using the default port, you do not need to select this setting.	IPv4 LAN WAN rules IPv4 DMZ WAN rules
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. This can be either the address of the WAN interface or another public IP address. You can also enter an address range. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices.	IPv4 LAN WAN rules IPv4 DMZ WAN rules
LAN Users	These settings apply to a LAN WAN inbound rule when the WAN mode is classical routing, and determine which computers on your network are affected by this rule. The options are: • **Any**. All computers and devices on your LAN. • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices. • **Group**. Select the LAN group to which the rule applies. Use the LAN Groups screen to assign computers to groups (see *Manage the Network Database* on page 97). Groups apply only to IPv4 rules. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 179. **Note:** For IPv4 LAN WAN inbound rules, this field does not apply when the WAN mode is NAT because your network presents only *one* IP address to the Internet.	LAN WAN rules LAN DMZ rules

Table 34. Inbound rules overview (continued)

Setting	Description	Inbound 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 addresses are covered by this rule. • **Single address**. Enter the required address in the Start field. • **Address range**. Enter the required addresses in the Start and Finish fields. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 179.	LAN WAN rules DMZ WAN rules
DMZ Users	The settings that determine which DMZ computers on the DMZ network are affected by this rule. The options are: • **Any**. All computers and devices on your DMZ network. • **Single address**. Enter the required address in the Start field to apply the rule to a single computer 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:** For IPv4 DMZ WAN inbound rules, this field does not apply when the WAN mode is NAT because your network presents only *one* IP address to the Internet.	DMZ WAN rules LAN DMZ rules
QoS Profile	The priority assigned to IP packets of this service. The priorities are defined by *Type of Service 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 VPN firewall marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Create Quality of Service Profiles for IPv4 Firewall Rules* on page 184. **Note:** There are no default QoS profiles on the VPN firewall. After you have created a QoS profile, it can become active only when you apply it to a nonblocking inbound or outbound firewall rule. **Note:** QoS profiles do not apply to LAN DMZ rules.	IPv4 LAN WAN rules IPv4 DMZ WAN rules
Log	The setting that determines whether packets covered by this rule are logged. The options are: • **Always**. Always log traffic that matches this rule. This is useful when you are debugging your rules. • **Never**. Never log traffic that matches this rule.	All rules

Table 34. Inbound rules overview (continued)

Setting	Description	Inbound Rules
Bandwidth Profile	Bandwidth limiting determines how the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Create Bandwidth Profiles* on page 181. For inbound traffic, you can configure bandwidth limiting only on the LAN interface for a LAN WAN rule. **Note:** Bandwidth limiting does not apply to the DMZ interface.	IPv4 LAN WAN rules

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

Order of Precedence for Rules

As you define a new rule, it is added to a table in a Rules screen as the last item in the list, as shown in the following figure, which shows the LAN WAN Rules screen for IPv4 as an example:

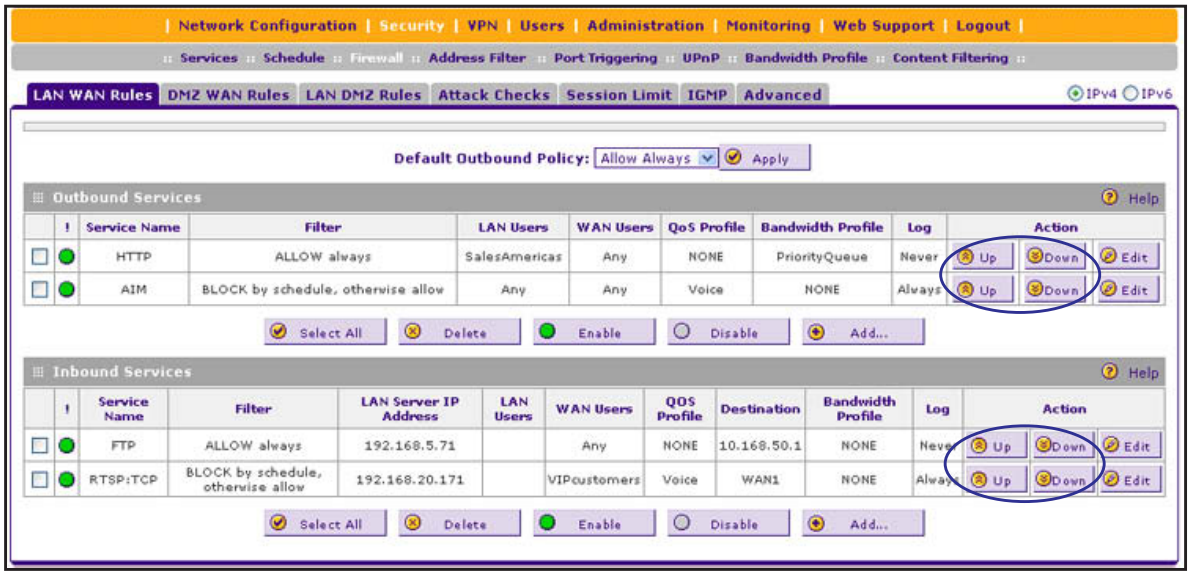

Figure 74.

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

Configure LAN WAN Rules

- *Create LAN WAN Outbound Service Rules*
- *Create LAN WAN Inbound Service 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 VPN firewall.

➢ **To change the default outbound policy for IPv4 traffic or to change existing IPv4 rules:**

1. Select **Security > Firewall**. The Firewall submenu tabs display with the LAN WAN Rules screen in view. In the upper right of the screen, the IPv4 radio button is selected by default. The LAN WAN Rules screen displays the IPv4 settings. (The following figure contains examples.)

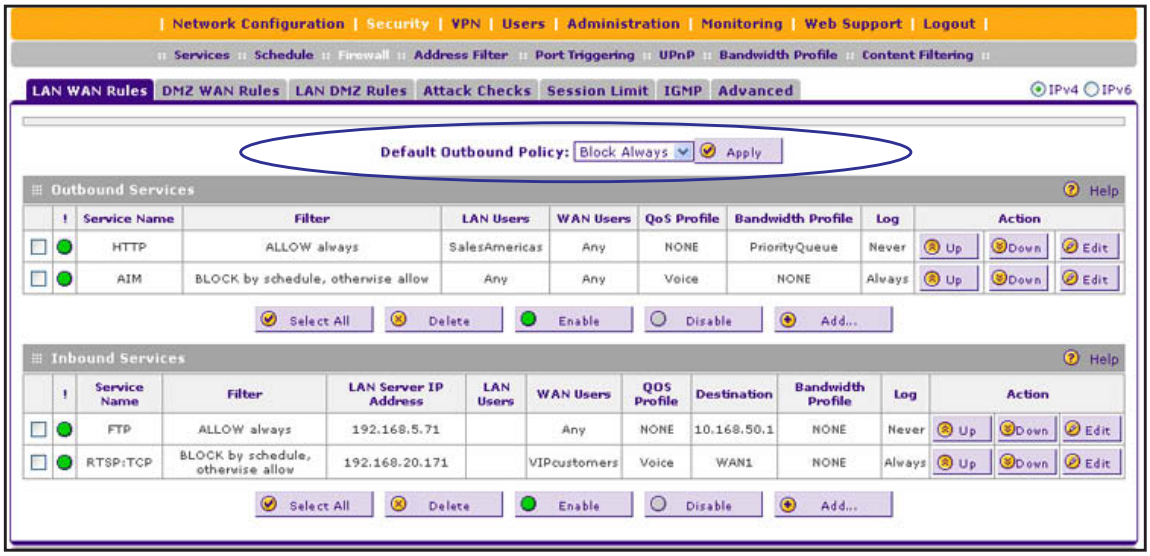

Figure 75.

2. From the Default Outbound Policy drop-down list, select **Block Always**. (By default, Allow Always is selected.)
3. Next to the drop-down list, click the **Apply** table button.

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

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Lets you change the definition of an existing rule. Depending on your selection, one of the following screens displays:
  - Edit LAN WAN Outbound Service screen for IPv4 (identical to *Figure 77* on page 148)
  - Edit LAN WAN Inbound Service screen for IPv4 (identical to *Figure 79* on page 150)

➢ **To change the default outbound policy for IPv6 traffic or to change existing IPv6 rules:**

1. Select **Security > Firewall**. The Firewall submenu tabs display with the LAN WAN Rules screen for IPv4 in view.
2. In the upper right of the screen, select the **IPv6** radio button. The LAN WAN Rules screen displays the IPv6 settings. (The following figure contains examples.)

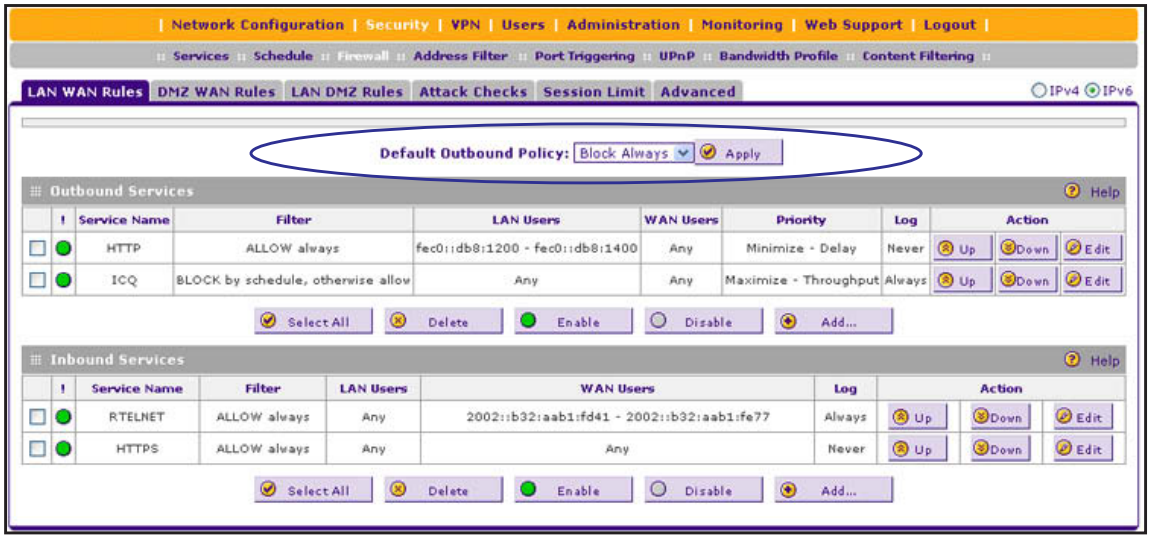

Figure 76.

3. From the Default Outbound Policy drop-down list, select **Block Always**. (By default, Allow Always is selected.)
4. Next to the drop-down list, click the **Apply** table button.

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

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Lets you change the definition of an existing rule. Depending on your selection, one of the following screens displays:
  - Edit LAN WAN Outbound Service screen for IPv6 (identical to *Figure 78* on page 149)
  - Edit LAN WAN Inbound Service screen for IPv6 (identical to *Figure 80* on page 151)

➢ **To enable, disable, or delete one or more IPv4 or IPv6 rules:**

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

Create LAN WAN Outbound Service Rules

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

WARNING:

Make sure that you understand the consequences of a LAN WAN outbound rule before you apply the rule. Incorrect configuration might cause serious connection problems.

You can also tailor these rules to your specific needs (see *Administrator Tips* on page 135).

IPv4 LAN WAN Outbound Rules

➢ **To create an IPv4 LAN WAN outbound rule:**

1. In the upper right of the LAN WAN Rules screen, the IPv4 radio button is selected by default. The screen displays the IPv4 settings (see *Figure 75* on page 145).

   Click the **Add** table button under the Outbound Services table. The Add LAN WAN Outbound Service screen for IPv4 displays:

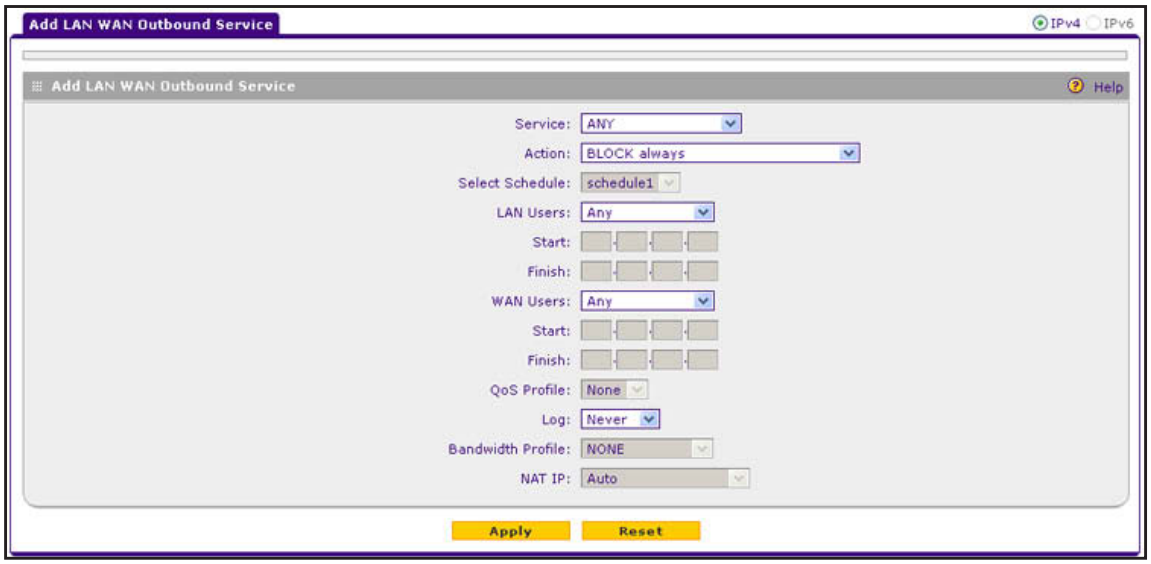

Figure 77.

2. Enter the settings as described in *Table 33* on page 137. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - LAN Users
   - WAN Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make selections from the following drop-down lists:
   - Select Schedule
   - QoS Profile
   - Bandwidth Profile
   - NAT IP (This drop-down list is available only when the WAN mode is NAT.)
3. Click **Apply** to save your changes. The new rule is now added to the Outbound Services table.

IPv6 LAN WAN Outbound Rules

➢ **To create an IPv6 LAN WAN outbound rule:**

1. In the upper right of the LAN WAN Rules screen, select the **IPv6** radio button. The screen displays the IPv6 settings (see *Figure 76* on page 146).
2. Click the **Add** table button under the Outbound Services table. The Add LAN WAN Outbound Service screen for IPv6 displays:

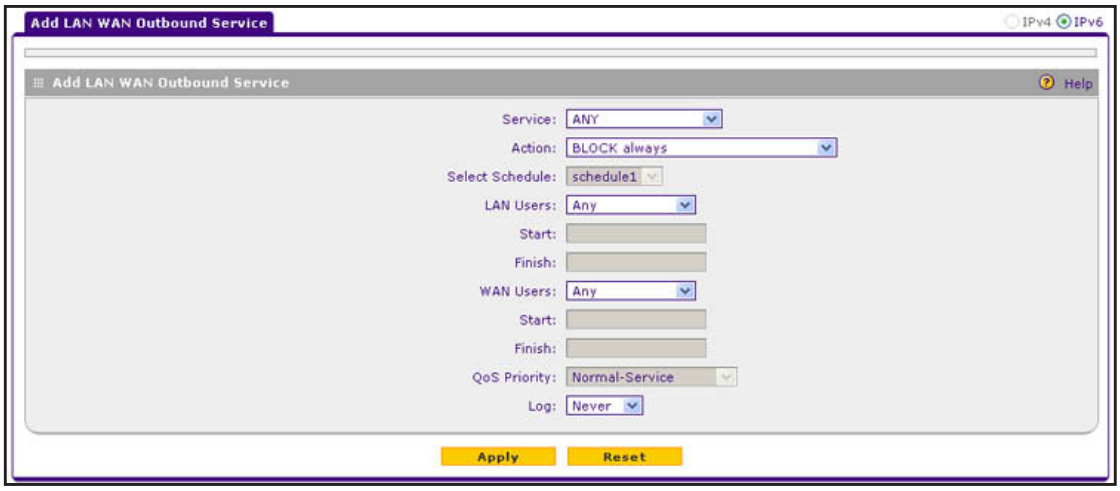

Figure 78.

3. Enter the settings as described in *Table 33* on page 137. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - LAN Users
   - WAN Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make a selection from the following drop-down lists:
   - Select Schedule
   - QoS Priority
4. Click **Apply** to save your changes. The new rule is now added to the Outbound Services table.

Create LAN WAN Inbound Service Rules

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

WARNING:

Make sure that you understand the consequences of a LAN WAN inbound rule before you apply the rule. Incorrect configuration might cause serious connection problems. If you are configuring the VPN firewall from a remote connection, you might be locked out.

IPv4 LAN WAN Inbound Service Rules

➢ **To create an IPv4 LAN WAN inbound rule:**

1. In the upper right of the LAN WAN Rules screen, the IPv4 radio button is selected by default. The screen displays the IPv4 settings (see *Figure 75* on page 145).

   Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen for IPv4 displays:

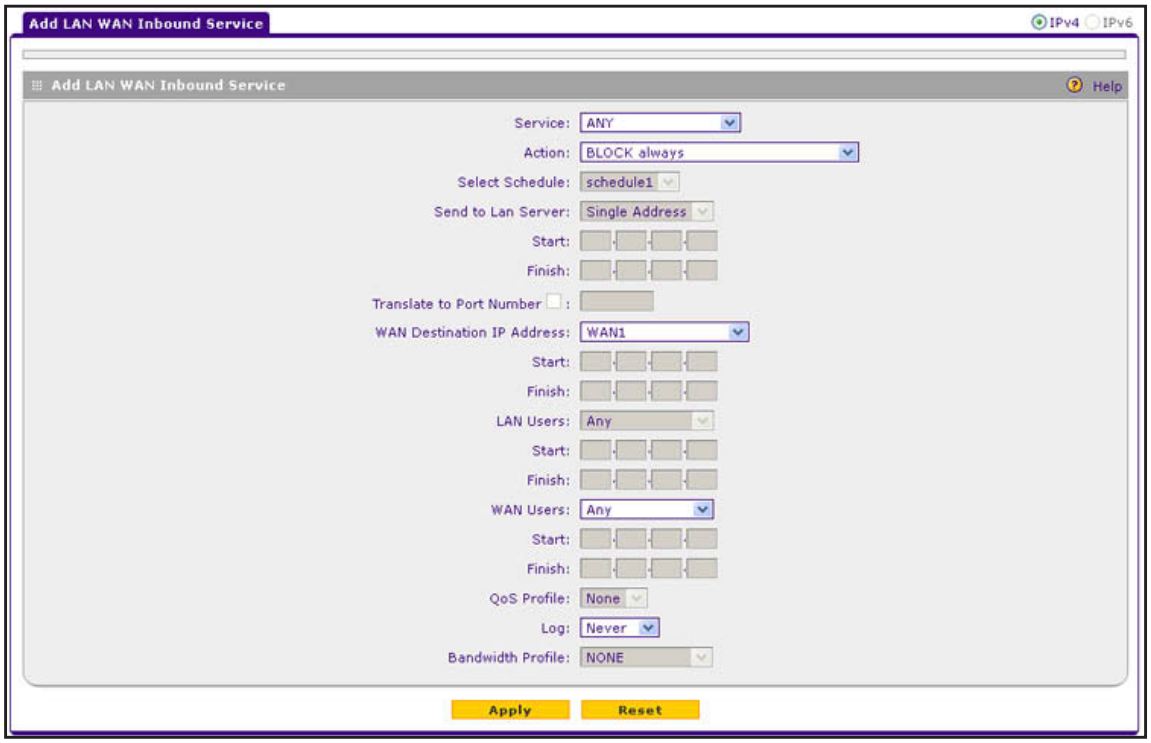

Figure 79.

2. Enter the settings as described in *Table 34* on page 141. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - WAN Destination IP Address
   - LAN Users (This drop-down list is available only when the WAN mode is Classical Routing. When the WAN mode is NAT, your network presents only one IP address to the Internet.)
   - WAN Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make selections from the following drop-down lists:

   - Select Schedule
   - Send to Lan Server

The following configurations are optional:

- Translate to Port Number
- QoS Profile
- Bandwidth Profile

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

IPv6 LAN WAN Inbound Rules

➢ **To create an IPv6 LAN WAN inbound rule:**

1. In the upper right of the LAN WAN Rules screen, select the **IPv6** radio button. The screen displays the IPv6 settings (see *Figure 76* on page 146).
2. Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen for IPv6 displays:

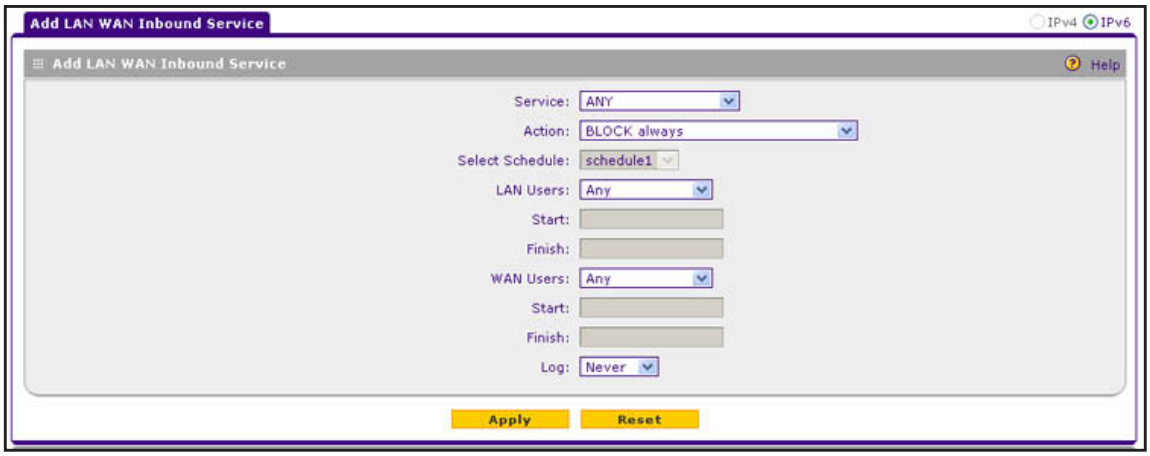

Figure 80.

3. Enter the settings as described in *Table 34* on page 141. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - LAN Users
   - WAN Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make a selection from the following drop-down list:

   - Select Schedule
4. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Configure DMZ WAN Rules

- *Create DMZ WAN Outbound Service Rules*
- *Create LAN WAN Inbound Service Rules*

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

There is no drop-down list that lets you set the default outbound policy as there is on the LAN WAN Rules screen. You can change the default outbound policy by enabling all outbound traffic and then blocking only specific services from passing through the VPN firewall. You do so by adding outbound services rules (see *Create DMZ WAN Outbound Service Rules* on page 154).

Note: Inbound rules on the LAN WAN Rules screen take precedence over inbound rules on the DMZ WAN Rules screen. When an inbound packet matches an inbound rule on the LAN WAN Rules screen, the packet is not matched against the inbound rules on the DMZ WAN Rules screen.

➢ **To access the DMZ WAN Rules screen for IPv4 or to change existing IPv4 rules:**

Select **Security > Firewall > DMZ WAN Rules**. In the upper right of the screen, the IPv4 radio button is selected by default. The DMZ WAN Rules screen displays the IPv4 settings. (The following figure contains examples.)

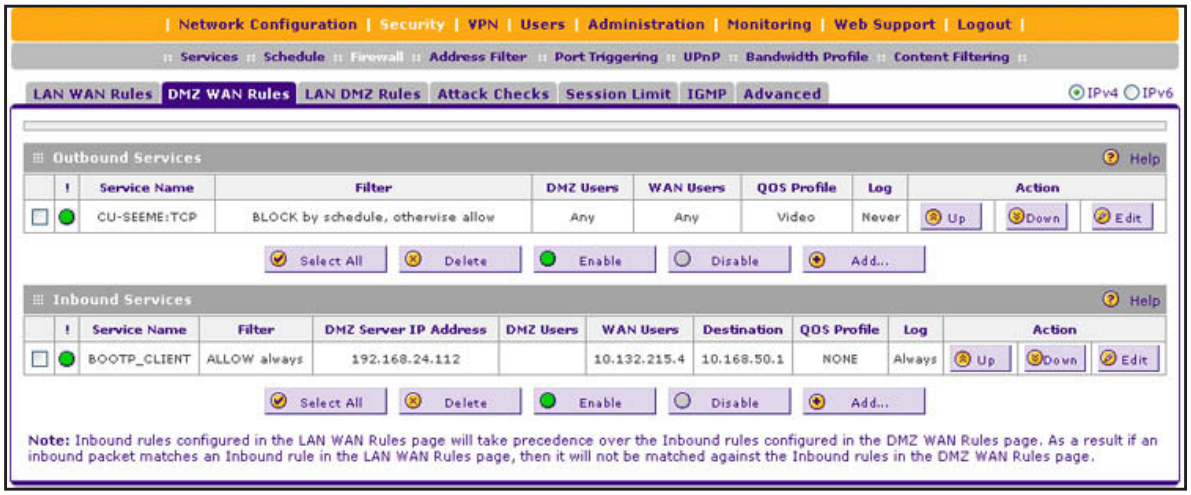

Figure 81.

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

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Lets you change the definition of an existing rule. Depending on your selection, one of the following screens displays:
  - Edit DMZ WAN Outbound Service screen for IPv4 (identical to *Figure 83* on page 154)
  - Edit DMZ WAN Inbound Service screen for IPv4 (identical to *Figure 85* on page 156)

➢ **To access the DMZ WAN Rules screen for IPv6 or to change existing IPv6 rules:**

1. Select **Security > Firewall > DMZ WAN Rules**. The Firewall submenu tabs display with the DMZ WAN Rules screen for IPv4 in view.
2. In the upper right of the screen, select the **IPv6** radio button. The DMZ WAN Rules screen displays the IPv6 settings. (The following figure contains examples.)

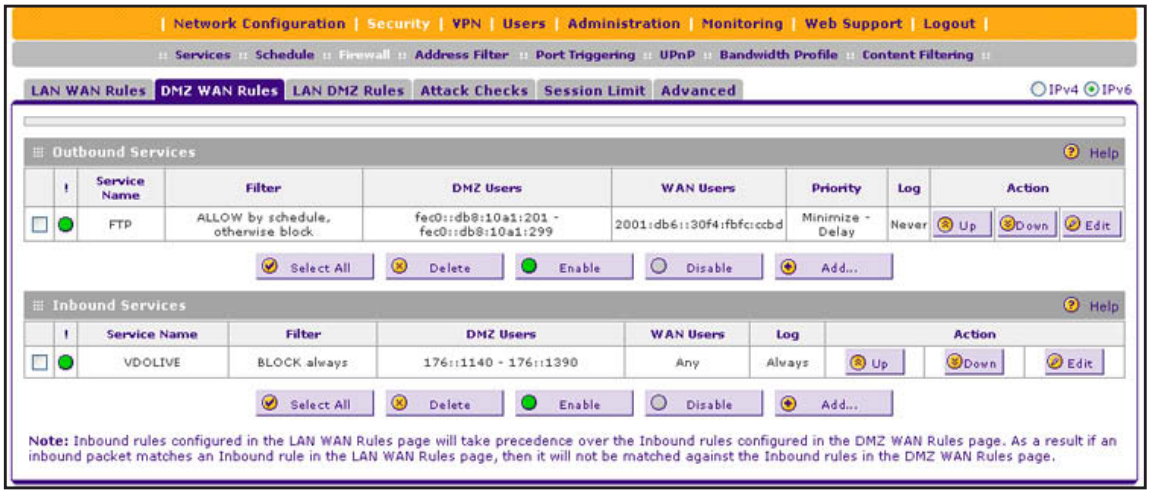

Figure 82.

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

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Lets you change the definition of an existing rule. Depending on your selection, one of the following screens displays:
  - Edit DMZ WAN Outbound Service screen for IPv6 (identical to *Figure 84* on page 155)
  - Edit DMZ WAN Inbound Service screen for IPv6 (identical to *Figure 86* on page 157)

➢ **To enable, disable, or delete one or more IPv4 or IPv6 rules:**

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

Create DMZ WAN Outbound Service Rules

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

IPv4 DMZ WAN Outbound Service Rules

➢ **To create an IPv4 DMZ WAN outbound rule:**

1. In the upper right of the DMZ WAN Rules screen, the IPv4 radio button is selected by default. The screen displays the IPv4 settings (see *Figure 81* on page 152).

   Click the **Add** table button under the Outbound Services table. The Add DMZ WAN Outbound Service screen for IPv4 displays:

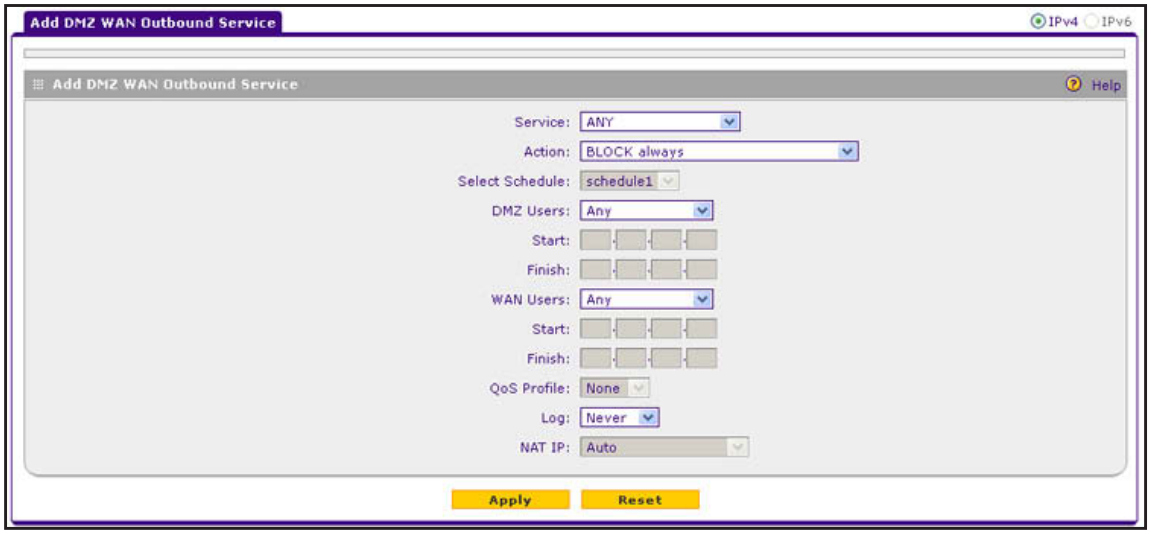

Figure 83.

2. Enter the settings as described in *Table 33* on page 137. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - DMZ Users
   - WAN Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make selections from the following drop-down lists:
   - Select Schedule
   - NAT IP (This drop-down list is available only when the WAN mode is NAT.)

   The following configuration is optional:
   - QoS Profile
3. Click **Apply**. The new rule is now added to the Outbound Services table. The rule is automatically enabled.

IPv6 DMZ WAN Outbound Service Rules

➢ **To create an IPv6 DMZ WAN outbound rule:**

1. In the upper right of the DMZ WAN Rules screen, select the **IPv6** radio button. The screen displays the IPv6 settings (see *Figure 82* on page 153).
2. Click the **Add** table button under the Outbound Services table. The Add DMZ WAN Outbound Service screen for IPv6 displays:

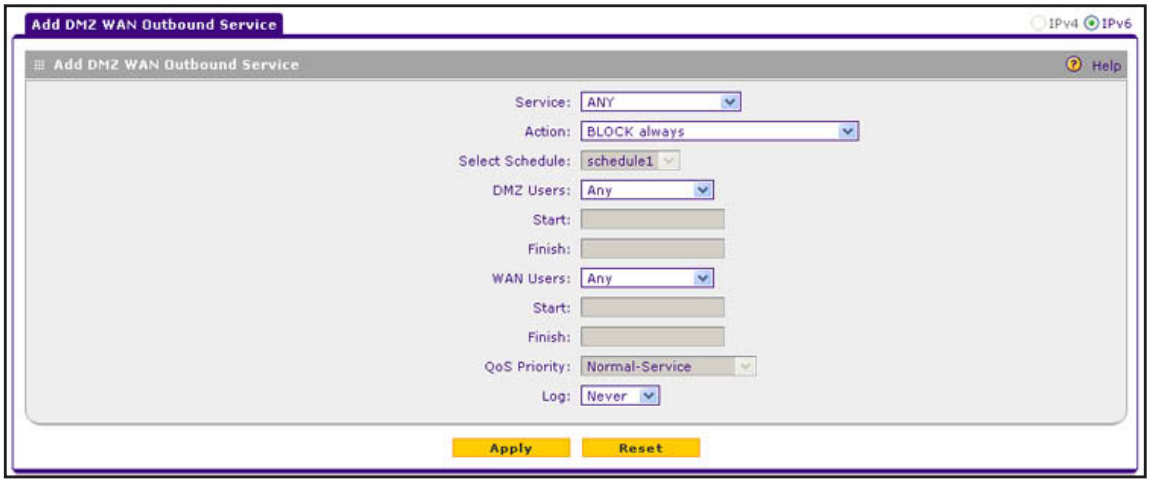

Figure 84.

3. Enter the settings as described in *Table 33* on page 137. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - DMZ Users
   - WAN Users

Unless your selection from the Action drop-down list is BLOCK always, you also need to make selections from the following drop-down lists:

- Select Schedule
- QoS Priority

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

Create DMZ WAN Inbound Service Rules

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

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

IPv4 DMZ WAN Inbound Service Rules

➢ **To create an IPv4 DMZ WAN inbound rule:**

1. In the upper right of the DMZ WAN Rules screen, the IPv4 radio button is selected by default. The screen displays the IPv4 settings (see *Figure 81* on page 152).

   Click the **Add** table button under the Inbound Services table. The Add DMZ WAN Inbound Service screen for IPv4 displays:

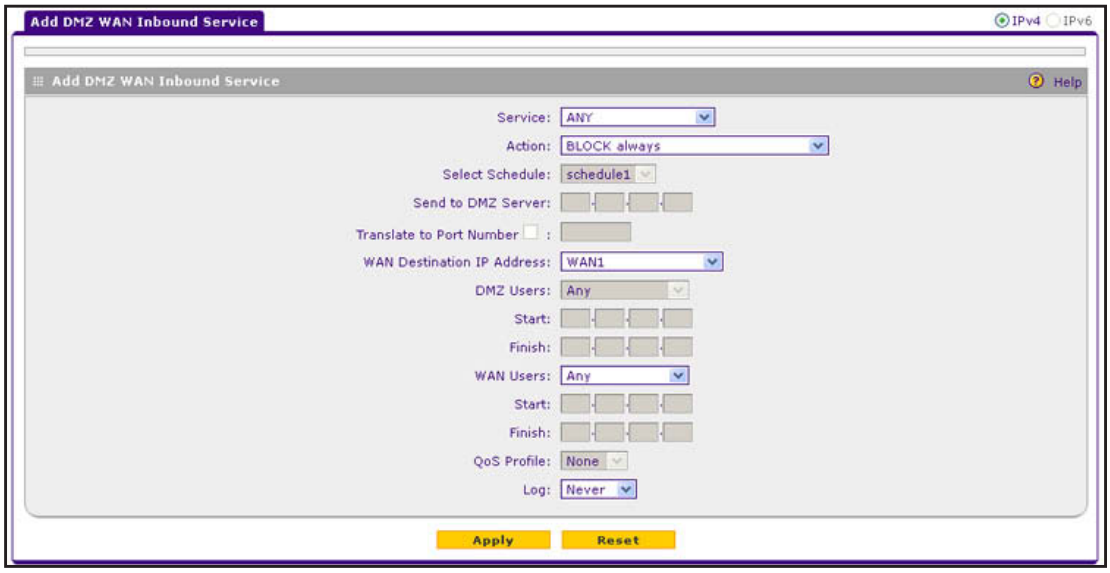

Figure 85.

2. Enter the settings as described in *Table 34* on page 141. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - WAN Destination IP Address
   - DMZ Users (This drop-down list is available only when the WAN mode is Classical Routing. When the WAN mode is NAT, your network presents only one IP address to the Internet.)
   - WAN Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make selections from the following drop-down lists:
   - Select Schedule
   - Send to DMZ Server

   The following configurations are optional:
   - Translate to Port Number
   - QoS Profile
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

IPv6 DMZ WAN Inbound Service Rules

➢ **To create an IPv6 DMZ WAN inbound rule:**

1. In the upper right of the DMZ WAN Rules screen, select the **IPv6** radio button. The screen displays the IPv6 settings (see *Figure 82* on page 153).
2. Click the **Add** table button under the Inbound Services table. The Add DMZ WAN Inbound Service screen for IPv6 displays:

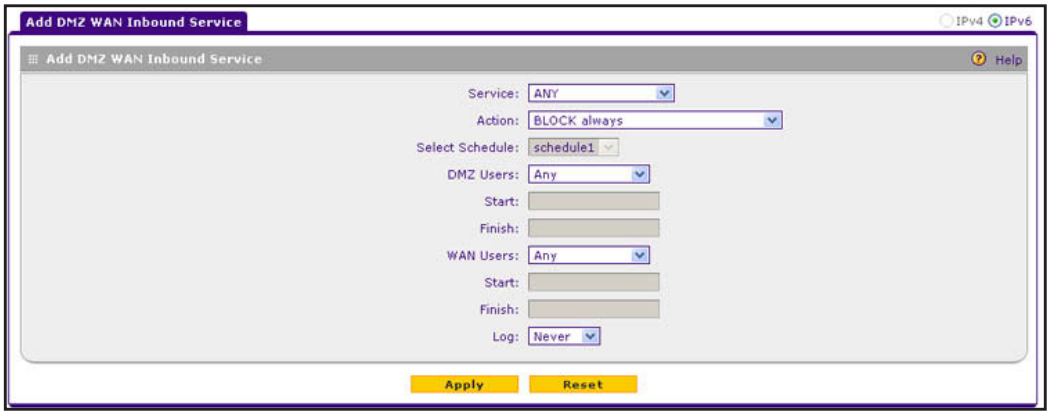

Figure 86.

3. Enter the settings as described in *Table 34* on page 141. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - DMZ Users
   - WAN Users

Unless your selection from the Action drop-down list is BLOCK always, you also need to make selections from the following drop-down list:

- Select Schedule

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

Configure LAN DMZ Rules

- *Create LAN DMZ Outbound Service Rules*
- *Create LAN DMZ Inbound Service Rules*

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

There is no drop-down list that lets you set the default outbound policy as there is on the LAN WAN Rules screen. You can change the default outbound policy by allowing all outbound traffic and then blocking specific services from passing through the VPN firewall. You do so by adding outbound service rules (see *Create LAN DMZ Outbound Service Rules* on page 160).

➢ **To access the LAN DMZ Rules screen for IPv4 or to change existing IPv4 rules:**

Select **Security > Firewall > LAN DMZ Rules**. In the upper right of the screen, the IPv4 radio button is selected by default. The LAN DMZ Rules screen displays the IPv4 settings. (The following figure contains examples.)

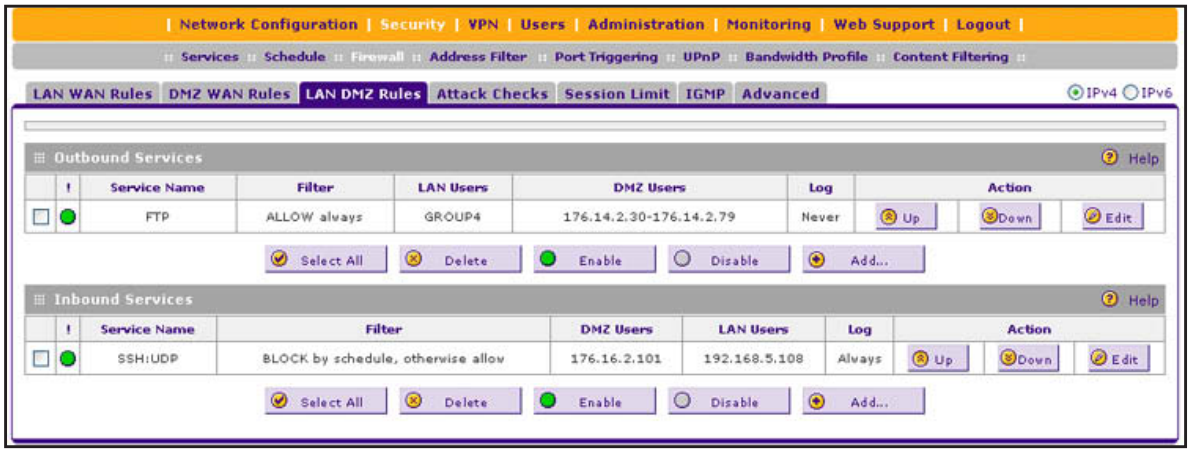

Figure 87.

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

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Lets you change the definition of an existing rule. Depending on your selection, one of the following screens displays:
  - Edit LAN DMZ Outbound Service screen for IPv4 (identical to *Figure 89* on page 160)
  - Edit LAN DMZ Inbound Service screen for IPv4 (identical to *Figure 91* on page 162)

➢ **To access the LAN DMZ Rules screen for IPv6 or to change existing IPv6 rules:**

1. Select **Security > Firewall > LAN DMZ Rules**. The Firewall submenu tabs display with the LAN DMZ Rules screen for IPv4 in view.
2. In the upper right of the screen, select the **IPv6** radio button. The LAN DMZ Rules screen displays the IPv6 settings. (The following figure contains examples.)

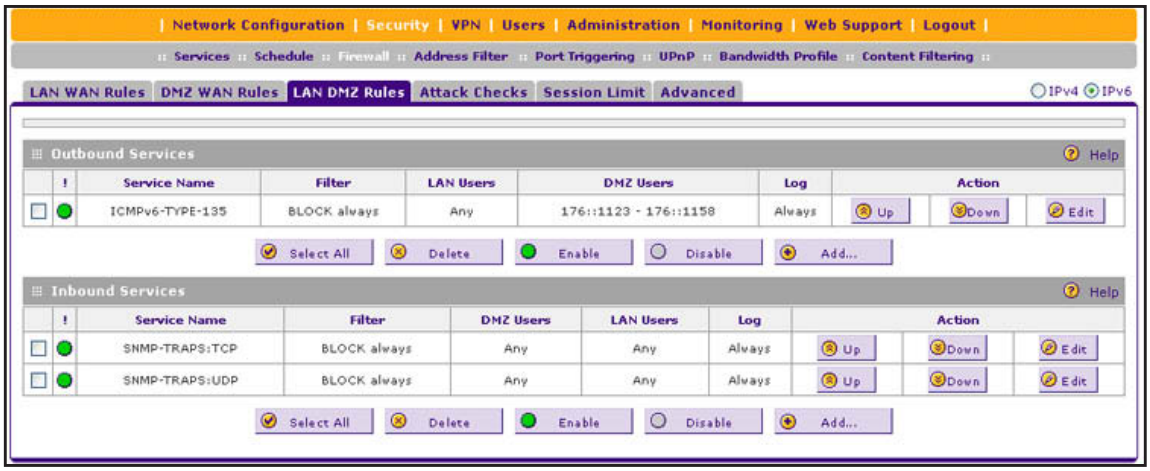

Figure 88.

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

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Lets you change the definition of an existing rule. Depending on your selection, one of the following screens displays:
  - Edit LAN DMZ Outbound Service screen for IPv6 (identical to *Figure 90* on page 161)
  - Edit LAN DMZ Inbound Service screen for IPv6 (identical to *Figure 92* on page 163)

➢ **To enable, disable, or delete one or more IPv4 or IPv6 rules:**

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

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

Create LAN DMZ Outbound Service Rules

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

IPv4 LAN DMZ Outbound Service Rules

➢ **To create an IPv4 LAN DMZ outbound rule:**

1. In the upper right of the LAN DMZ Rules screen, the IPv4 radio button is selected by default. The screen displays the IPv4 settings (see *Figure 87* on page 158).

   Click the **Add** table button under the Outbound Services table. The Add LAN DMZ Outbound Service screen for IPv4 displays:

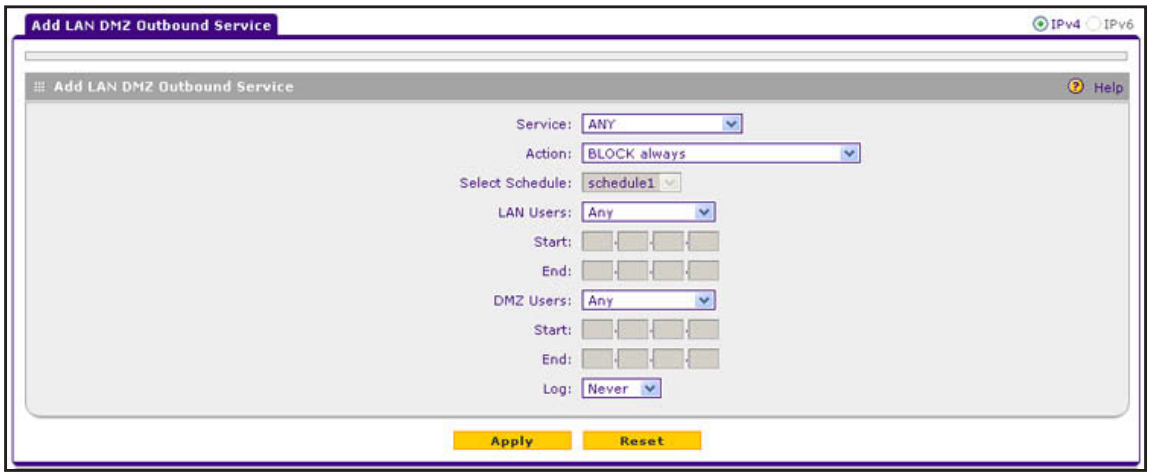

Figure 89.

2. Enter the settings as described in *Table 33* on page 137. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - LAN Users
   - DMZ Users

Unless your selection from the Action drop-down list is BLOCK always, you also need to make a selection from the following drop-down list:

- Select Schedule

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

IPv6 LAN DMZ Outbound Service Rules

➢ **To create an IPv6 LAN DMZ outbound rule:**

1. In the upper right of the LAN DMZ Rules screen, select the **IPv6** radio button. The screen displays the IPv6 settings (see *Figure 88* on page 159).
2. Click the **Add** table button under the Outbound Services table. The Add LAN DMZ Outbound Service screen for IPv6 displays:

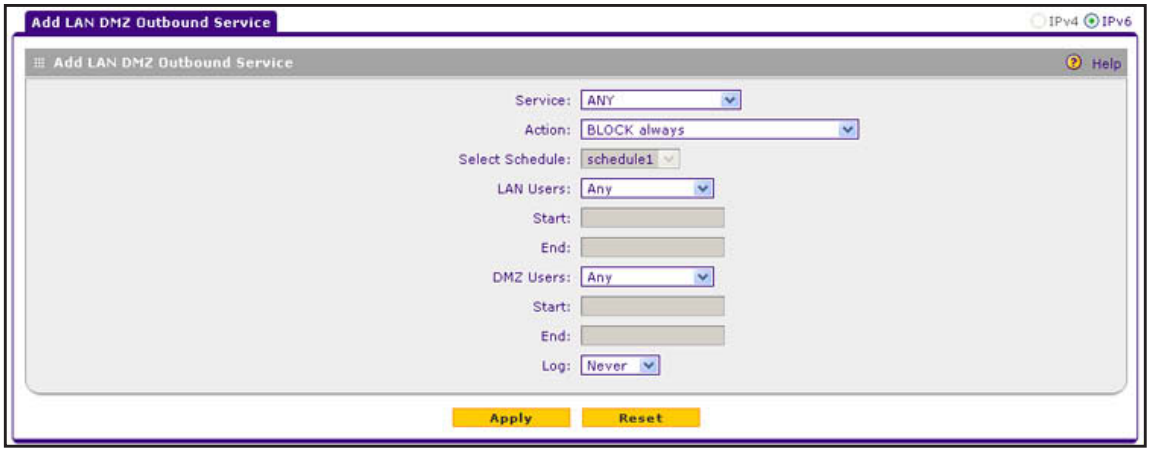

Figure 90.

3. Enter the settings as described in *Table 33* on page 137. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - LAN Users
   - DMZ Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make a selection from the following drop-down list:
   - Select Schedule
4. Click **Apply**. The new rule is now added to the Outbound Services table. The rule is automatically enabled.

Create LAN DMZ Inbound Service Rules

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

IPv4 LAN DMZ Inbound Service Rules

➢ **To create an IPv4 LAN DMZ inbound rule:**

1. In the upper right of the LAN DMZ Rules screen, the IPv4 radio button is selected by default. The screen displays the IPv4 settings (see *Figure 87* on page 158).

   Click the **Add** table button under the Inbound Services table. The Add LAN DMZ Inbound Service screen for IPv4 displays:

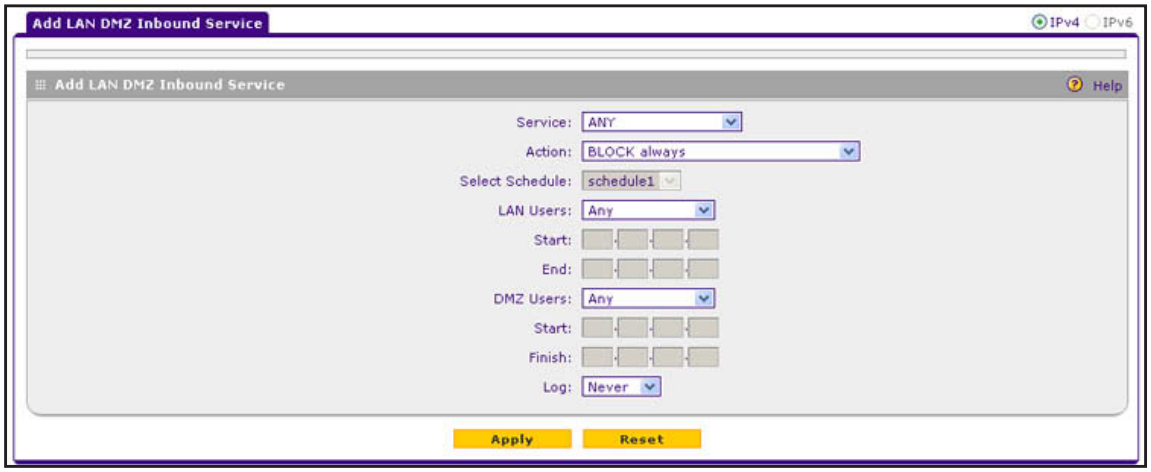

Figure 91.

2. Enter the settings as described in *Table 34* on page 141. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - LAN Users
   - DMZ Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make a selection from the following drop-down list:
   - Select Schedule
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

IPv6 LAN DMZ Inbound Service Rules

➢ **To create an IPv6 LAN DMZ inbound rule:**

1. In the upper right of the LAN DMZ Rules screen, select the **IPv6** radio button. The screen displays the IPv6 settings (see *Figure 88* on page 159).
2. Click the **Add** table button under the Inbound Services table. The Add LAN DMZ Inbound Service screen for IPv6 displays:

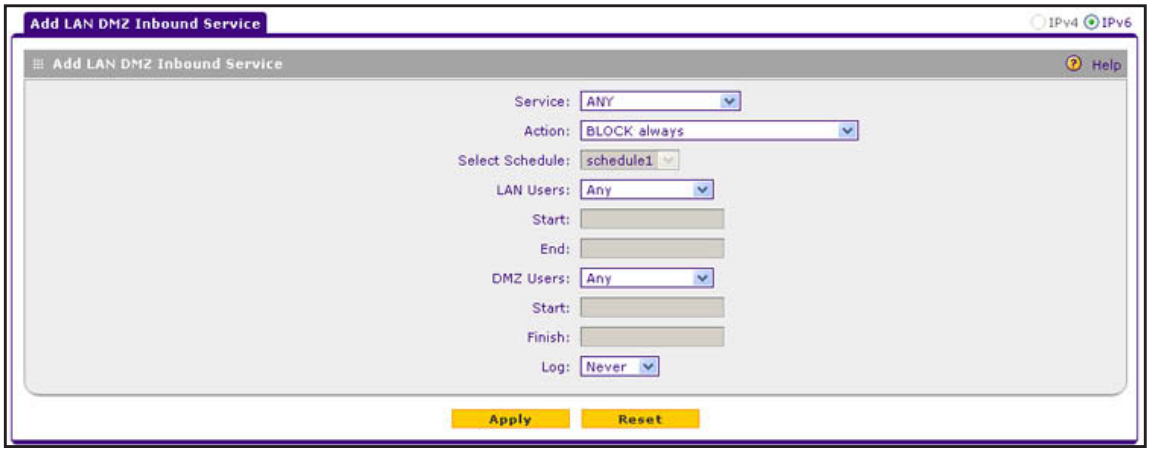

Figure 92.

3. Enter the settings as described in *Table 34* on page 141. In addition to selections from the Service, Action, and Log drop-down lists, you need to make selections from the following drop-down lists:
   - LAN Users
   - DMZ Users

   Unless your selection from the Action drop-down list is BLOCK always, you also need to make a selection from the following drop-down list:
   - Select Schedule
4. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Examples of Firewall Rules

Examples of Inbound Firewall Rules

IPv4 LAN WAN Inbound Rule: Host a Local Public Web Server

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

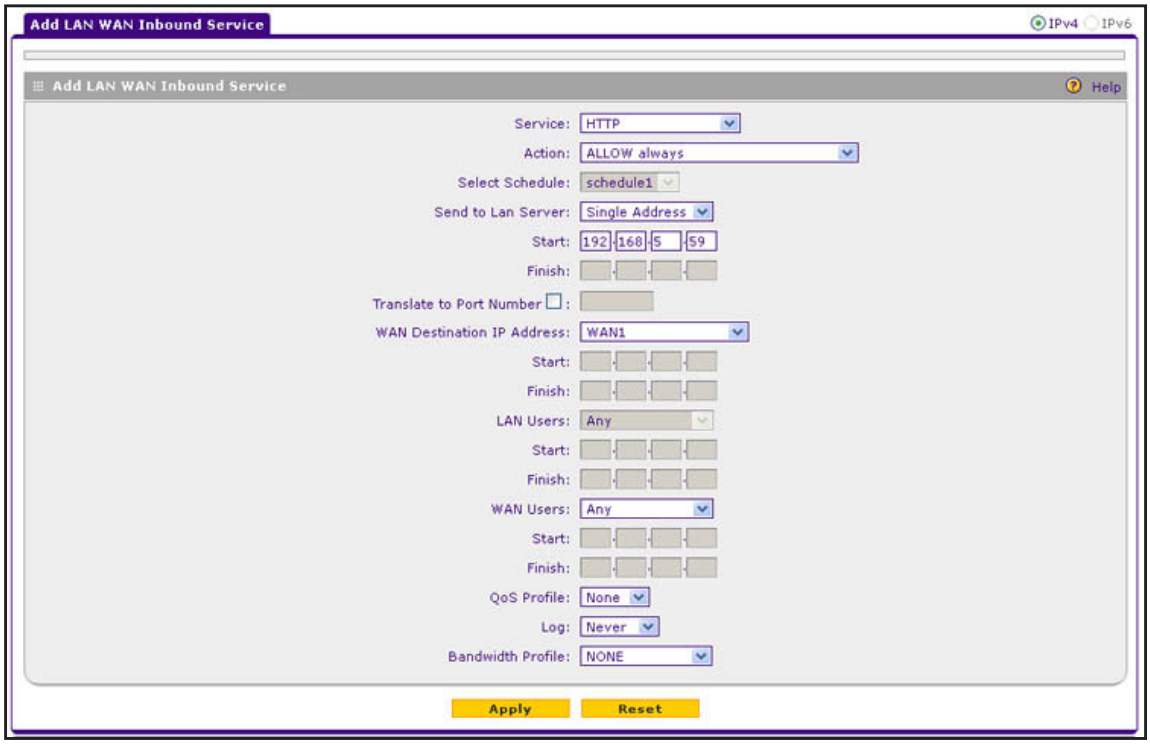

Figure 93.

IPv4 LAN WAN Inbound Rule: Allow a Videoconference from Restricted Addresses

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

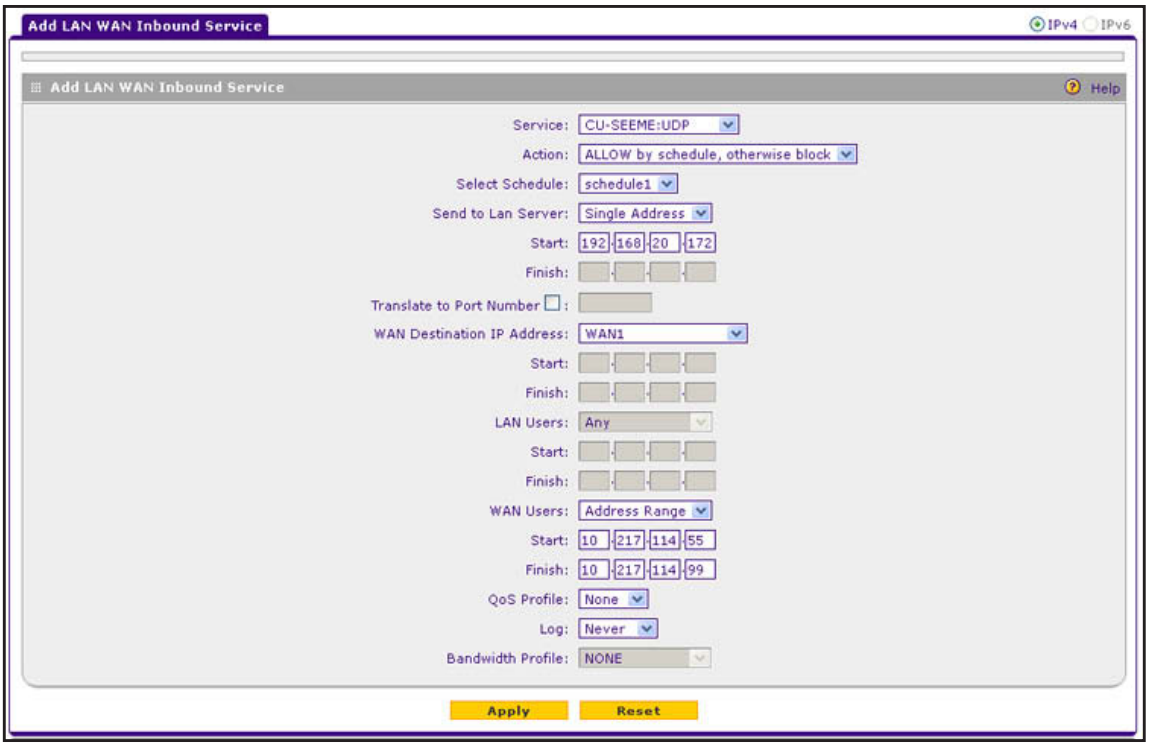

Figure 94.

IPv4 LAN WAN or IPv4 DMZ WAN Inbound Rule: Set Up One-to-One NAT Mapping

In this example, multi-NAT is configured to support multiple public IP addresses on one WAN interface. An inbound rule configures the VPN firewall 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 VPN firewall:
  - WAN IP address. 10.1.0.118
  - LAN IP address subnet. 192.168.1.1 with subnet 255.255.255.0
  - DMZ IP address subnet. 176.16.10.1 with subnet 255.255.255.0
- Web server computer on the VPN firewall’s LAN:
  - LAN IP address. 192.168.1.2
  - DMZ IP address. 176.16.10.2
  - Access to the web server is through the public IP address. 10.168.50.1

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 computers through NAT. The other addresses are available to map to your servers.

➢ **To configure the VPN firewall for additional IP addresses:**

1. Select **Security > Firewall**. The Firewall submenu tabs display.
2. If your server is to be on your LAN, click the **LAN WAN Rules** submenu tab. (If your server is to be on your DMZ, click the **DMZ WAN Rules** submenu tab.)
3. In the upper right of the LAN WAN Rules screen, the IPv4 radio button is selected by default. The screen displays the IPv4 setting.

   Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays:

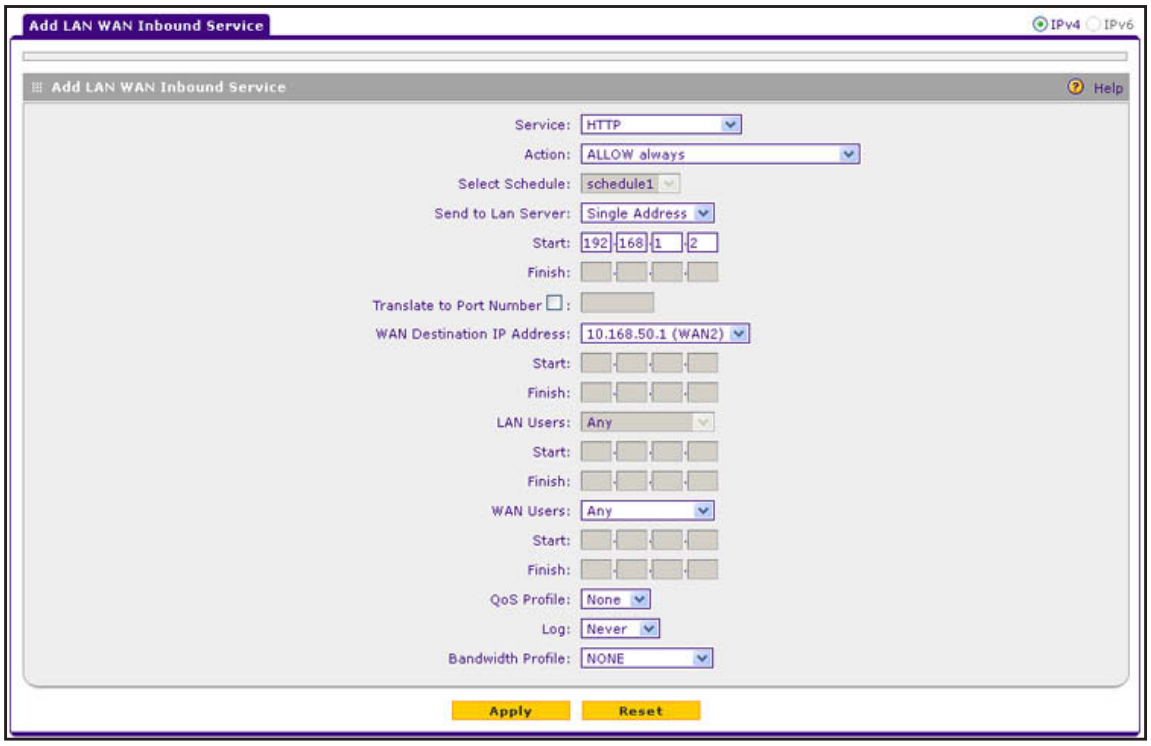

Figure 95.

4. From the Service drop-down list, select **HTTP** for a web server.
5. From the Action drop-down list, select **ALLOW Always**.
6. In the Send to LAN Server field, enter the local IP address of your web server (192.168.1.2 in this example).
7. From the WAN Destination IP Address drop-down list, select the web server. In this example, the secondary 192.168.50.1 (WAN2) address is shown. You first need to define

this address on the WAN2 Secondary Addresses screen (see *Configure Secondary WAN Addresses* on page 47) before you can select it from the WAN Destination IP Address drop-down list.

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

To test the connection from a computer on the Internet, type **http://<IP_address>**, in which <IP_address> is the public IP address that you have mapped to your web server in *Step 6*. You should see the home page of your web server.

IPv4 LAN WAN or IPv4 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.

WARNING:

Do not set up an exposed host from a remote connection because you will likely lock yourself out from the VPN firewall.

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

1. Create an inbound rule that allows all protocols.
2. Place the rule below all other inbound rules.

See an example in the following figure.

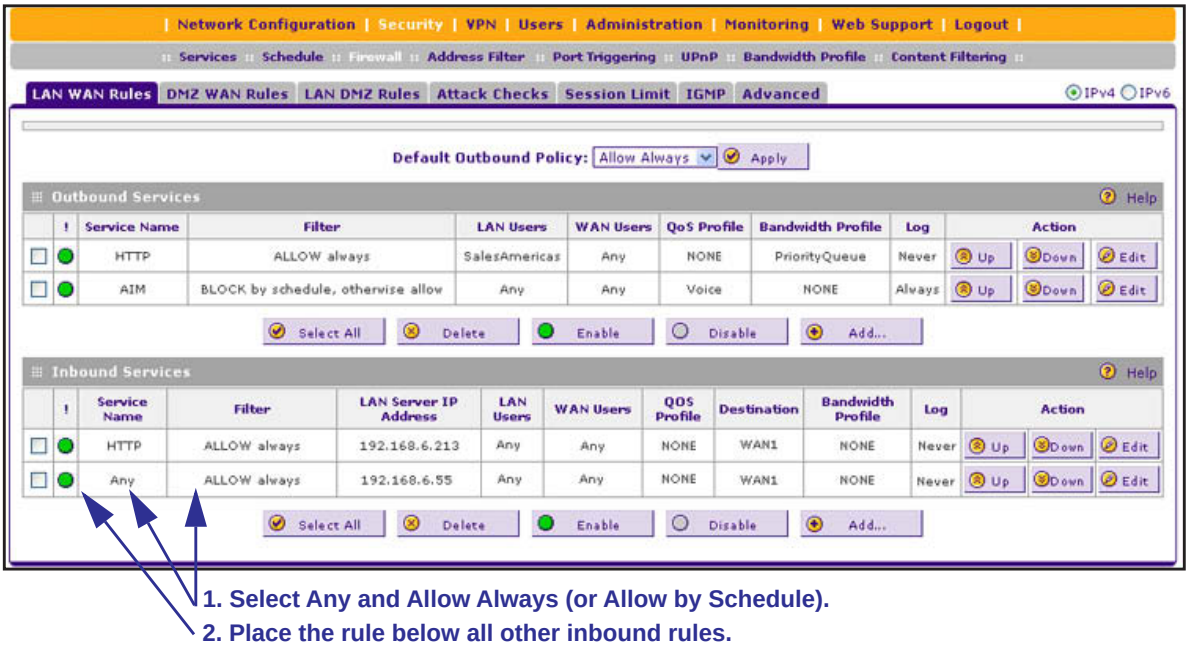

Figure 96.

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.

IPv6 LAN WAN Inbound Rule: Restrict RTelnet from a Single WAN User to a Single LAN User

If you want to restrict incoming RTelnet sessions from a single IPv6 WAN user to a single IPv6 LAN user, specify the initiating IPv6 WAN address and the receiving IPv6 LAN address. See an example in the following figure.

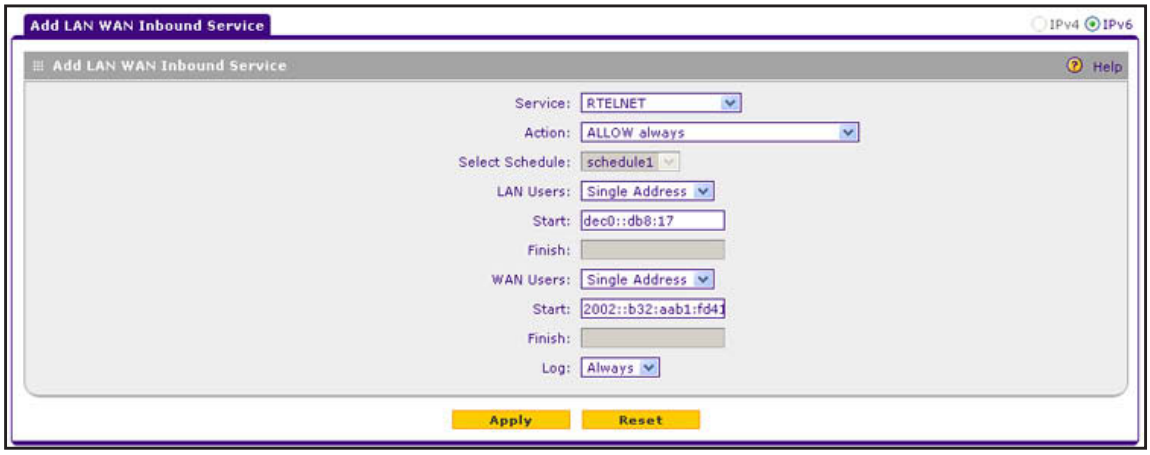

Figure 97.

Examples of Outbound Firewall Rules

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

IPv4 LAN WAN Outbound Rule: Block Instant Messenger

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

You can also enable the VPN firewall to log any attempt to use Instant Messenger during the blocked period. See an example in the following figure.

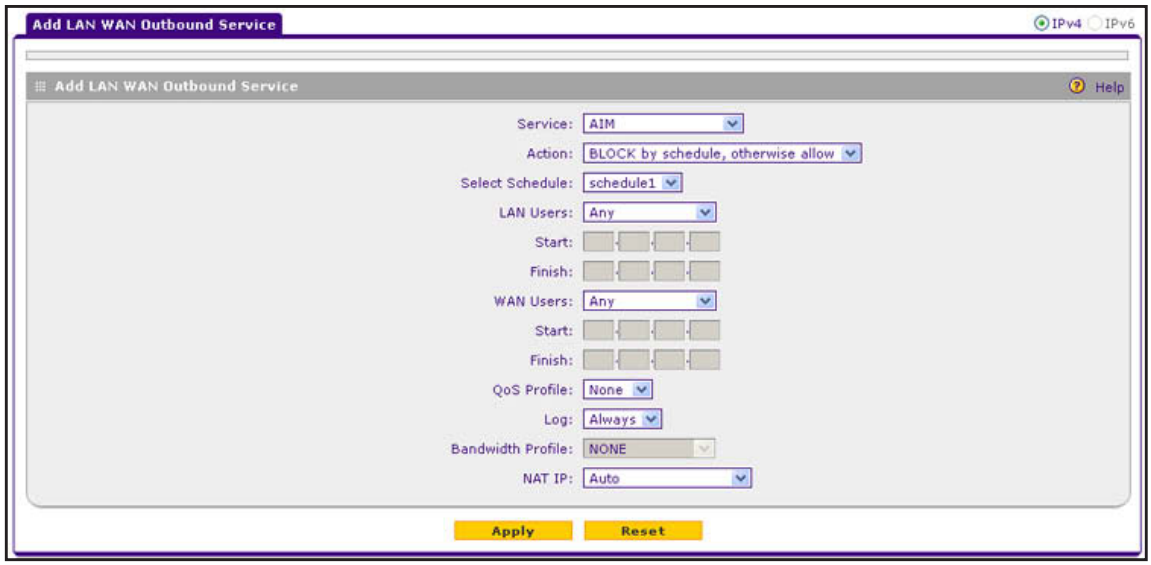

Figure 98.

IPv6 DMZ WAN Outbound Rule: Allow a Group of DMZ User to Access an FTP Site on the Internet

If you want to allow a group of DMZ users to access a particular FTP site on the Internet during working hours, you can create an outbound rule to allow such traffic by specifying the IPv6 DMZ start and finish addresses and the IPv6 WAN address. On the Schedule screen, create a schedule that specifies working hours, and assign it to the rule.

You can also configure the QoS profile to maximize the throughput. See an example in the following figure.

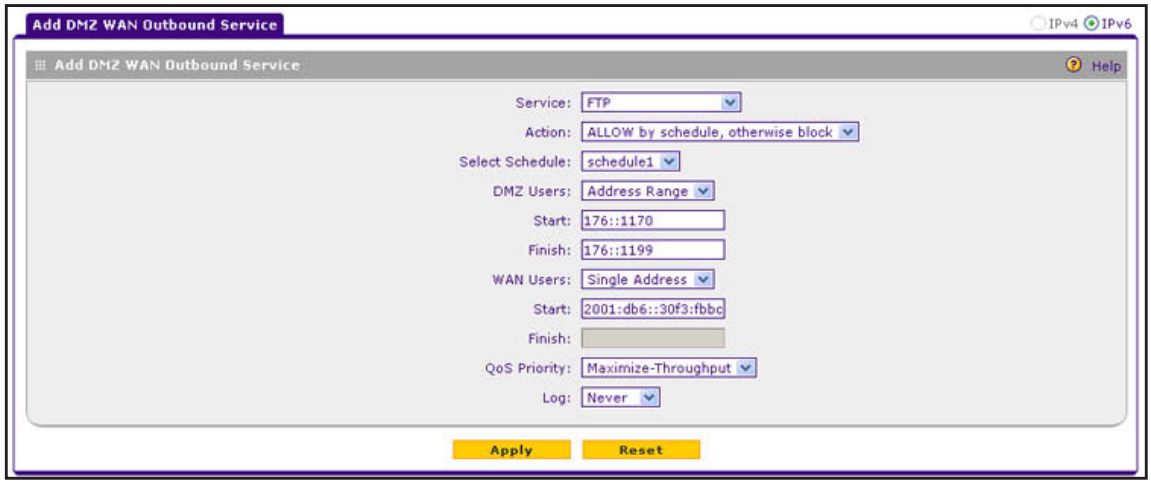

Figure 99.

Configure Other Firewall Features

You can configure attack checks, set session limits, configure multicast pass-through, and manage the application level gateway (ALG) for SIP sessions.

Attack Checks

The Attack Checks screen allows you to specify whether the VPN firewall should be protected against common attacks in the DMZ, LAN, and WAN networks. The various types of IPv4 attack checks are listed on the Attack Checks screen and defined in *Table 35* on page 171. For IPv6, the only options are to specify whether to allow a ping on the WAN port and whether to allow VPN pass-through for IPSec.

IPv4 Attack Checks

➢ **To enable IPv4 attack checks for your network environment:**

1. Select **Security > Firewall > Attack Checks**. In the upper right of the screen, the IPv4 radio button is selected by default. The Attack Checks screen displays the IPv4 settings:

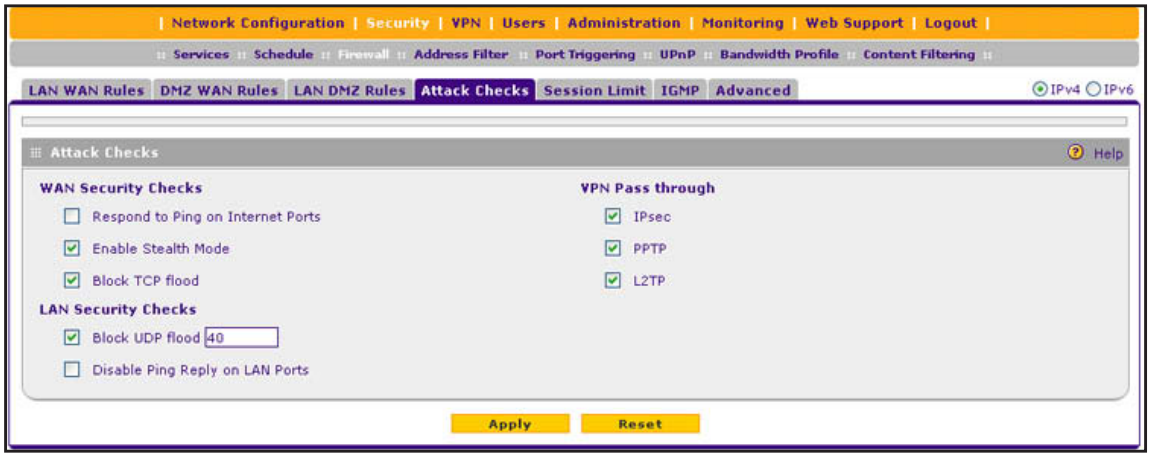

Figure 100.

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

Table 35. Attack Checks screen settings for IPv4

Setting	Description
WAN Security Checks	
Respond to Ping on Internet Ports	Select the **Respond to Ping on Internet Ports** check box to enable the VPN firewall to respond to a ping from the Internet to its IPv4 address. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to enable the VPN firewall to respond to a ping from the Internet.
Enable Stealth Mode	Select the **Enable Stealth Mode** check box (which is the default setting) to prevent the VPN firewall from responding to port scans from the WAN, thus making it less susceptible to discovery and attacks.
Block TCP flood	Select the **Block TCP flood** check box (which is the default setting) to enable the VPN firewall to drop all invalid TCP packets and to protect the VPN firewall from a SYN flood attack. A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN (synchronize) requests to a target system. When the system responds, the attacker does not complete the connections, thus leaving the connection half open and flooding the server with SYN messages. No legitimate connections can then be made.
LAN Security Checks	
Block UDP flood	Select the **Block UDP flood** check box (which is the default setting) to prevent the VPN firewall from accepting more than a specified number of simultaneous, active User Datagram Protocol (UDP) connections from a single device on the LAN. In the field, enter the number of connections per second that define a UDP flood. You can enter a number from 1 to 40. The default value is 40. The VPN firewall drops UDP packets that exceed the specified number of connections per second. A UDP flood is a form of denial of service attack that can be initiated when one device sends many UDP packets to random ports on a remote host. As a result, the distant host does the following: 1. Checks for the application listening at that port. 2. Sees that no application is listening at that port. 3. Replies with an ICMP Destination Unreachable packet. When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker might also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach the attacker, thus making the attacker's network location anonymous.
Disable Ping Reply on LAN Ports	Select the **Disable Ping Reply on LAN Ports** check box to prevent the VPN firewall from responding to a ping on a LAN port. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to prevent the VPN firewall from responding to a ping on a LAN port.

Table 35. Attack Checks screen settings for IPv4 (continued)

Setting	Description
VPN Pass through	
IPSec PPTP L2TP	When the VPN firewall functions in NAT mode, all packets going to the remote VPN gateway are first filtered through NAT and then encrypted according to the VPN policy. For example, if a VPN client or gateway on the LAN side of the VPN firewall wants to connect to another VPN endpoint on the WAN side (placing the VPN firewall between two VPN endpoints), encrypted packets are sent to the VPN firewall. Because the VPN firewall filters the encrypted packets through NAT, the packets become invalid unless you enable the VPN Pass through feature. To enable the VPN tunnel to pass the VPN traffic without any filtering, select any or all of the following check boxes: • **IPSec**. Disables NAT filtering for IPSec tunnels. • **PPTP**. Disables NAT filtering for PPTP tunnels. • **L2TP**. Disables NAT filtering for L2TP tunnels. By default, all three check boxes are selected.

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

IPv6 Attack Checks

➢ **To enable IPv6 attack checks for your network environment:**

1. Select **Security > Firewall > Attack Checks**.
2. In the upper right of the screen, select the **IPv6** radio button. The Attack Checks screen displays the IPv6 settings:

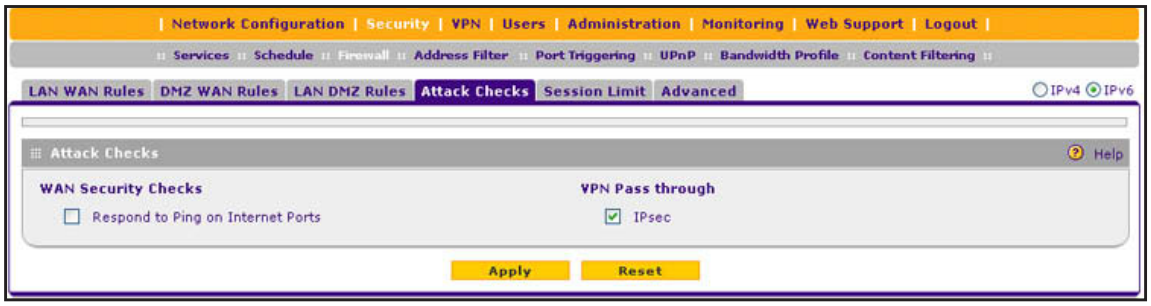

Figure 101.

3. Configure the following settings:
   - **Respond to Ping on Internet Ports**. Select the **Respond to Ping on Internet Ports** check box to enable the VPN firewall to respond to a ping from the Internet to its IPv6 address. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to enable the VPN firewall to respond to a ping from the Internet.
   - **IPsec**. Select the **IPsec** check box to enable IPSec VPN traffic that is initiated from the LAN to reach the WAN, irrespective of the default firewall outbound policy and custom firewall rules.
4. Click **Apply** to save your settings.

Set Limits for IPv4 Sessions

The session limits feature allows you to specify the total number of sessions that are allowed, per user, over an IPv4 connection across the VPN firewall. The session limits feature is disabled by default.

➢ **To enable and configure session limits:**

1. Select **Security > Firewall > Session Limit**. The Session Limit screen displays:

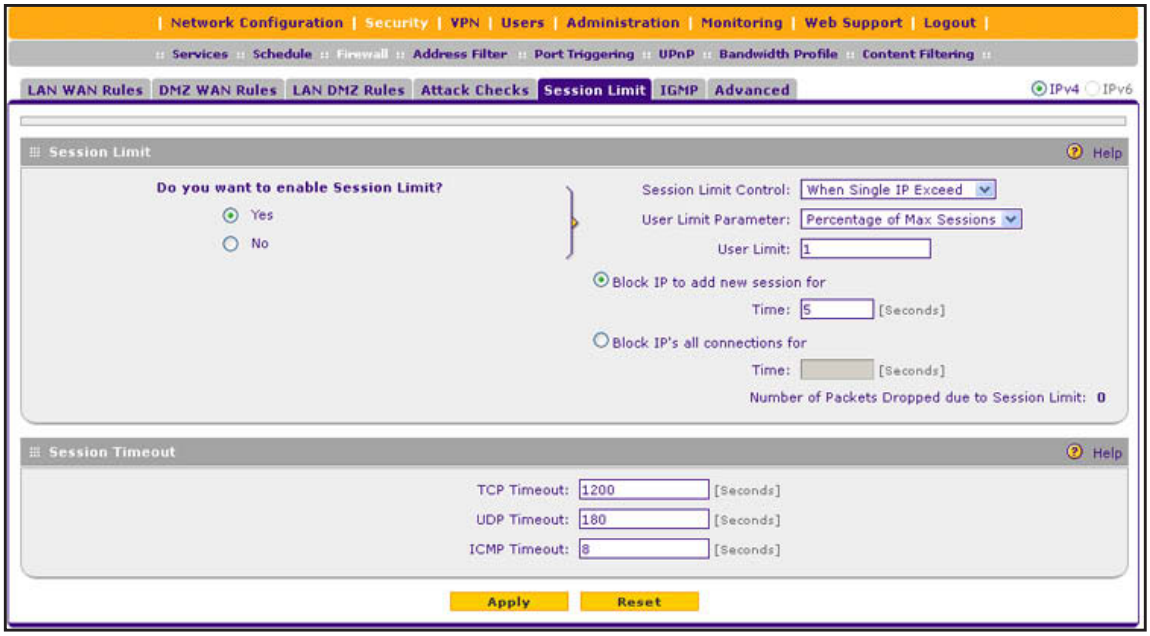

Figure 102.

2. Select the **Yes** radio button under Do you want to enable Session Limit?
3. Enter the settings as described in the following table:

Table 36. Session Limit screen settings

Setting	Description
Session Limit	
Session Limit Control	From the drop-down list, select one of the following options: • **When single IP exceeds**. When the limit is reached, no new session is allowed from the IP address. A new session is allowed only when an existing session is terminated or times out. You need to specify the action and period by selecting one of the following radio buttons: - **Block IP to add new session for**. No new session is allowed from the IP address for a period. In the time field, specify the period in seconds. - **Block IP's all connections for**. All sessions from the IP address are terminated, and new sessions are blocked for a period. In the time field, specify the period in seconds. • **Single IP Cannot Exceed**. When the limit is reached, no new session is allowed from the IP address for a specified period, or all sessions from the IP address are terminated and new sessions are blocked for a specified period.

Table 36. Session Limit screen settings (continued)

Setting	Description
User Limit Parameter	From the User Limit Parameter drop-down list, select one of the following options: • **Percentage of Max Sessions**. A percentage of the total session connection capacity of the VPN firewall. • **Number of Sessions**. An absolute number of maximum sessions.
User Limit	Enter a number to indicate the user limit. Note the following: • 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 VPN firewall. (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 you should consider when you configure a session limit.
Total Number of Packets Dropped due to Session Limit	This is a nonconfigurable counter that displays the total number of dropped packets when the session limit is reached.
Session Timeout	
TCP Timeout	For each protocol, specify a time-out in seconds. A session expires if no data for the session is received during the time-out period. The default time-out periods are 3600 seconds for TCP sessions, 180 seconds for UDP sessions, and 120 seconds for ICMP sessions.
UDP Timeout	
ICMP Timeout	

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

Configure Multicast Pass-Through for IPv4 Traffic

IP multicast pass-through allows multicast packets that originate in the WAN, such as packets from a media streaming or gaming application, to be forwarded to the LAN subnet. Internet Group Management Protocol (IGMP) is used to support multicast between IP hosts and their adjacent neighbors.

➢ **To configure multicast pass-through:**

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

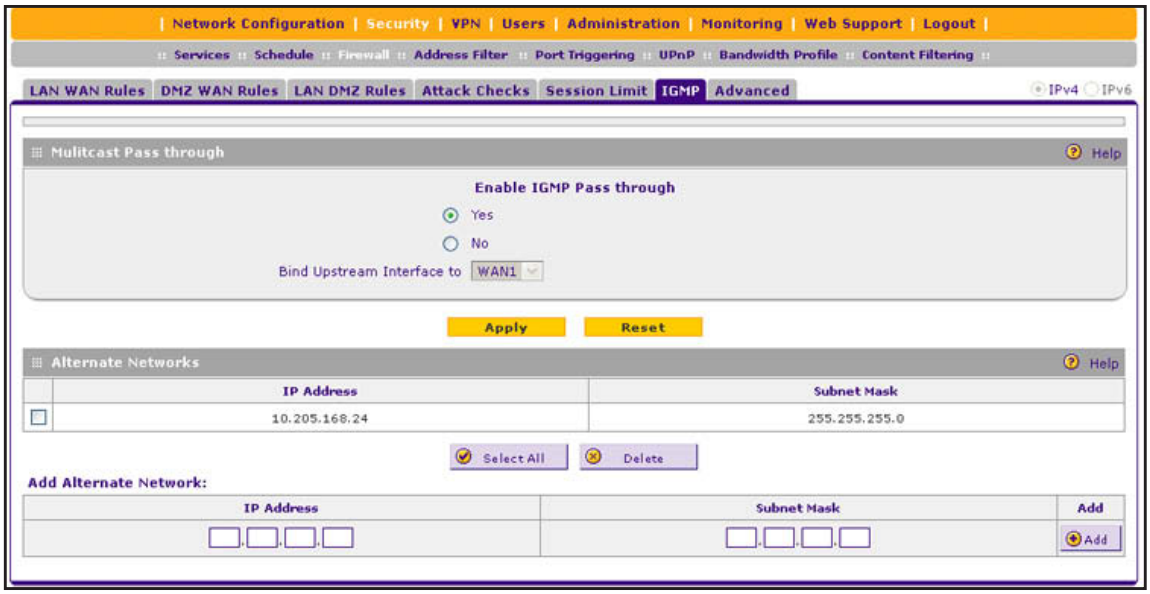

Figure 103.

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

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

3. If load balancing is configured, select the upstream interface to which multicast traffic is bound because only a single interface can function as the upstream interface. From the Bind Upstream Interface to drop-down list, select the interface. The default interface is WAN1.

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

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

   a. In the Alternate Networks section of the screen, below the table, enter the following settings:

   - **IP Address**. Enter the multicast source IP address.
   - **Subnet Mask**. Enter the subnet mask for the multicast source address.

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

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

➢ **To delete one or more multicast source addresses:**

1. In the Alternate Networks table, select the check box to the left of each address that you want to delete, or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Manage the Application Level Gateway for SIP Sessions

The application level gateway (ALG) facilitates multimedia sessions such as voice over IP (VoIP) sessions that use the Session Initiation Protocol (SIP) across the firewall and provides support for multiple SIP clients. SIP support for the ALG, which is an IPv4 feature, is disabled by default.

➢ **To enable ALG for SIP:**

1. Select **Security > Firewall > Advanced**. The Advanced screen displays:

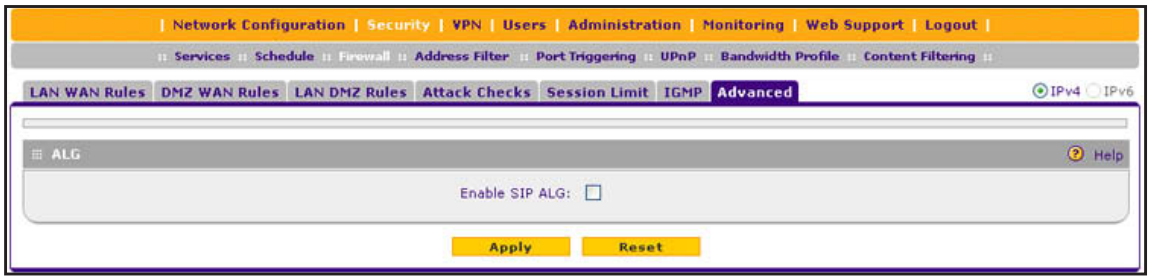

Figure 104.

2. Select the **Enable SIP ALG** check box.
3. Click **Apply** to save your settings.

Services, Bandwidth Profiles, and QoS Profiles

- *Add Customized Services*
- *Create IP Groups*
- *Create Bandwidth Profiles*
- *Create Quality of Service Profiles for IPv4 Firewall Rules*
- *Quality of Service Priorities for IPv6 Firewall Rules*

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 and IP groups, see *Add Customized Services* on page 177 and *Create IP Groups* on page 179.
- **Bandwidth profiles**. A bandwidth profile allocates and limits traffic bandwidth for the LAN users to which an IPv4 firewall rule is applied. For information about creating bandwidth profiles, see *Create Bandwidth Profiles* on page 181.

- **QoS profiles and priorities**. 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 for IPv4 firewall rules, see *Create Quality of Service Profiles for IPv4 Firewall Rules* on page 184. For information about predefined QoS priorities that are available for IPv6 firewall rules, see *Quality of Service Priorities for IPv6 Firewall Rules* on page 186.

Note: A schedule narrows down the period during which a firewall rule is applied. For information about specifying schedules, see *Set a Schedule to Block or Allow Specific Traffic* on page 189.

Add Customized Services

Services are functions performed by server computers at the request of client computers. You can configure up to 124 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. However, on the VPN firewall you can select service numbers in the range from 1 to 65535.

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

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

➢ **To add a customized service:**

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

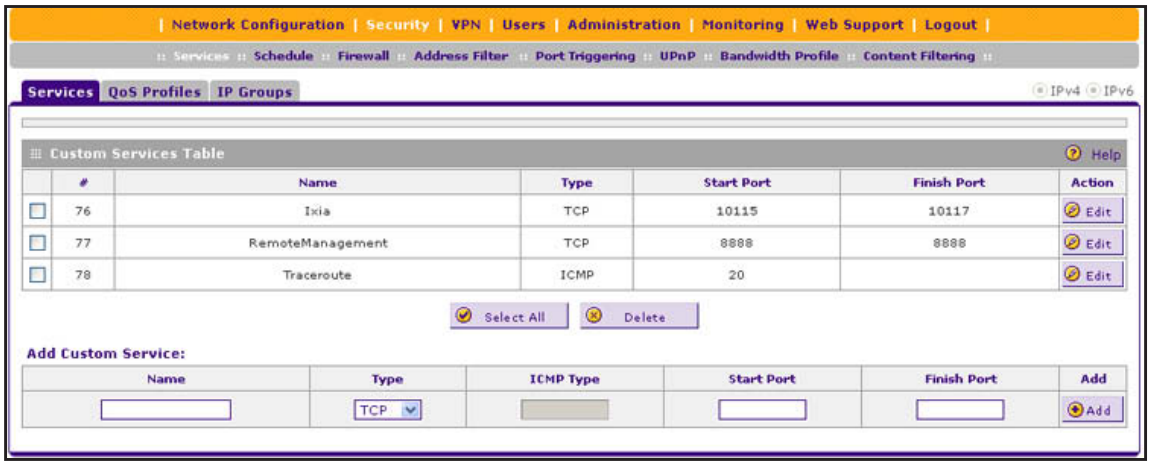

Figure 105.

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

Table 37. Services screen settings

Setting	Description
Name	A descriptive name of the service for identification and management purposes.
Type	From the Type drop-down list, select the Layer 3 protocol that the service uses as its transport protocol: • **TCP** • **UDP** • **ICMP** • **ICMPv6**
ICMP Type	A numeric value that can range between 0 and 40. For a list of ICMP types, see *http://www.iana.org/assignments/icmp-parameters*. **Note:** This field is enabled only when you select ICMP or ICMPv6 from the Type drop-down list.
Start Port	The first TCP or UDP port of a range that the service uses. **Note:** This field is enabled only when you select TCP or UDP from the Type drop-down list.
Finish Port	The last TCP or UDP port of a range that the service uses. If the service uses only a single port number, enter the same number in the Start Port and Finish Port fields. **Note:** This field is enabled only when you select TCP or UDP from the Type drop-down list.

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

➢ **To edit a service:**

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

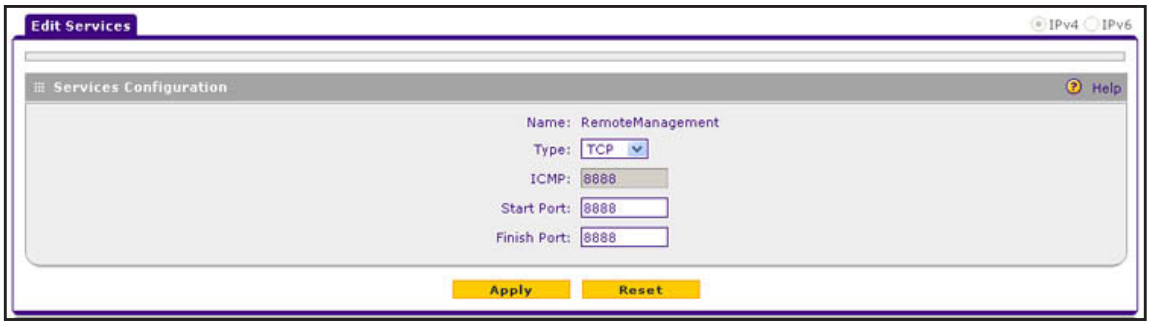

Figure 106.

2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified service is displayed in the Custom Services table.

➢ **To delete one or more services:**

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

Create IP Groups

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

➢ **To create an IP group:**

1. Select **Security > Services > IP Groups**. The IP Groups screen displays. (The following figure shows two groups in the Custom IP Groups Table as examples.)

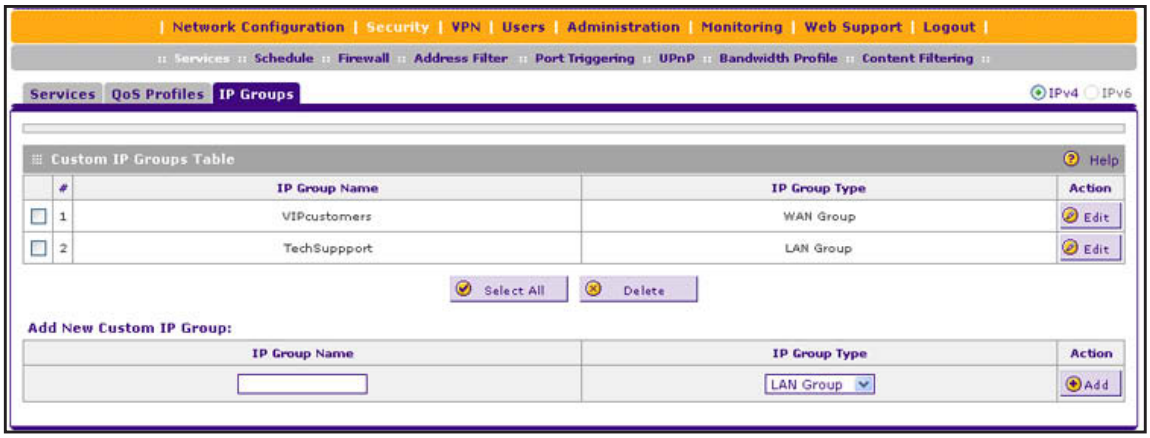

Figure 107.

2. In the Add New Custom IP Group section of the screen, do the following:
   - In the IP Group Name field, enter a name for the group.
   - From the IP Group Type drop-down list, select **LAN Group** or **WAN Group**.
3. Click **Apply** to save your changes. The new IP group is displayed in the Custom IP Groups Table.
4. In the Custom IP Groups Table, click the **Edit** table button to the right of the IP group that you just created. The Edit IP Group screen displays. (The following figure shows two IP addresses in the IP Addresses Grouped table as examples.)

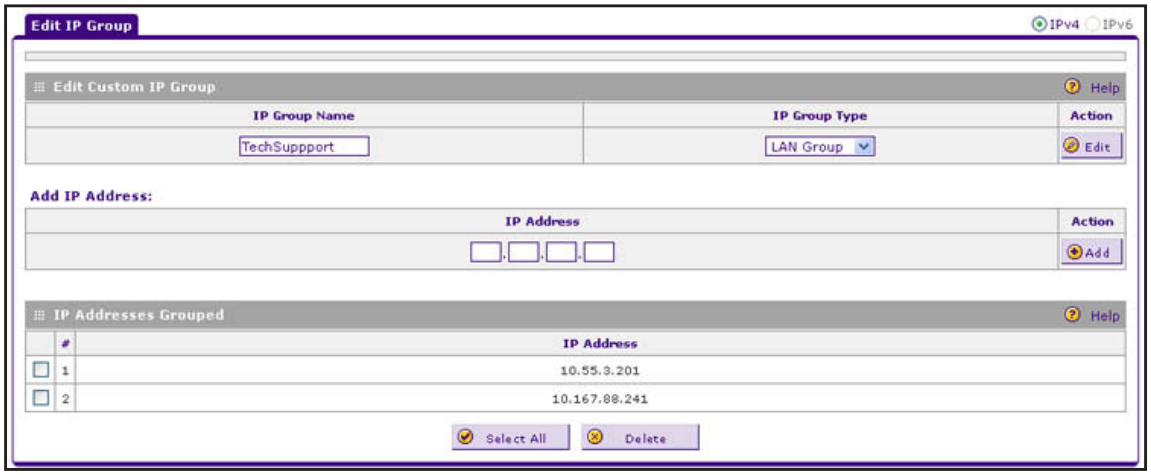

Figure 108.

5. In the IP Address fields, type an IP address.
6. Click the **Add** table button to add the IP address to the IP Addresses Grouped table.
7. Repeat the previous two steps to add more IP addresses to the IP Addresses Grouped table.
8. Click the **Edit** table button to return to the IP Groups screen.

➢ **To edit an IP group:**

1. In the Custom IP Groups Table, click the **Edit** table button to the right of the IP group that you want to edit. The Edit IP Group screen displays.
2. In the Edit New Custom IP Group section of the screen, modify the settings that you wish to change:
   - You can change the group name.
   - You can change the group type.
   - You can delete an IP address from the IP Addresses Grouped table by selecting the check box to the left of the IP address that you want to delete and then clicking the **Delete** table button. You can delete all IP addresses by clicking the **Select All** table button and clicking the **Delete** table button.
   - You can add IP addresses to the IP Addresses Grouped Table (see *Step 4*, *Step 5*, and *Step 6* in the previous procedure).
3. Click the **Edit** table button to return to IP Groups screen.

➢ **To delete an IP group:**

1. In the Custom IP Groups table, select the check box to the left of the IP group that you want to delete, or click the **Select All** table button to select all groups.
2. Click the **Delete** table button.

Create Bandwidth Profiles

Bandwidth profiles determine how data is communicated with the hosts. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic, thus allocating LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN link. A single bandwidth profile can be for both outbound and inbound traffic.

For outbound IPv4 traffic, you can apply bandwidth profiles on the WAN interface; for inbound IPv4 traffic, you can apply bandwidth profiles to a LAN interface. Bandwidth profiles do not apply to the DMZ interface, nor to IPv6 traffic.

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 for IPv4 (see *Figure 77* on page 148)
- Add LAN WAN Inbound Services screen for IPv4 (see *Figure 79* on page 150)

➢ **To add and enable a bandwidth profile:**

1. Select **Security > Bandwidth Profiles**. The Bandwidth Profiles screen displays. (The following figure shows some examples.)

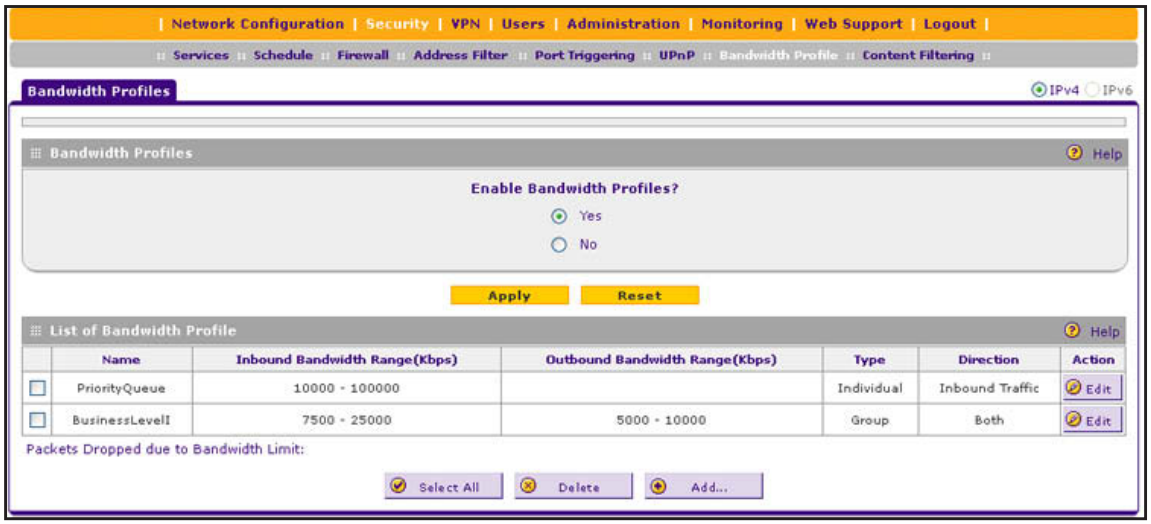

Figure 109.

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

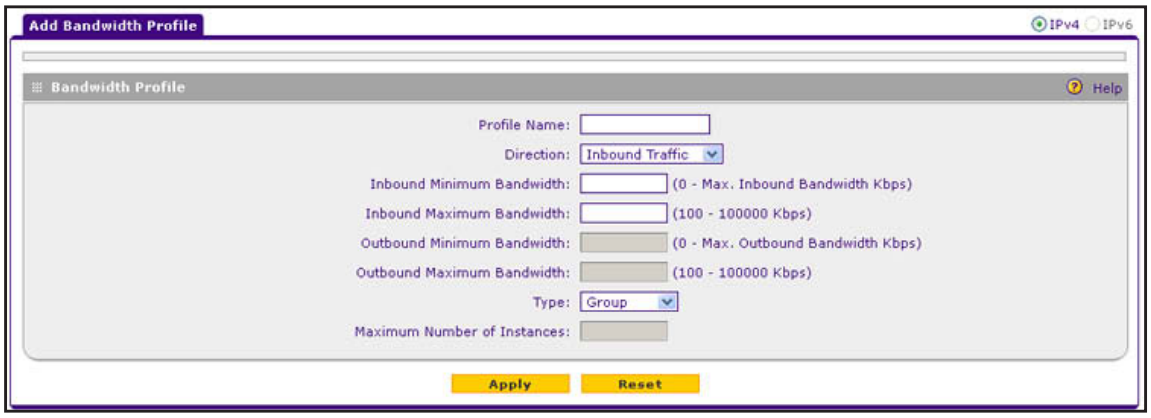

Figure 110.

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

Table 38. Add Bandwidth Profile screen settings

Setting	Description
Profile Name	A descriptive name of the bandwidth profile for identification and management purposes.
Direction	From the Direction drop-down list, select the traffic direction for the bandwidth profile: • **Inbound Traffic**. The bandwidth profile is applied only to inbound traffic. Specify the inbound minimum and maximum bandwidths. • **Outbound Traffic**. The bandwidth profile is applied only to outbound traffic. Specify the outbound minimum and maximum bandwidths. • **Both**. The bandwidth profile is applied to both outbound and inbound traffic. Specify both the outbound and inbound minimum and maximum bandwidths.

Table 38. Add Bandwidth Profile screen settings (continued)

Setting	Description	
Inbound Minimum Bandwidth	The inbound minimum allocated bandwidth in Kbps. There is no default setting.	
Inbound Maximum Bandwidth	The inbound maximum allowed bandwidth in Kbps. The maximum allowable bandwidth is 100,000 Kbps, and you cannot configure less than 100 Kbps. There is no default setting.	
Outbound Minimum Bandwidth	The outbound minimum allocated bandwidth in Kbps. There is no default setting.	
Outbound Maximum Bandwidth	The outbound maximum allowed bandwidth in Kbps. The maximum allowable bandwidth is 100,000 Kbps, and you cannot configure less than 100 Kbps. There is no default setting.	
Type	From the Type drop-down list, select the type for the bandwidth profile: • **Group**. The profile applies to all users, that is, all users share the available bandwidth. • **Individual**. The profile applies to an individual user, that is, each user can use the available bandwidth.	
	Maximum Number of Instances	If you select Individual from the Type drop-down list, you need to specify the maximum number of class instances that can be created by the individual bandwidth profile. **Note:** If the number of users exceeds the configured number of instances, the same bandwidth is shared among all the users of that bandwidth profile.

4. Click **Apply** to save your settings. The new bandwidth profile is added to the List of Bandwidth Profiles table.
5. In the Bandwidth Profiles section of the screen, select the **Yes** radio button under Enable Bandwidth Profiles? (By default, the **No** radio button is selected.)
6. Click **Apply** to save your settings.

➢ **To edit a bandwidth profile:**

1. In the List of Bandwidth Profiles table, click the **Edit** table button to the right of the bandwidth profile that you want to edit. The Edit Bandwidth Profile screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified bandwidth profile is displayed in the List of Bandwidth Profiles table.

➢ **To delete one or more bandwidth profiles:**

1. In the List of Bandwidth Profiles table, select the check box to the left of each bandwidth profile that you want to delete, or click the **Select All** table button to select all profiles.
2. Click the **Delete** table button to delete the selected profile or profiles.

Create Quality of Service Profiles for IPv4 Firewall Rules

A Quality of Service (QoS) profile defines the relative priority of an IP packet when multiple connections are scheduled for simultaneous transmission on the VPN firewall. A QoS profile becomes active only when it is associated with a nonblocking inbound or outbound firewall rule or service, and traffic matching the firewall rule or service is processed by the VPN firewall. Priorities are defined by *Type of Service in the Internet Protocol Suite standards*, RFC 1349.

You can assign a QoS profile to an IPv4 firewall rule on the following screens:

- Add LAN WAN Outbound Services screen for IPv4 (see *Figure 77* on page 148)
- Add LAN WAN Inbound Services screen for IPv4 (see *Figure 79* on page 150)
- Add DMZ WAN Outbound Services screen for IPv4 (see *Figure 83* on page 154)
- Add DMZ WAN Inbound Services screen for IPv4 (*Figure 85* on page 156)

There is no default QoS profile on the VPN firewall. You *could* create QoS profiles similar to the QoS priorities that are listed in the following section, *Quality of Service Priorities for IPv6 Firewall Rules*.

Note: To configure and apply QoS profiles successfully, familiarity with QoS concepts such QoS priority queues, IP precedence, DHCP, and their values is helpful.

➢ **To create a QoS profile:**

1. Select **Security > Services > QoS Profiles**. The QoS Profiles screen displays. (The following figure shows some profiles in the List of QoS Profiles table as examples.)

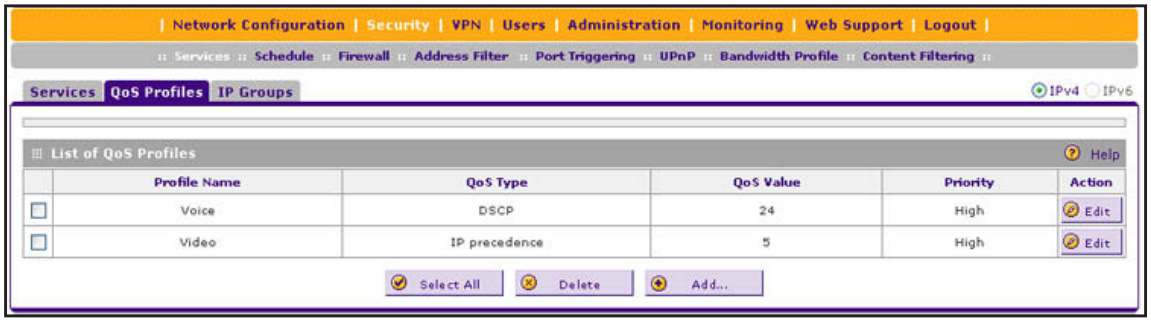

Figure 111.

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

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

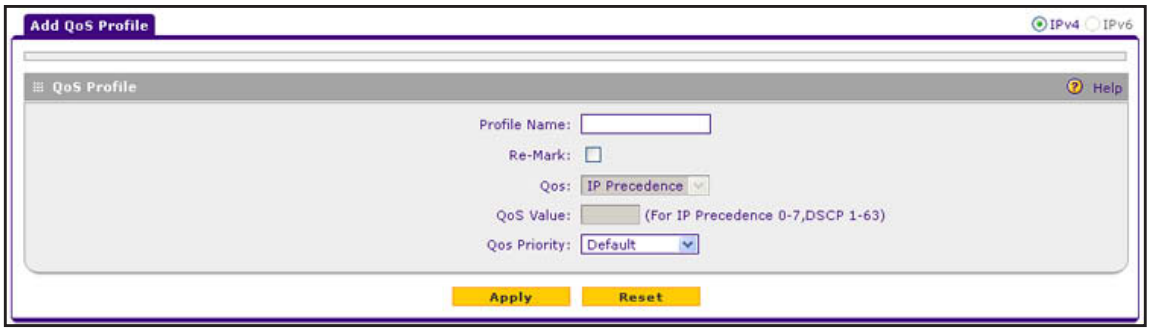

Figure 112.

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

Table 39. Add QoS Profile screen settings

Setting	Description	
Profile Name	A descriptive name of the QoS profile for identification and management purposes.	
Re-Mark	Select the **Re-Mark** check box to set the Differentiated Services (DiffServ) mark in the Type of Service (ToS) byte of an IP header by specifying the QoS type (IP precedence or DHCP) and QoS value. If you clear the Re-Mark check box (which is the default setting), the QoS profile is specified only by the QoS priority.	
	QoS	From the QoS drop-down list, select one of the following traffic classification methods: • **IP Precedence**. A legacy method that sets the priority in the ToS byte of an IP header. • **DSCP**. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (which is the same as the ToS byte) of an IP header.
	QoS Value	The QoS value in the ToS or DiffServ byte of an IP header. The QoS value that you enter depends on your selection from the QoS drop-down list: • For IP Precedence, select a value from 0 to 7. • For DSCP, select a value from 1 to 63.
QoS Priority	The QoS priority represents the classification level of the packet among the priority queues within the VPN firewall. If you select **Default**, packets are mapped based on the ToS bits in their IP headers. From the QoS Priority drop-down list, select one of the following priority queues: • **Default** • **High** • **Medium High** • **Medium** • **Low**	

4. Click **Apply** to save your settings. The new QoS profile is added to the List of QoS Profiles table.

- **To edit a QoS profile:**

  1. In the List of QoS Profiles table, click the **Edit** table button to the right of the QoS profile that you want to edit. The Edit QoS Profile screen displays.
  2. Modify the settings that you wish to change (see the previous table).
  3. Click **Apply** to save your changes. The modified QoS profile is displayed in the List of QoS Profiles table.

- **To delete a QoS profile:**

  1. In the List of QoS Profiles table, select the check box to the left of the QoS profile that you want to delete, or click the **Select All** table button to select all profiles.
  2. Click the **Delete** table button.

Quality of Service Priorities for IPv6 Firewall Rules

For IPv6 firewall rules and services, you cannot configure QoS profiles, but there are default QoS priorities that you can assign on the following screens:

- Add LAN WAN Outbound Services screen for IPv6 (see *Figure 78* on page 149)
- Add DMZ WAN Outbound Services screen for IPv6 (see *Figure 84* on page 155)

QoS priorities are preconfigured and cannot be edited:

- **Normal-Service**. Used when no special priority is given to the traffic. IP packets are marked with a ToS value of 0.
- **Minimize-Cost**. Used when data needs to be transferred over a link that has a lower cost. IP packets are marked with a ToS value of 2.
- **Maximize-Reliability**. Used when data needs to travel to the destination over a reliable link and with little or no retransmission. IP packets are marked with a ToS value of 4.
- **Maximize-Throughput**. Used when the volume of data transferred during an interval is important even if the latency over the link is high. IP packets are marked with a ToS value of 8.
- **Minimize-Delay**. Used when the time required (latency) for the packet to reach the destination needs to be low. IP packets are marked with a ToS value of 16.

Configure Content Filtering

To restrict internal LAN users from access to certain sites on the Internet, you can use the content filtering and web component blocking features of the VPN firewall. By default, these features are disabled; all requested traffic from any website is allowed. If you enable one or more of these features and users try to access a blocked site, they see a “Blocked by NETGEAR” message.

Note: Content filtering is supported for IPv4 users and groups only.

Several types of blocking are available:

- **Web component blocking**. You can block the following web component types: proxy, Java, ActiveX, and cookies. Even sites that are listed in the Trusted Domains table are subject to web component blocking when the blocking of a particular web component is enabled.
  - **Proxy**. A proxy server (or simply, proxy) allows computers to route connections to other computers through the proxy, thus circumventing certain firewall rules. For example, if connections to a specific IP address are blocked by a firewall rule, the requests can be routed through a proxy that is not blocked by the rule, rendering the restriction ineffective. Enabling this feature blocks proxy servers.
  - **Java**. Blocks Java applets from being downloaded from pages that contain them. Java applets are small programs embedded in web pages that enable dynamic functionality of the page. A malicious applet can be used to compromise or infect computers. Enabling this setting blocks Java applets from being downloaded.
  - **ActiveX**. Similar to Java applets, ActiveX controls are installed on a Windows computer running Internet Explorer. A malicious ActiveX control can be used to compromise or infect computers. Enabling this setting blocks ActiveX applets from being downloaded.
  - **Cookies**. Cookies are used to store session information by websites that usually require login. However, several websites use cookies to store tracking information and browsing habits. Enabling this option blocks cookies from being created by a website.

Note: Many websites require that cookies be accepted for the site to be accessed correctly. Blocking cookies might interfere with useful functions provided by these websites.

- **Keyword blocking (domain name blocking)**. You can specify up to 32 words to block. If any of these words appear in the website name (URL) or in a newsgroup name, the website or newsgroup is blocked by the VPN firewall.

  You can apply the keywords to one or more LAN groups. Requests from the computers in the groups are blocked where keyword blocking has been enabled. Blocking does not occur for the computers in the groups where keyword blocking has been disabled.

  You can bypass keyword blocking for trusted domains by adding the exact matching domain to the Trusted Domains table. Access to the domains or keywords on this list by computers in the groups for which keyword blocking has been enabled is allowed without any blocking.

  Keyword application examples:

  - If the keyword “xxx” is specified, the URL http://www.companycom/xxx.html is blocked, as is the newsgroup alt.pictures.xxx.

- If the keyword ".com" is specified, only websites with other domain suffixes (such as .edu, .org, or .gov) can be viewed.
- If you wish to block all Internet browsing access, enter **.** (period) as the keyword.

➢ **To enable and configure content filtering:**

1. Select **Security > Content Filtering**. The Block Sites screen displays. (The following figure shows some examples.)

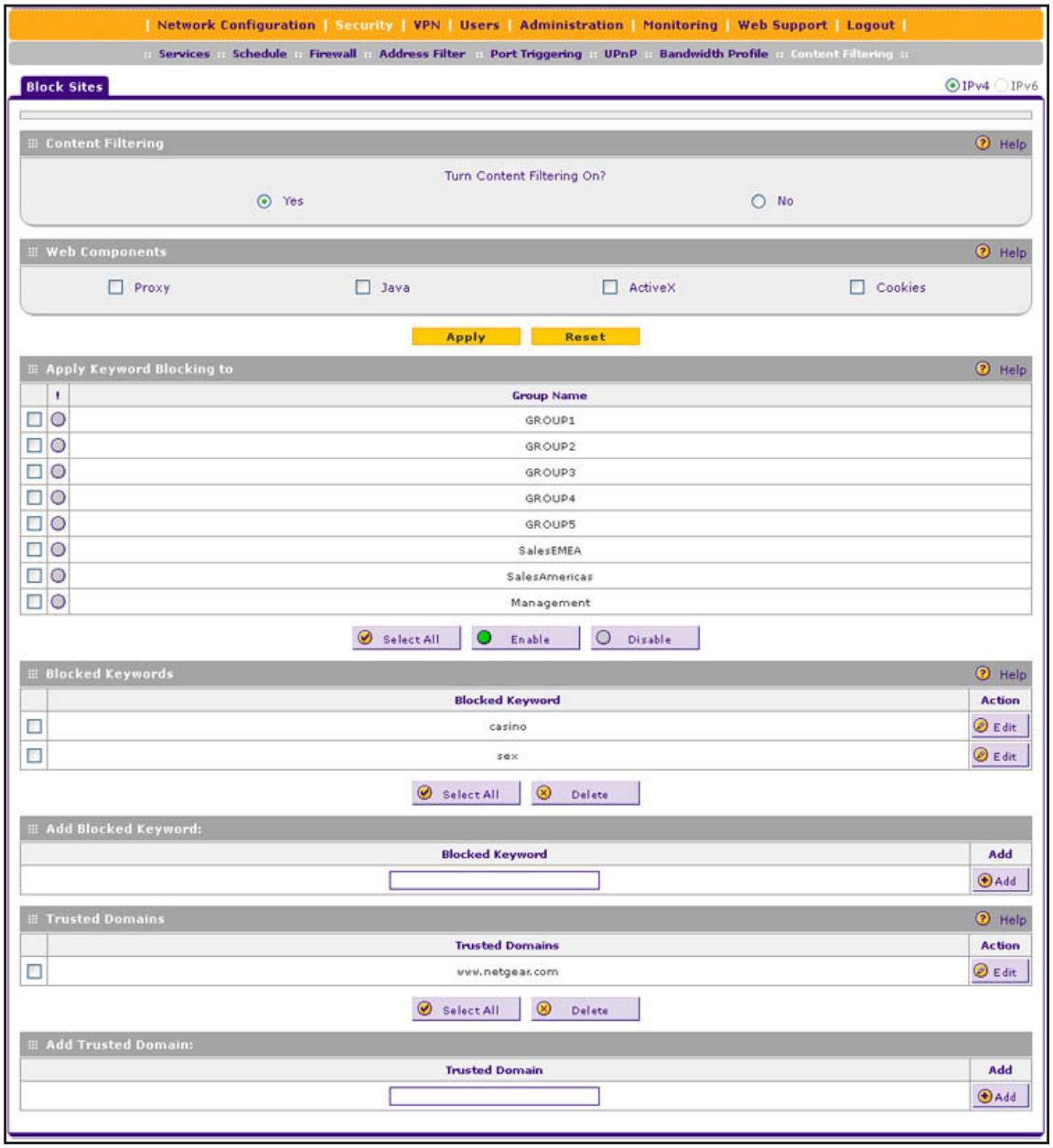

Figure 113.

2. In the Content Filtering section of the screen, select the **Yes** radio button.

3. In the Web Components section of the screen, select the components that you want to block (by default, none of these components are blocked, that is, none of these check boxes are selected):
   - **Proxy**. Blocks proxy servers.
   - **Java**. Blocks Java applets from being downloaded.
   - **ActiveX**. Blocks ActiveX applets from being downloaded.
   - **Cookies**. Blocks cookies from being created by a website.

   These components are described in the introduction of this section on page 186.
4. Click **Apply** to enable content filtering and blocking of the selected web components. The screen controls are activated.

➢ **To apply keyword blocking to LAN groups:**

1. In the Apply Keyword Blocking to section of the screen, select the check boxes for the groups to which you want to apply keyword blocking, or click the **Select All** button to select all groups.
2. To activate keyword blocking for these groups, click the **Enable** button. To deactivate keyword blocking for the selected groups, click the **Disable** button.

Note: If you changed the LAN group names on the Edit Group Names screen (see *Change Group Names in the Network Database* on page 100), the new names are displayed on the Block Sites screen.

➢ **To build your list of blocked keywords or blocked domain names:**

1. In the Add Blocked Keyword section of the screen, in the Blocked Keyword field, enter a keyword or domain name.
2. After each entry, click the **Add** table button. The keyword or domain name is added to the Blocked Keywords table.

   To edit an entry, click the **Edit** table button in the Action column to the right of the entry.

➢ **To build your list of trusted domains:**

1. In the Add Trusted Domain section of the screen, in the Trusted Domains field, enter a domain name.
2. After each entry, click the **Add** table button. The domain name is added to the Trusted Domains table.

   To edit an entry, click the **Edit** table button in the Action column to the right of the entry.

Set a Schedule to Block or Allow Specific Traffic

Schedules define the time frames under which firewall rules can be applied. Three schedules, Schedule 1, Schedule 2, and Schedule 3, can be defined, and you can select any one of these when defining firewall rules.

➢ **To set a schedule:**

1. Select **Security > Services > Schedule 1**. The Schedule 1 screen displays:

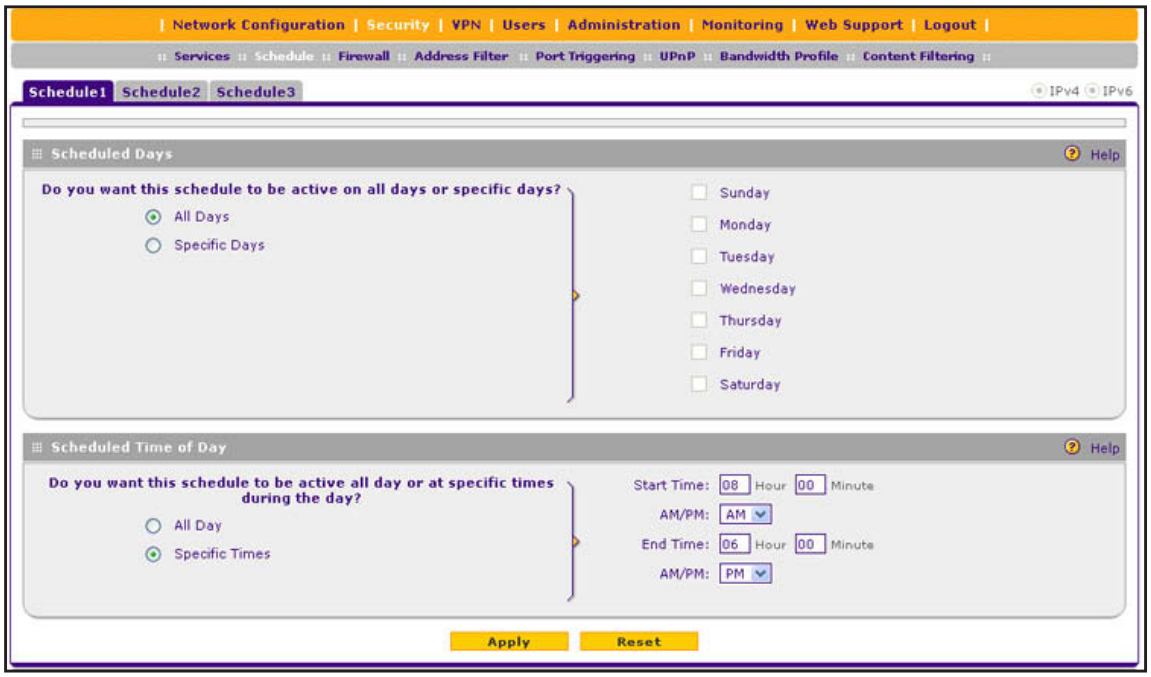

Figure 114.

2. In the Scheduled Days section, select one of the following radio buttons:
   - **All Days**. The schedule is in effect all days of the week.
   - **Specific Days**. The schedule is in effect only on specific days. To the right of the radio buttons, select the check box for each day that you want the schedule to be in effect.
3. In the Scheduled Time of Day section, select one of the following radio buttons:
   - **All Day**. The schedule is in effect all hours of the selected day or days.
   - **Specific Times**. The schedule is in effect only during specific hours of the selected day or days. To the right of the radio buttons, fill in the Start Time and End Time fields (Hour, Minute, AM/PM) during which the schedule is in effect.
4. Click **Apply** to save your settings to Schedule 1.

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

Enable Source MAC Filtering

The Source MAC Filter screen enables you to permit or block traffic coming from certain known computers or devices.

By default, the source MAC address filter is disabled. All the traffic received from computers 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 computers 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 137.

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

1. Select **Security > Address Filter**. The Address Filter submenu tabs display, with the Source MAC Filter screen in view. (The following figure shows one address in the MAC Addresses table as an example.)

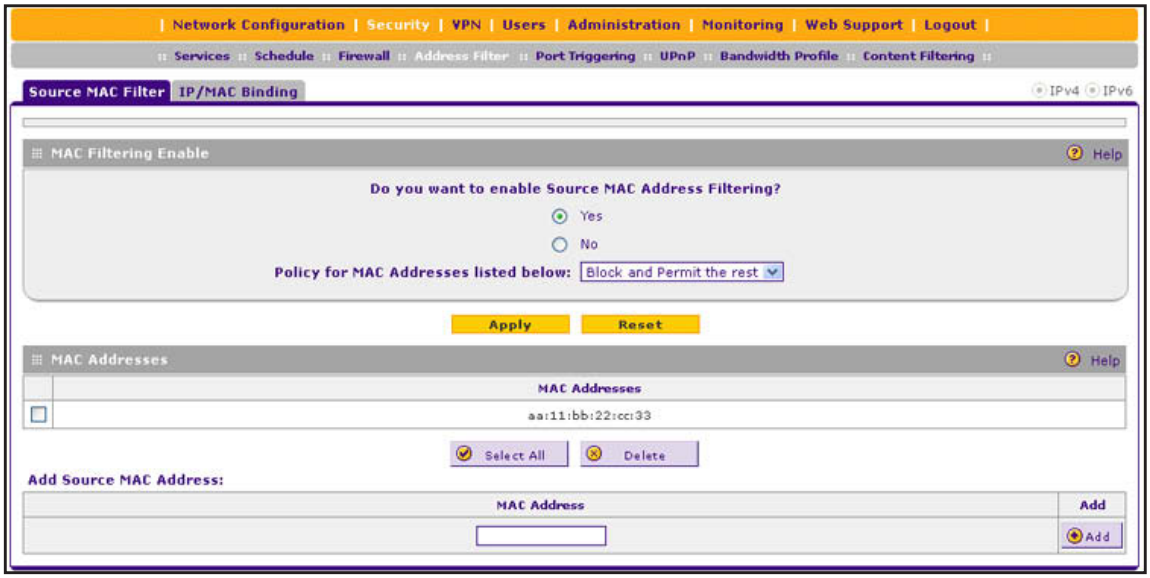

Figure 115.

2. In the MAC Filtering Enable section, select the **Yes** radio button.
3. In the same section, from the Policy for MAC Addresses listed below drop-down list, select one of the following options:
   - **Block and Permit the rest**. Traffic coming from all addresses in the MAC Addresses table is blocked. Traffic from all other MAC addresses is permitted.
   - **Permit and Block the rest**. Traffic coming from all addresses in the MAC Addresses table is permitted. Traffic from all other MAC addresses is blocked.
4. Click **Apply** to save your settings. The MAC Address field in the Add Source MAC Address section of the screen now becomes available.
5. Build your list of source MAC addresses to be permitted or blocked by entering the first MAC address in the MAC Address field. A MAC address needs to be entered in the format xx:xx:xx:xx:xx:xx, in which x is a numeric (0 to 9) or a letter between a and f (inclusive), for example: aa:11:bb:22:cc:33.

WARNING:

If you select Permit and Block the rest from the drop-down list but do not add the MAC address of the computer from which you are accessing the web management interface, you are locked out of the web management interface.

6. Click the **Add** table button. The MAC address is added to the MAC Addresses table.
7. Repeat the previous two steps to add more MAC addresses to the MAC Addresses table.

➢ **To remove one or more MAC addresses from the table:**

1. Select the check box to the left of each MAC address that you want to delete, or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Set Up IP/MAC Bindings

IP/MAC binding allows you to bind an IPv4 or IPv6 address to a MAC address and the other way around. Some computers or devices are configured with static addresses. To prevent users from changing their static IP addresses, the IP/MAC binding feature needs to be enabled on the VPN firewall. If the VPN firewall detects packets with an IP address that matches the IP address in the IP/MAC Bindings table but does not match the related MAC address in the IP/MAC Bindings table (or the other way around), the packets are dropped. If you have enabled the logging option for the IP/MAC binding feature, these packets are logged before they are dropped. The VPN firewall displays the total number of dropped packets that violate either the IP-to-MAC binding or the MAC-to-IP binding.

Note: You can bind IP addresses to MAC addresses for DHCP assignment on the LAN Groups submenu. See *Manage the Network Database* on page 97.

As an example, assume that three computers on the LAN are set up as follows, and that their IPv4 and MAC addresses are added to the IP/MAC Bindings table:

- Host 1. MAC address (00:01:02:03:04:05) and IP address (192.168.10.10)
- Host 2. MAC address (00:01:02:03:04:06) and IP address (192.168.10.11)
- Host 3. MAC address (00:01:02:03:04:07) and IP address (192.168.10.12)

There are three possible scenarios in relation to the addresses in the IP/MAC Bindings table:

- Host 1 has not changed its IP and MAC addresses. A packet coming from Host 1 has IP and MAC addresses that match those in the IP/MAC Bindings table.

- Host 2 has changed its MAC address to 00:01:02:03:04:09. The packet has an IP address that matches the IP address in the IP/MAC Bindings table but a MAC address that does not match the MAC address in the IP/MAC Bindings table.
- Host 3 has changed its IP address to 192.168.10.15. The packet has a MAC address that matches the MAC address in the IP/MAC Bindings table but an IP address that does not match the IP address in the IP/MAC Bindings table.

In this example, the VPN firewall blocks the traffic coming from Host 2 and Host 3, but allows the traffic coming from Host 1 to any external network. The total count of dropped packets is displayed.

IPv4/MAC Bindings

➢ **To set up a binding between a MAC address and an IPv4 address:**

1. Select **Security > Address Filter > IP/MAC Binding**. In the upper right of the screen, the IPv4 radio button is selected by default. The IP/MAC Binding screen displays the IPv4 settings. (The following figure shows a binding in the IP/MAC Binding table as an example.)

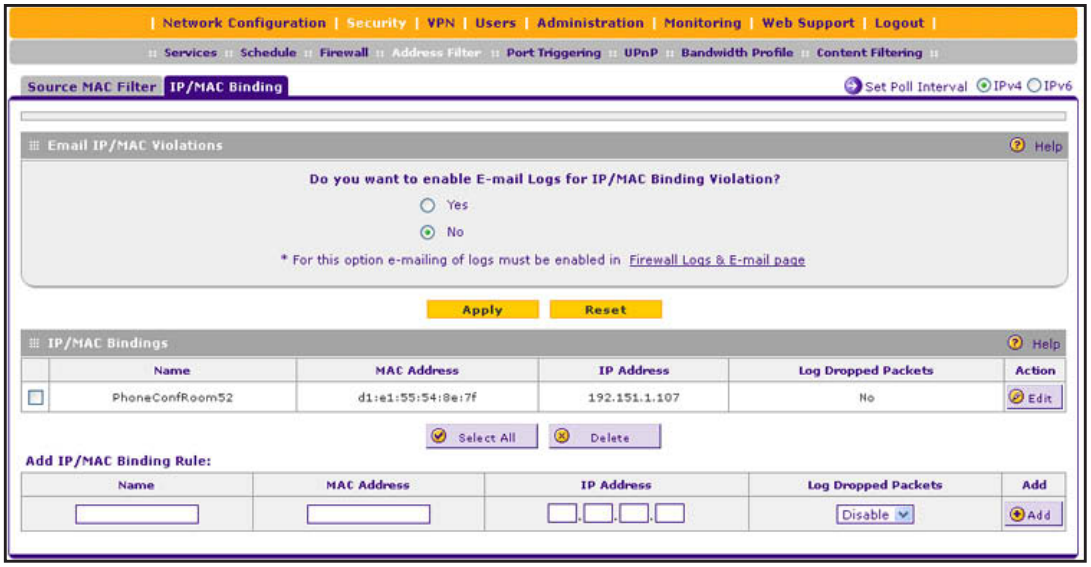

Figure 116.

2. In the Email IP/MAC Violations section of the screen, specify if you want to enable email logs for IP/MAC binding violations. (You have to do this only once.) Select one of the following radio buttons:
   - **Yes**. IP/MAC binding violations are emailed. Click the **Firewall Logs & E-mail page** link to ensure that emailing of logs is enabled on the Firewall Logs & E-mail screen (see *Configure Logging, Alerts, and Event Notifications* on page 362).
   - **No**. IP/MAC binding violations are not emailed.
3. Click **Apply** to save your changes.

4. In the IP/MAC Bindings sections of the screen, enter the settings as described in the following table:

Table 40. IP/MAC Binding screen settings for IPv4

Setting	Description
Name	A descriptive name of the binding for identification and management purposes.
MAC Address	The MAC address of the computer or device that is bound to the IP address.
IP Address	The IPv4 address of the computer or device that is bound to the MAC address.
Log Dropped Packets	To log the dropped packets, select **Enable** from the drop-down list. The default setting is Disable.

5. Click the **Add** table button. The new IP/MAC rule is added to the IP/MAC Bindings table.

➢ **To edit an IP/MAC binding:**

1. In the IP/MAC Bindings table, click the **Edit** table button to the right of the IP/MAC binding that you want to edit. The Edit IP/MAC Binding screen displays.
2. Modify the settings that you wish to change (see the previous table; you can change the MAC address, IPv4 address, and logging status).
3. Click **Apply** to save your changes. The modified IP/MAC binding displays in the IP/MAC Bindings table.

➢ **To remove one or more IP/MAC bindings from the table:**

1. Select the check box to the left of each IP/MAC binding that you want to delete, or click the **Select All** table button to select all bindings.
2. Click the **Delete** table button.

➢ **To change the IPv4 MAC polling interval from its default setting of 10 seconds:**

1. On the IP/MAC Bindings screen for IPv4, to the right of the IP/MAC Binding tab, click the **Set Poll Interval** option arrow. The IP MAC Binding Poll Interval pop-up screen displays:

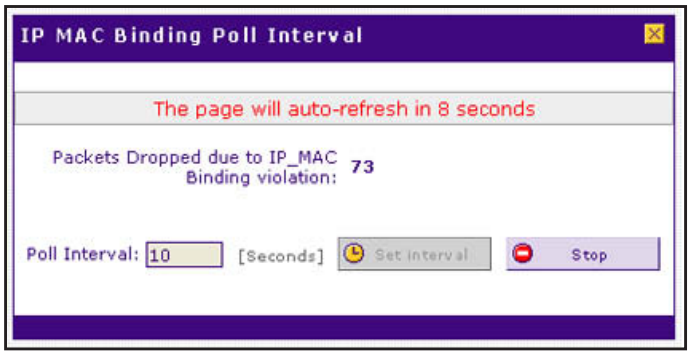

Figure 117.

2. Click the **Stop** button. Wait until the Poll Interval field becomes available.
3. Enter new poll interval in seconds.

4. Click the **Set Interval** button. Wait for the confirmation that the operation has succeeded before you close the window.

IPv6/MAC Bindings

➢ **To set up a binding between a MAC address and an IPv6 address:**

1. Select **Security > Address Filter > IP/MAC Binding**.
2. In the upper right of the screen, select the **IPv6** radio button. The IP/MAC Binding screen displays the IPv6 settings. (The following figure shows a binding in the IP/MAC Binding table as an example.)

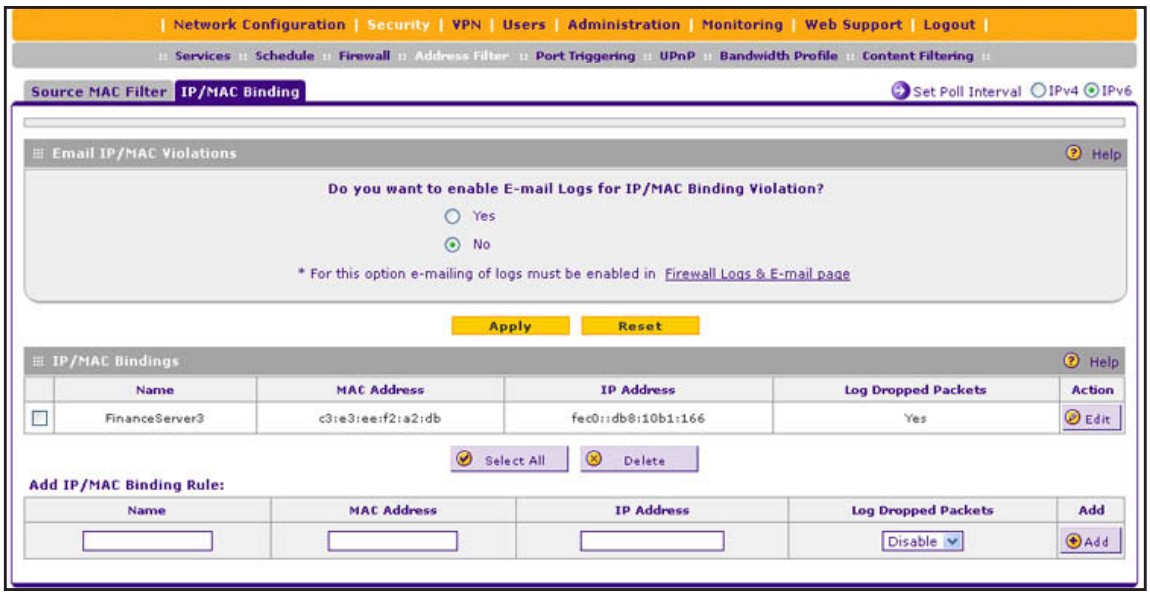

Figure 118.

3. In the Email IP/MAC Violations section of the screen, specify if you want to enable email logs for IP/MAC binding violations. (You have to do this only once.) Select one of the following radio buttons:
   - **Yes**. IP/MAC binding violations are emailed. Click the **Firewall Logs & E-mail page** link to ensure that emailing of logs is enabled on the Firewall Logs & E-mail screen (see *Configure Logging, Alerts, and Event Notifications* on page 362).
   - **No**. IP/MAC binding violations are not emailed.
4. Click **Apply** to save your changes.
5. In the IP/MAC Bindings sections of the screen, enter the settings as described in the following table:

Table 41. IP/MAC Binding screen settings for IPv6

Setting	Description
Name	A descriptive name of the binding for identification and management purposes.
MAC Address	The MAC address of the computer or device that is bound to the IP address.

Table 41. IP/MAC Binding screen settings for IPv6 (continued)

Setting	Description
IP Address	The IPv6 address of the computer or device that is bound to the MAC address.
Log Dropped Packets	To log the dropped packets, select **Enable** from the drop-down list. The default setting is Disable.

6. Click the **Add** table button. The new IP/MAC rule is added to the IP/MAC Bindings table.

➢ **To edit an IP/MAC binding:**

1. In the IP/MAC Bindings table, click the **Edit** table button to the right of the IP/MAC binding that you want to edit. The Edit IP/MAC Binding screen displays.
2. Modify the settings that you wish to change (see the previous table; you can change the MAC address, IPv6 address, and logging status).
3. Click **Apply** to save your changes. The modified IP/MAC binding displays in the IP/MAC Bindings table.

➢ **To remove one or more IP/MAC bindings from the table:**

1. Select the check box to the left of each IP/MAC binding that you want to delete, or click the **Select All** table button to select all bindings.
2. Click the **Delete** table button.

➢ **To change the IPv6 MAC polling interval from its default setting of 10 seconds:**

1. On the IP/MAC Bindings screen for IPv6, to the right of the IP/MAC Binding tab, click the **Set Poll Interval** option arrow. The IP MAC Binding Poll Interval (IPv6) pop-up screen displays:

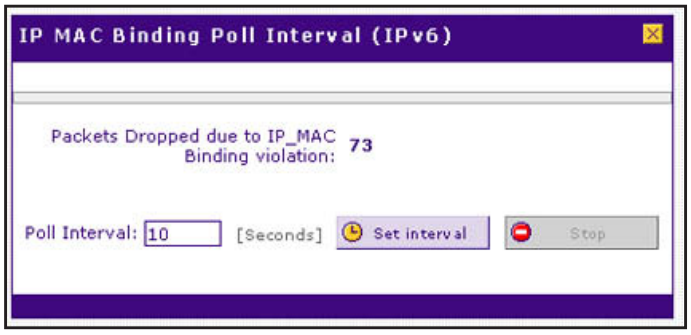

Figure 119.

2. Click the **Stop** button. Wait until the Poll Interval field becomes available.
3. Enter new poll interval in seconds.
4. Click the **Set Interval** button. Wait for the confirmation that the operation has succeeded before you close the window.

Configure Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port triggering feature requires that you know the port numbers used by the application.

Note: Port triggering is supported for IPv4 devices only.

Once configured, port triggering operates as follows:

1. A computer makes an outgoing connection using a port number that is defined in the Port Triggering Rules table.
2. The VPN firewall 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 computer.
3. The remote system receives the computer's request and responds using the incoming port or ports that are associated with the rule in the port triggering table on the VPN firewall.
4. The VPN firewall matches the response to the previous request and forwards the response to the computer.

Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a request from the LAN network. As such, it would be handled in accordance with the inbound port forwarding rules, and most likely would be blocked.

Note these restrictions on port triggering:

- Only one computer can use a port triggering application at any time.
- After a computer has finished using a port triggering application, there is a short time-out period before the application can be used by another computer. This time-out period is required so the VPN firewall can determine that the application has terminated.

Note: For additional ways of allowing inbound traffic, see *Inbound Rules (Port Forwarding)* on page 140.

➢ **To add a port triggering rule:**

1. Select **Security > Port Triggering**. The Port Triggering screen displays. (The following figure shows a rule in the Port Triggering Rules table as an example.)

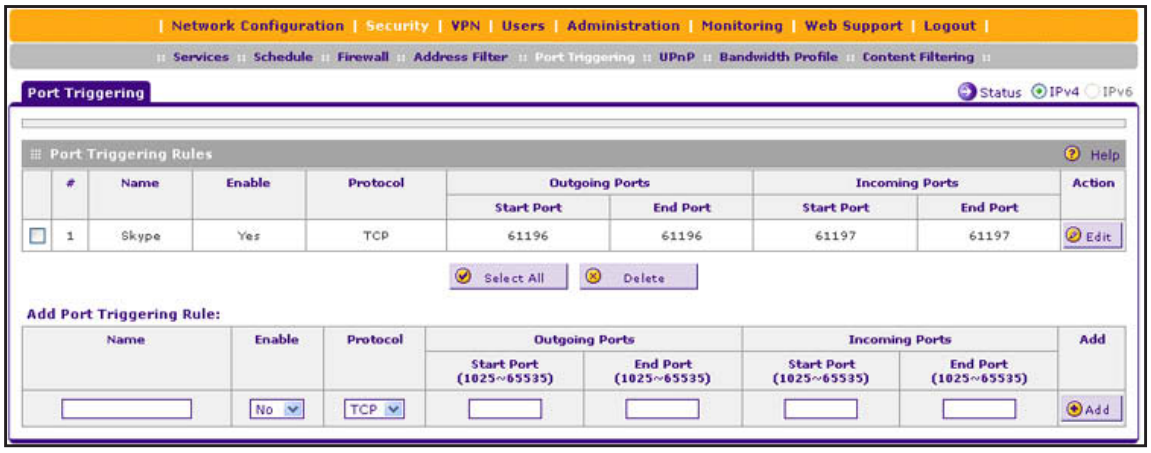

Figure 120.

2. In the Add Port Triggering Rule section, enter the settings as described in the following table:

Table 42. Port Triggering screen settings

Setting	Description	
Name	A descriptive name of the rule for identification and management purposes.	
Enable	From the drop-down list, select **Yes** to enable the rule. (You can define a rule but not enable it.) The default setting is No.	
Protocol	From the drop-down list, select the protocol to which the rule applies: • **TCP**. The rule applies to an application that uses the Transmission Control Protocol (TCP). • **UDP**. The rule applies to an application that uses the User Datagram Protocol (UDP).	
Outgoing Ports	Start Port	The start port (1025–65535) of the range for triggering.
	End Port	The end port (1025–65535) of the range for triggering.
Incoming Ports	Start Port	The start port (1025–65535) of the range for responding.
	End Port	The end port (1025–65535) of the range for responding.

3. Click the **Add** table button. The new port triggering rule is added to the Port Triggering Rules table.

➢ **To edit a port triggering rule:**

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

- **To remove one or more port triggering rules from the table:**

  1. Select the check box to the left of each port triggering rule that you want to delete, or click the **Select All** table button to select all rules.
  2. Click the **Delete** table button.

- **To display the status of the port triggering rules:**

  Click the **Status** option arrow in the upper right of the Port Triggering screen. A pop-up screen displays, showing the status of the port triggering rules.

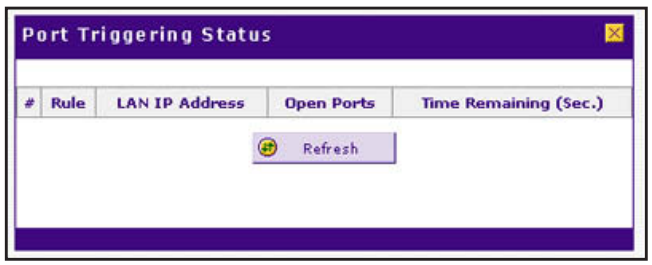

Figure 121.

Configure Universal Plug and Play

The Universal Plug and Play (UPnP) feature enables the VPN firewall to automatically discover and configure devices when it searches the LAN and WAN.

Note: UPnP is supported for IPv4 devices only.

- **To configure UPnP:**

  1. Select **Security > UPnP**. The UPnP screen displays:

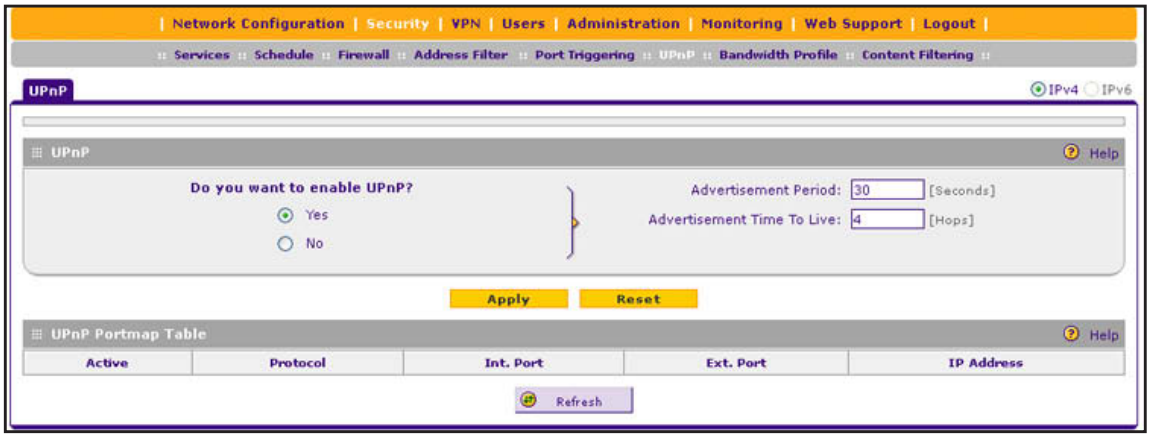

Figure 122.

The UPnP Portmap Table in the lower part of the screen shows the IP addresses and other settings of UPnP devices that have accessed the VPN firewall and that have been automatically detected by the VPN firewall:

- **Active**. A Yes or No indicates if the UPnP device port that established a connection is active.
- **Protocol**. Indicates the network protocol such as HTTP or FTP that is used by the device to connect to the VPN firewall.
- **Int. Port**. Indicates if any internal ports are opened by the UPnP device.
- **Ext. Port**. Indicates if any external ports are opened by the UPnP device.
- **IP Address**. Lists the IP address of the UPnP device accessing the VPN firewall.

2. To enable the UPnP feature, select the **Yes** radio button. (The feature is disabled by default.) To disable the feature, select **No**.
3. Fill in the following fields:
   - **Advertisement Period**. Enter the period in seconds that specifies how often the VPN firewall should broadcast its UPnP information to all devices within its range. The default setting is 30 seconds.
   - **Advertisement Time to Live**. Enter a number that specifies how many steps (hops) each UPnP packet is allowed to propagate before being discarded. Small values limit the UPnP broadcast range. The default setting is four hops.
4. Click **Apply** to save your settings.

To refresh the contents of the UPnP Portmap Table, click **Refresh**.

Virtual Private Networking Using IPSec and L2TP Connections

5

This chapter describes how to use the IP security (IPSec) virtual private networking (VPN) features of the VPN firewall to provide secure, encrypted communications between your local network and a remote network or computer. The chapter contains the following sections:

Considerations for Dual WAN Port Systems

If two WAN ports are configured for either IPv4 or IPv6, you can enable either auto-rollover mode for increased system reliability or load balancing mode for optimum bandwidth efficiency. The selection of the WAN mode determines how you need to configure the VPN features.

The use of fully qualified domain names (FQDNs) in VPN policies is mandatory when the WAN ports function in auto-rollover mode or load balancing mode, and is also required for VPN tunnel failover. When the WAN ports function in load balancing mode, you cannot configure VPN tunnel failover. An FQDN is optional when the WAN ports function in load balancing mode if the IP addresses are static, but mandatory if the WAN IP addresses are dynamic.

See *Virtual Private Networks* on page 421 for more information about the IP addressing requirements for VPNs in the dual WAN modes.

For information about how to select and configure a Dynamic DNS service for resolving FQDNs, see *Configure Dynamic DNS* on page 49. For information about WAN mode configuration, see *Configure the IPv4 WAN Mode* on page 29.

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

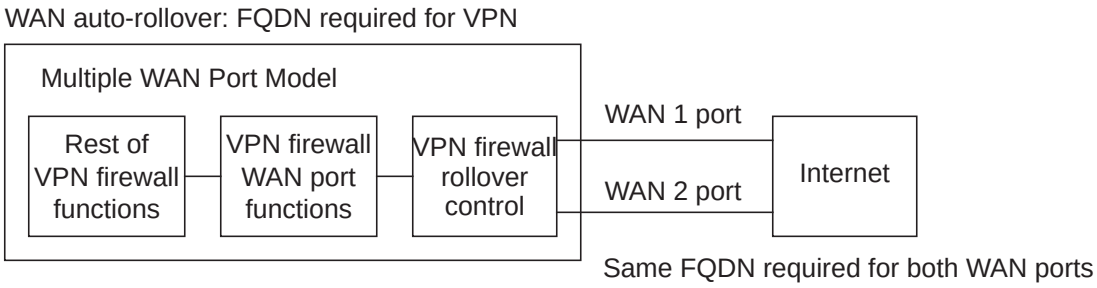

Figure 123.

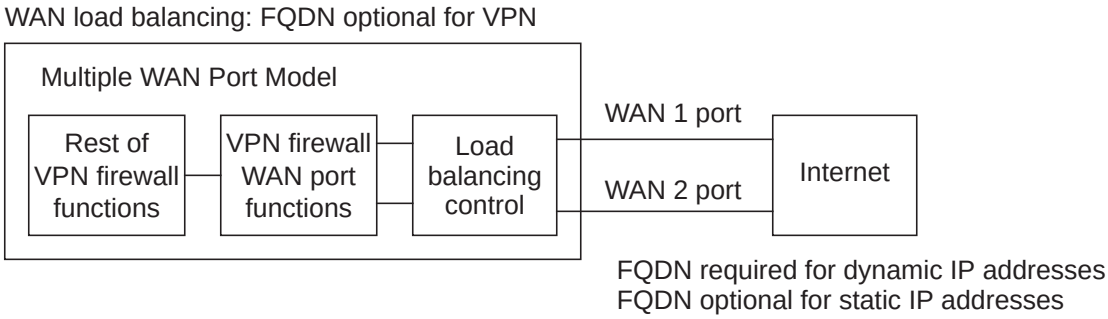

Figure 124.

The following table summarizes the WAN addressing requirements (FQDN or IP address) for a VPN tunnel in either dual WAN mode.

Table 43. 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
VPN Gateway-to-Gateway (gateway to gateway)	Fixed	FQDN required	FQDN Allowed (optional)
	Dynamic	FQDN required	FQDN required
VPN Telecommuter (client to gateway through a NAT router)	Fixed	FQDN required	FQDN Allowed (optional)
	Dynamic	FQDN required	FQDN required

a. After a rollover, all tunnels need to be reestablished using the new WAN IP address.

Use the IPSec VPN Wizard for Client and Gateway Configurations

You can use the IPSec VPN Wizard to configure multiple gateway or client VPN tunnel policies.

The following sections provide wizard and NETGEAR ProSafe VPN Client software configuration procedures:

- *Create an IPv4 Gateway-to-Gateway VPN Tunnel with the Wizard* on page 204
- *Create an IPv6 Gateway-to-Gateway VPN Tunnel with the Wizard* on page 208
- *Create an IPv4 Client-to-Gateway VPN Tunnel with the Wizard* on page 212

Note: Although the VPN firewall supports IPv6, the NETGEAR ProSafe VPN Client supports IPv4 only; a future release of the VPN Client might support IPv6.

Configuring a VPN tunnel connection requires that you specify all settings on both sides of the VPN tunnel to match or mirror each other precisely, which can be a daunting task. The VPN Wizard efficiently guides you through the setup procedure with a series of questions that determine the IPSec keys and VPN policies it sets up. The VPN Wizard also configures the settings for the network connection: security association (SA), traffic selectors, authentication algorithm, and encryption. The settings that the VPN Wizard uses are based on the recommendations of the VPN Consortium (VPNC), an organization that promotes multivendor VPN interoperability.

Create an IPv4 Gateway-to-Gateway VPN Tunnel with the Wizard

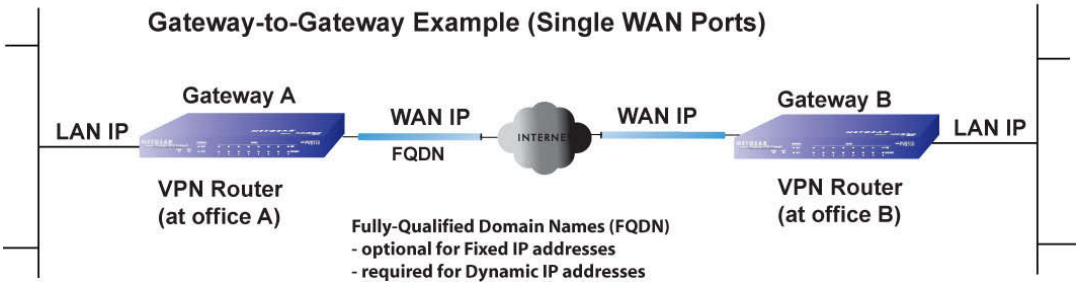

Figure 125.

➢ **To set up an IPv4 gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. In the upper right of the screen, the IPv4 radio button is selected by default. The VPN Wizard screen displays the IPv4 settings. (The following screen contains some examples that do not relate to other examples in this manual.)

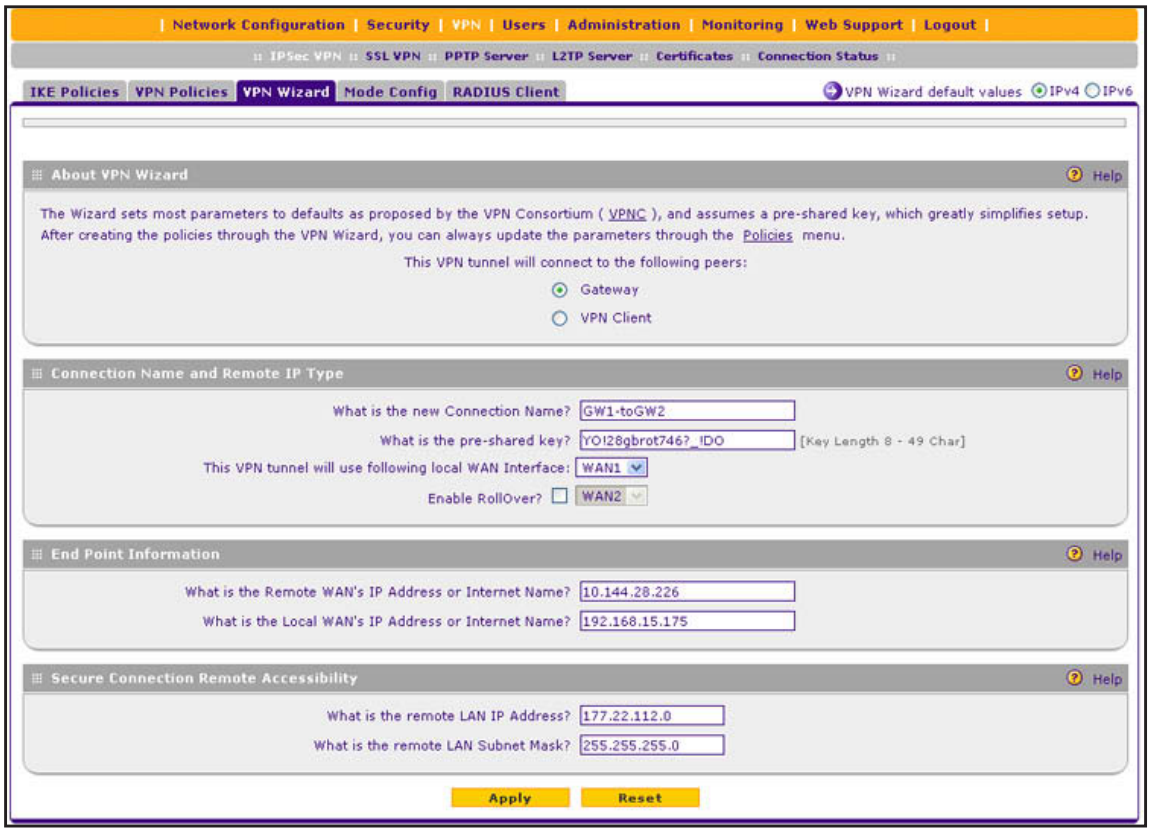

Figure 126.

To view the wizard default settings, click the **VPN Wizard default values** option arrow in the upper right of the screen. A pop-up screen displays (see the following figure), showing the wizard default values. The default values are the same for IPv4 and IPv6.

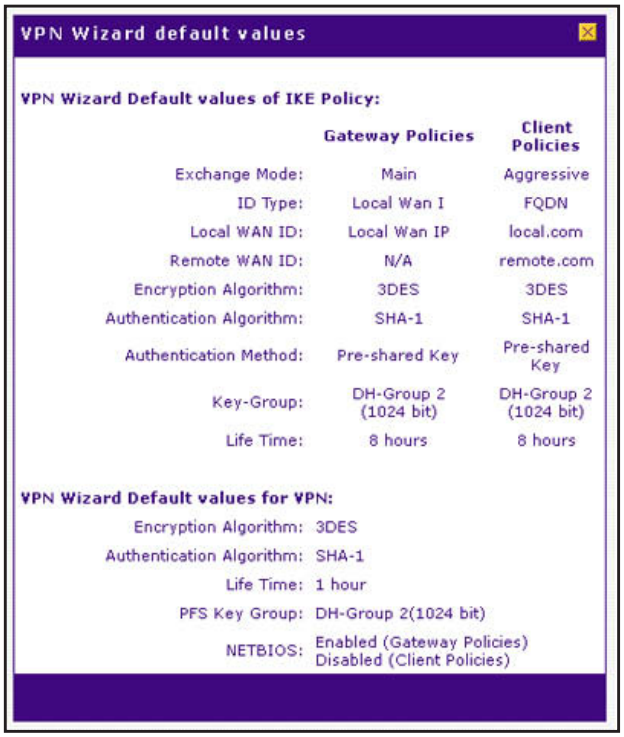

Figure 127.

2. Complete the settings as described in the following table:

Table 44. IPSec VPN Wizard settings for an IPv4 gateway-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **Gateway** radio button. The local WAN port's IP address or Internet name displays in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.

Table 44. IPSec VPN Wizard settings for an IPv4 gateway-to-gateway tunnel (continued)

Setting	Description
This VPN tunnel will use the following local WAN Interface	Select a WAN interface from the drop-down list to specify which local WAN interface the VPN tunnel uses as the local endpoint.
	(Optional) Select the **Enable RollOver?** check box to enable VPN rollover, and select a WAN interface from the drop-down list to the right of the check box to specify the interface to which the VPN rollover should occur. **Note:** If the VPN firewall is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure this manually.
End Point Information[a]	
What is the Remote WAN's IP Address or Internet Name?	Enter the IPv4 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 IPv4 address of the VPN firewall's active WAN interface is automatically entered.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	Enter the LAN IPv4 address of the remote gateway. **Note:** The remote LAN IPv4 address needs to be in a different subnet from the local LAN IP address. For example, if the local subnet is 192.168.1.x, the remote subnet could be 192.168.10.x but could not be 192.168.1.x. If this information is incorrect, the tunnel fails to connect.
What is the remote LAN Subnet Mask?	Enter the LAN subnet mask for 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 an FQDN is not supported.

Tip: To ensure that tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keep-alives, which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive. For more information, see *Configure Keep-Alives* on page 266.

Tip: For DHCP WAN configurations, first set up the tunnel with IP addresses. After you validate the connection, you can use the wizard to create new policies using the FQDN for the WAN addresses.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen for IPv4. By default, the VPN policy is enabled.

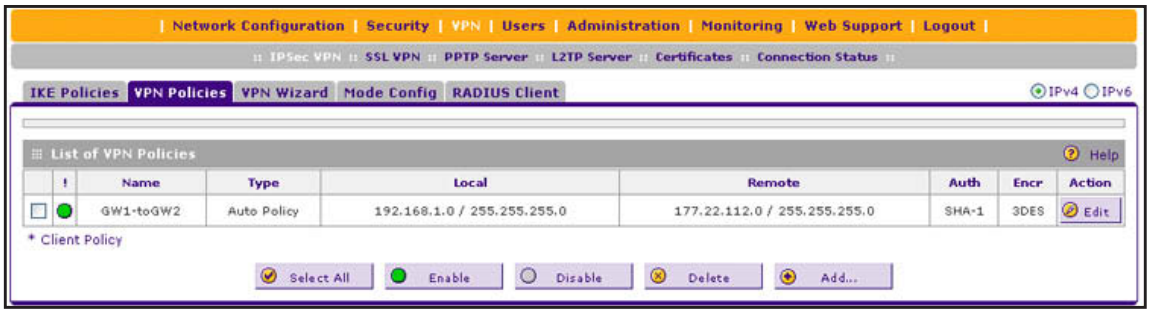

Figure 128.

4. Configure a VPN policy on the remote gateway that allows connection to the VPN firewall.
5. Activate the IPSec VPN connection:
   a. Select **VPN > Connection Status**. The Connection Status submenu tabs display with the IPSec VPN Connection Status screen in view:

Figure 129.

   b. Locate the policy in the table, and click the **Connect** table button. The IPSec VPN connection becomes active.

Note: When using FQDNs, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel fails because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

Create an IPv6 Gateway-to-Gateway VPN Tunnel with the Wizard

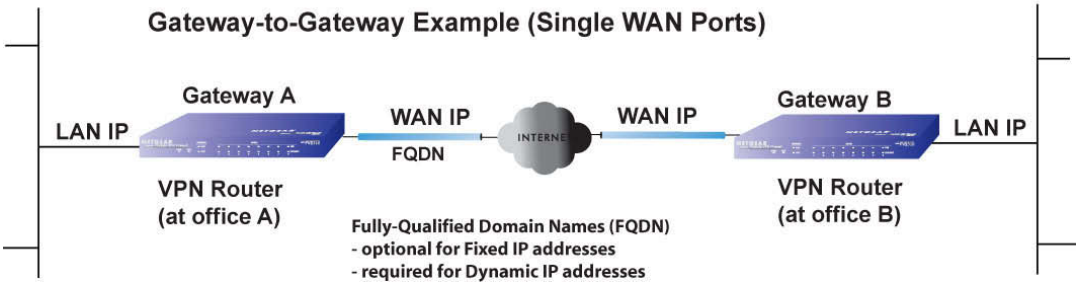

Figure 130.

➢ **To set up an IPv6 gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**.
2. In the upper right of the screen, select the **IPv6** radio button. The VPN Wizard screen displays the IPv6 settings. (The following screen contains some examples that do not relate to other examples in this manual.)

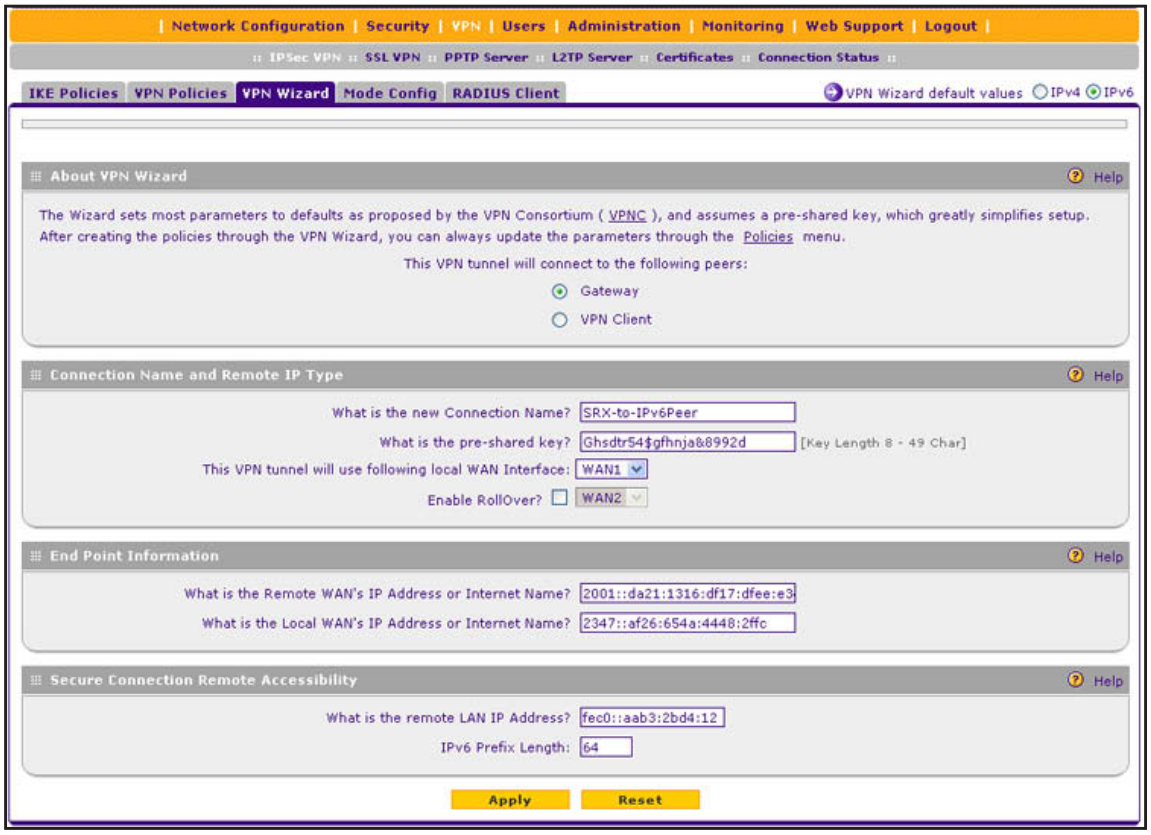

Figure 131.

To view the wizard default settings, click the **VPN Wizard default values** option arrow in the upper right of the screen. A pop-up screen displays (see the following figure), showing the wizard default values. The default values are the same for IPv4 and IPv6.

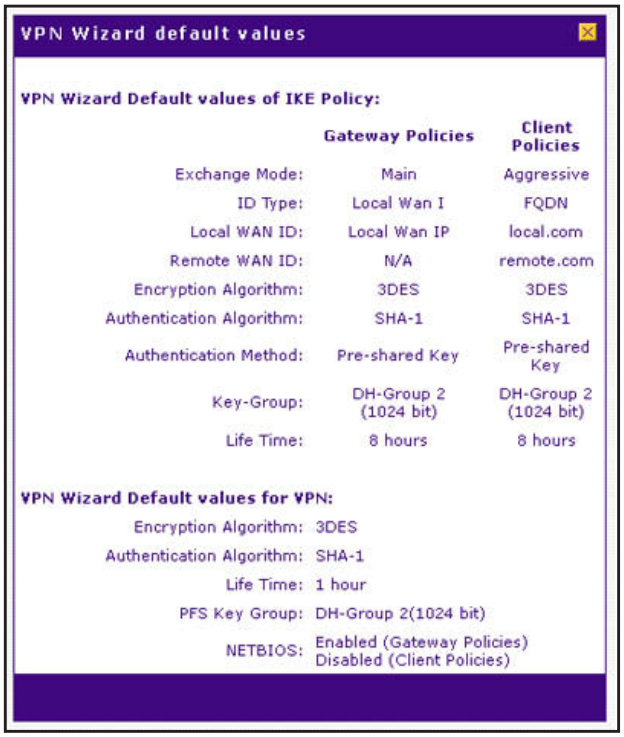

Figure 132.

3. Complete the settings as described in the following table:

Table 45. IPSec VPN Wizard settings for an IPv6 gateway-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **Gateway** radio button. The local WAN port's IP address or Internet name displays in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.

Table 45. IPSec VPN Wizard settings for an IPv6 gateway-to-gateway tunnel (continued)

Setting	Description
This VPN tunnel will use the following local WAN Interface	Select a WAN interface from the drop-down list to specify which local WAN interface the VPN tunnel uses as the local endpoint.
	(Optional) Select the **Enable RollOver?** check box to enable VPN rollover, and select a WAN interface from the drop-down list to the right of the check box to specify the interface to which the VPN rollover should occur. **Note:** If the VPN firewall is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure this manually.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.
End Point Information[a]	
What is the Remote WAN's IP Address or Internet Name?	Enter the IPv6 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 IPv6 address of the VPN firewall's active WAN interface is automatically entered.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	Enter the LAN IPv6 address of the remote gateway. **Note:** The remote LAN IPv6 address needs to be different from the local LAN IPv6 address. For example, if the local LAN IPv6 address is fec0::1, the remote LAN IPv6 address could be fec0:1::1 but could not be fec0::1. If this information is incorrect, the tunnel fails to connect.
IPv6 Prefix Length	Enter the prefix length for 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 an FQDN is not supported.

Tip: To ensure that tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keep-alives, which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive. For more information, see *Configure Keep-Alives* on page 266.

Tip: For DHCP WAN configurations, first set up the tunnel with IP addresses. After you validate 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 for IPv6. By default, the VPN policy is enabled.

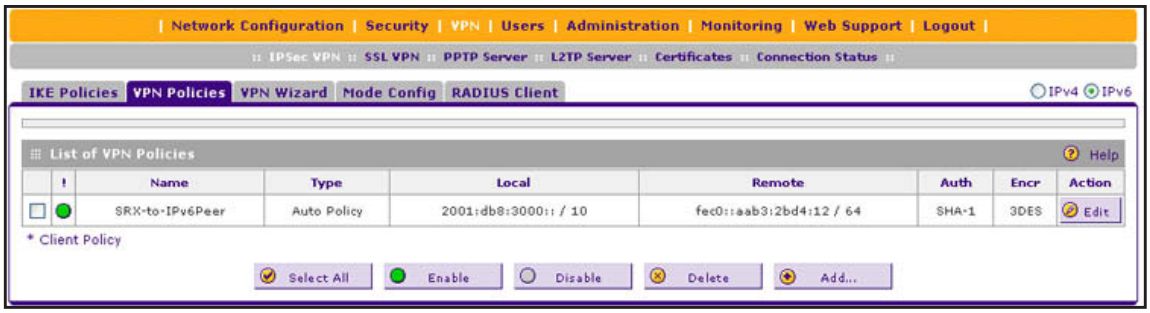

Figure 133.

5. Configure a VPN policy on the remote gateway that allows connection to the VPN firewall.
6. Activate the IPSec VPN connection:
   a. Select **VPN > Connection Status**. The Connection Status submenu tabs display with the IPSec VPN Connection Status screen in view:

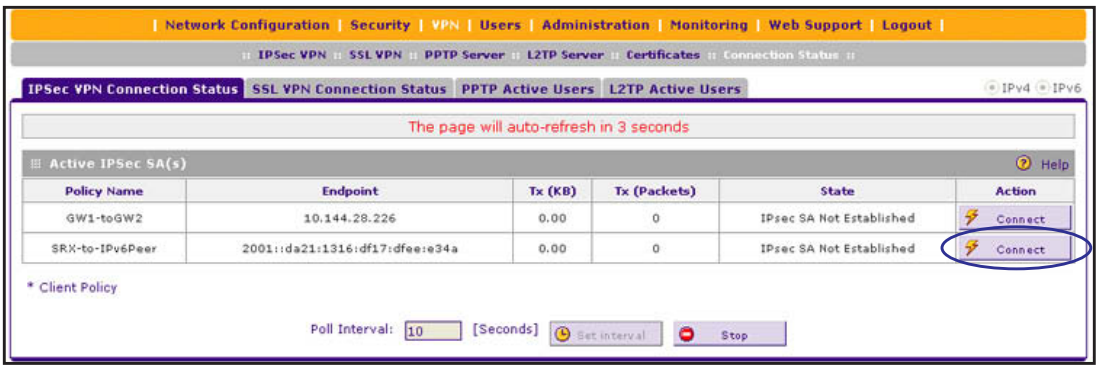

Figure 134.

   b. Locate the policy in the table, and click the **Connect** table button. The IPSec VPN connection becomes active.

Note: When using FQDNs, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel fails because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

Create an IPv4 Client-to-Gateway VPN Tunnel with the Wizard

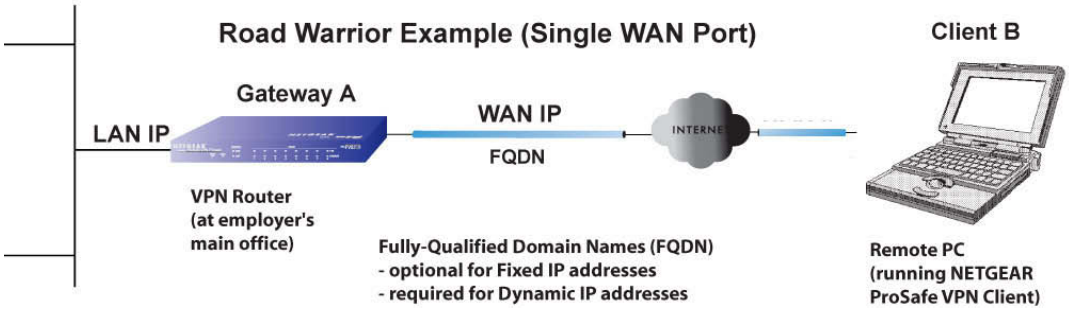

Figure 135.

To configure a VPN client tunnel, follow the steps in the following sections:

- *Use the VPN Wizard to Configure the Gateway for a Client Tunnel* on page 212.
- *Use the NETGEAR VPN Client Wizard to Create a Secure Connection* on page 215 *or Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 220.

Use the VPN Wizard to Configure the Gateway for a Client Tunnel

➢ **To set up a client-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. In the upper right of the screen, the IPv4 radio button is selected by default. The VPN Wizard screen displays the IPv4 settings. (The following figure contains an example.)

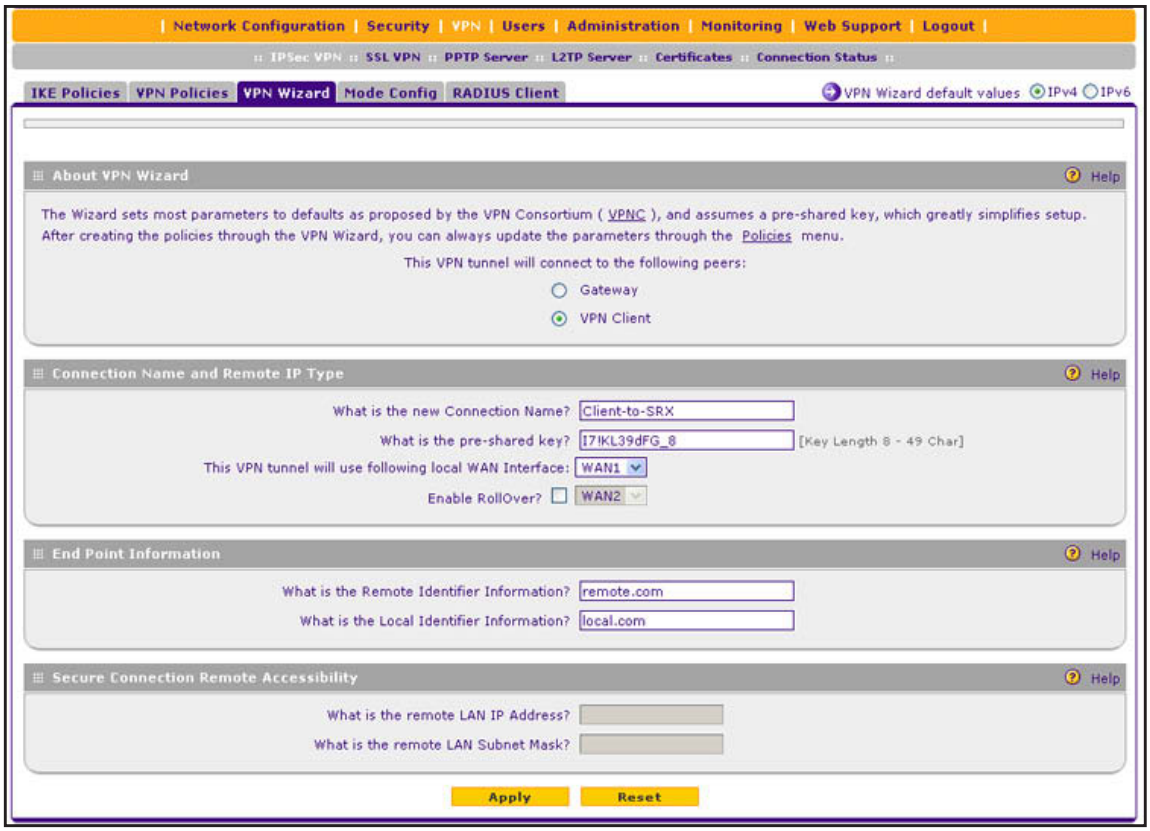

Figure 136.

To display the wizard default settings, click the **VPN Wizard default values** option arrow in the upper right of the screen. A pop-up screen displays (see *Figure 127* on page 205), showing the wizard default values. After you complete the wizard, you can modify these settings for the tunnel policy that you have set up.

2. Complete the settings as described in the following table:

Table 46. IPSec VPN Wizard settings for a client-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **VPN Client** radio button. The default remote FQDN (remote.com) and the default local FQDN (local.com) display in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the VPN client.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway, or the remote VPN client. This key needs to have a minimum length of 8 characters and cannot exceed 49 characters.

Table 46. IPSec VPN Wizard settings for a client-to-gateway tunnel (continued)

Setting	Description
This VPN tunnel will use the following local WAN Interface	Select a WAN interface from the drop-down list to specify which local WAN interface the VPN tunnel uses as the local endpoint.
	Select the **Enable RollOver?** check box to enable VPN rollover, and select a WAN interface from the drop-down list to the right of the check box to specify the interface to which the VPN rollover should occur. **Note:** If the VPN firewall is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure this manually.
End Point Information[a]	
What is the Remote Identifier Information?	When you select the Client radio button in the About VPN Wizard section of the screen, the default remote FQDN (remote.com) is automatically entered. Use the default remote FQDN, or enter another FQDN. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter client.com as the local ID on the VPN client.
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 (local.com) is automatically entered. Use the default local FQDN, or enter another FQDN. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter router.com as the remote ID on the VPN client.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	These fields are masked out for VPN client connections.
What is the remote LAN Subnet Mask?	

a. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen for IPv4. By default, the VPN policy is enabled.

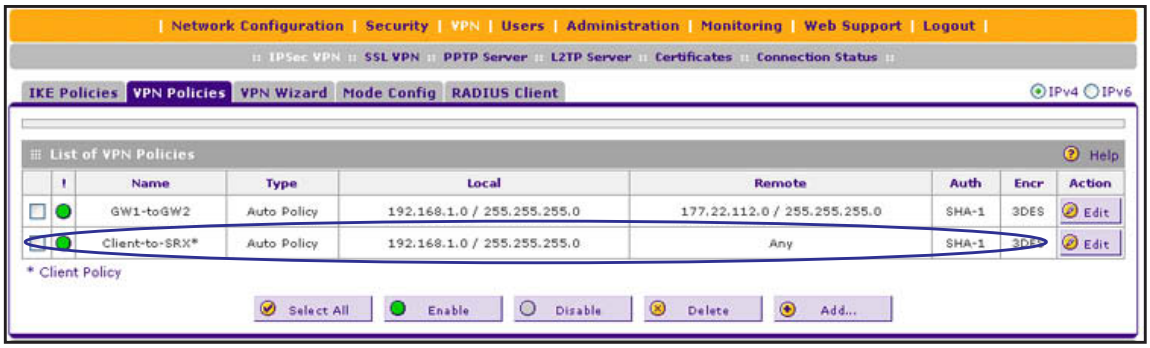

Figure 137.

Note: When you are using FQDNs, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel fails because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

4. Optional step: Collect the information that you need to configure the VPN client. You can print the following table to keep track of this information.

Table 47. Information required to configure the VPN client

Component	Enter the information that you collected	Example
Pre-shared key		I7!KL39dFG_8
Remote identifier information		remote.com
Local identifier information		local.com
Router's LAN network IPv4 address		192.168.1.0
Router's WAN IPv4 address		192.168.15.175

Use the NETGEAR VPN Client Wizard to Create a Secure Connection

The VPN client lets you set up the VPN connection manually (see *Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 220) or with the integrated Configuration Wizard, which is the easier and preferred method. The Configuration Wizard configures the default settings and provides basic interoperability so that the VPN client can easily communicate with the VPN firewall (or third-party VPN devices). The Configuration Wizard does not let you enter the local and remote IDs, so you need to manually enter this information.

Note: Perform these tasks from a computer that has the NETGEAR ProSafe VPN Client installed. The VPN Client supports IPv4 only; a future release of the VPN Client might support IPv6.

➢ **To use the Configuration Wizard to set up a VPN connection between the VPN client and the VPN firewall:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays:

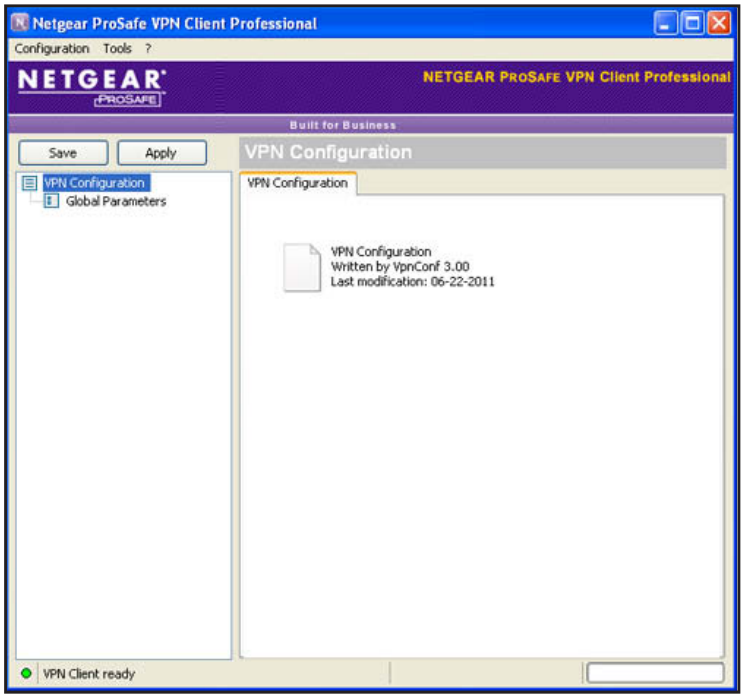

Figure 138.

2. From the main menu on the Configuration Panel screen, select **Configuration > Wizard**. The Choice of the remote equipment wizard screen (screen 1 of 3) displays:

Figure 139.

3. Select the **A router or a VPN gateway** radio button, and click **Next**. The VPN tunnel parameters wizard screen (screen 2 of 3) displays:

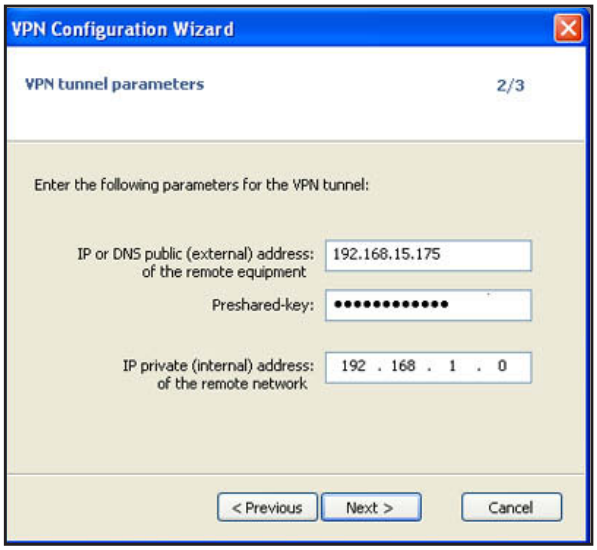

Figure 140.

4. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. Enter the remote IP address or DNS name of the VPN firewall. For example, enter **192.168.15.175**.
   - **Preshared key**. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **I7!KL39dFG_8**.
   - **IP private (internal) address of the remote network**. Enter the remote private IP address of the VPN firewall. For example, enter **192.168.1.0**. This IP address enables communication with the entire 192.168.1.x subnet.
5. Click **Next**. The Configuration Summary wizard screen (screen 3 of 3) displays:

Figure 141.

6. This screen is a summary screen of the new VPN configuration. Click **Finish**.
7. Specify the local and remote IDs:
   a. In the tree list pane of the Configuration Panel screen, click **Gateway** (the default name given to the authentication phase). The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.
   b. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays:

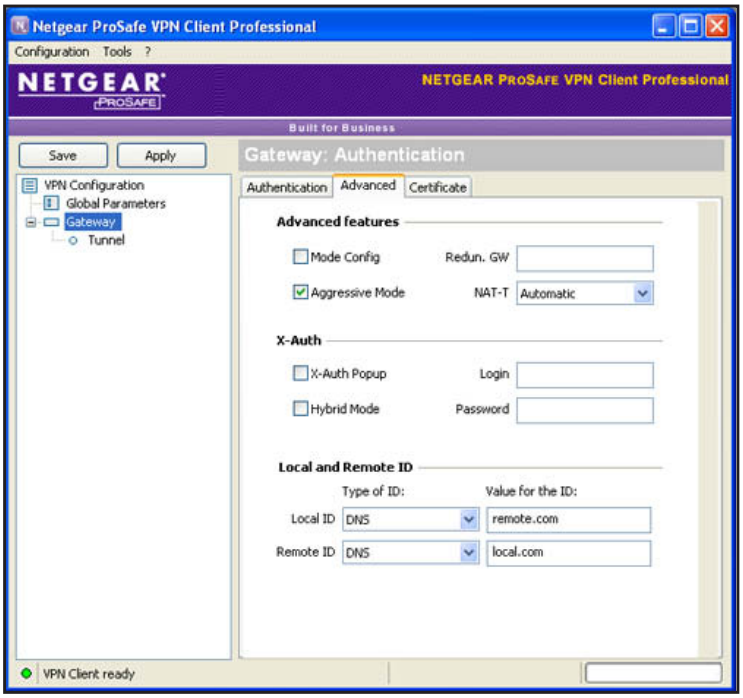

Figure 142.

c. Specify the settings that are described in the following table.

Table 48. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **remote.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter router.com as the remote ID on the VPN client.

8. Configure the global parameters:

   a. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen:

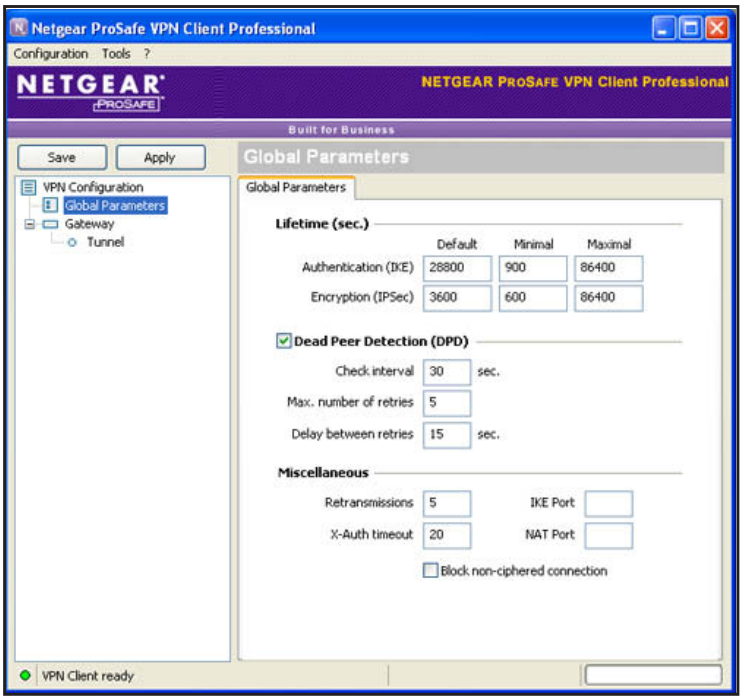

Figure 143.

b. Specify the default lifetimes in seconds:

- **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the VPN firewall.
- **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the VPN firewall.

9. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN client configuration is now complete.

Instead of using the wizard on the VPN client, you can also manually configure the VPN client, which is described in the following section.

Manually Create a Secure Connection Using the NETGEAR VPN Client

Note: Perform these tasks from a computer that has the NETGEAR ProSafe VPN Client installed.

To manually configure a VPN connection between the VPN client and the VPN firewall, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and specify the global parameters.

Configure the Authentication Settings (Phase 1 Settings)

➢ **To create new authentication settings:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays:

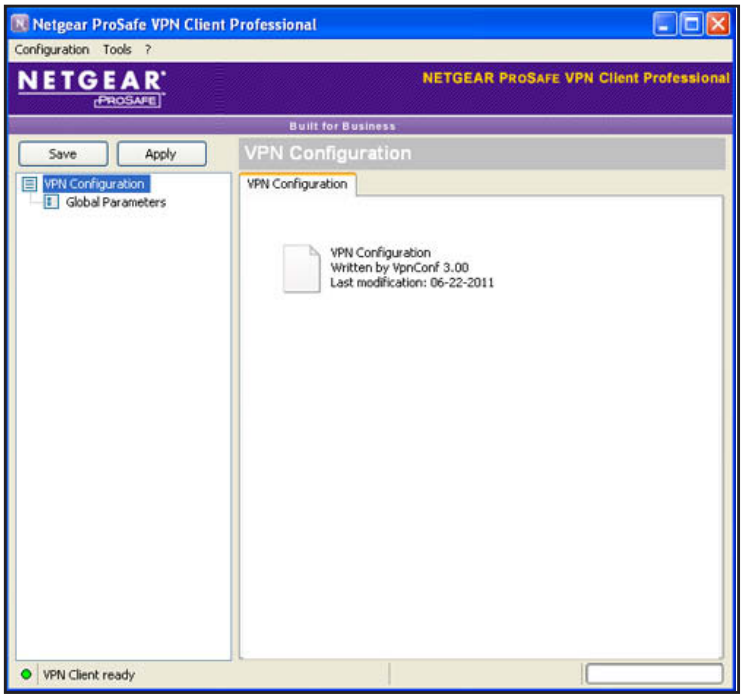

Figure 144.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.

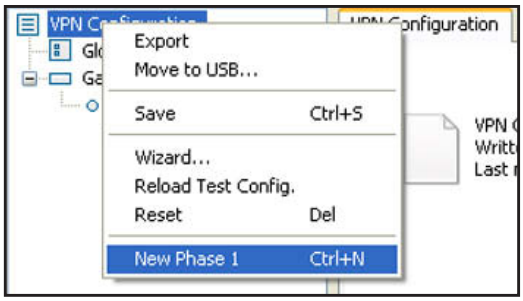

Figure 145.

3. Change the name of the authentication phase (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Type **vpn_client**.
   d. Click anywhere in the tree list pane.

Note: *This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

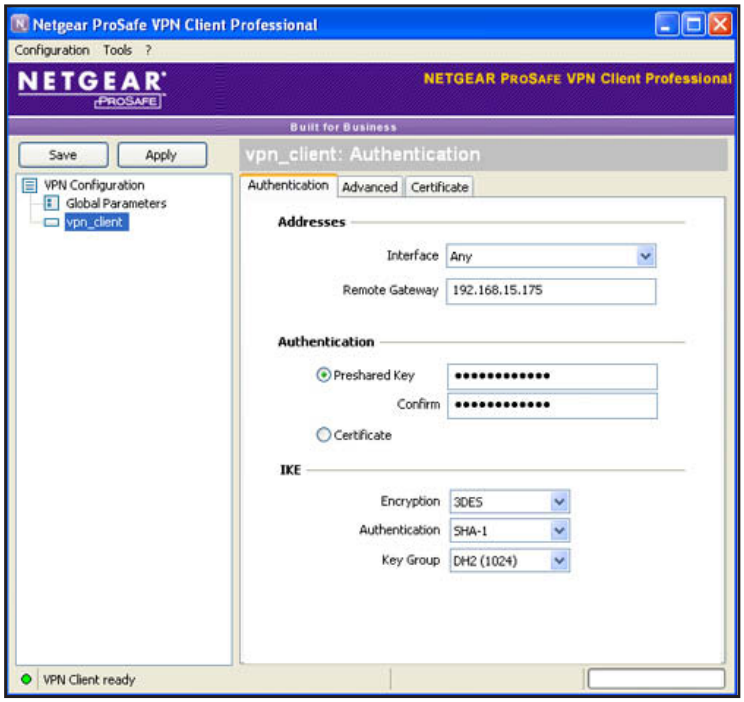

Figure 146.

4. Specify the settings that are described in the following table.

Table 49. VPN client authentication settings

Setting	Description	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the VPN firewall. For example, enter **192.168.15.175**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **I7!KL39dFG_8**. Confirm the key in the Confirm field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.
6. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays:

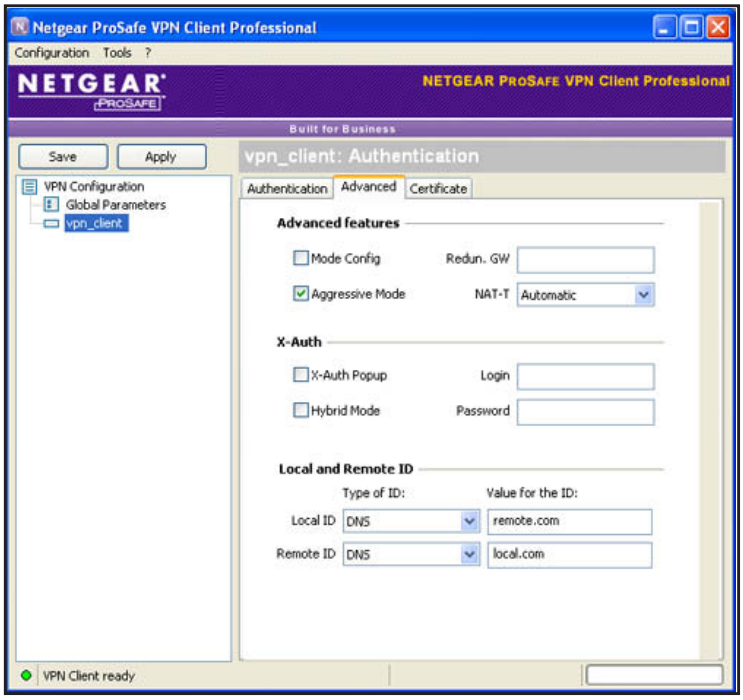

Figure 147.

7. Specify the settings that are described in the following table.

Table 50. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and VPN firewall to negotiate NAT-T.

Table 50. VPN client advanced authentication settings (continued)

Setting	Description
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **remote.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter router.com as the remote ID on the VPN client.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the IPSec Configuration (Phase 2 Settings)

Note: On the VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **vpn_client** authentication phase name, and select **New Phase 2**.
2. Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Type **netgear_platform**.
   d. Click anywhere in the tree list pane.

   Note: *This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

   The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default:

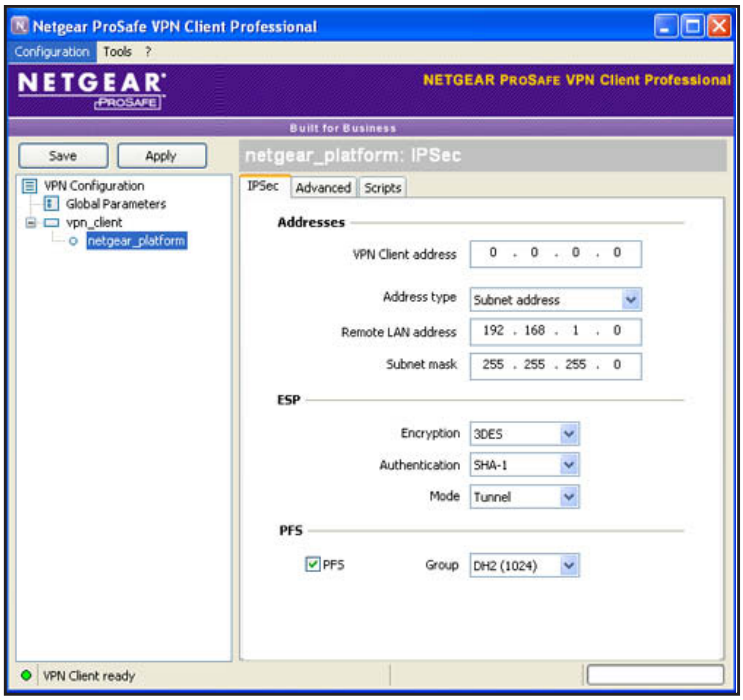

Figure 148.

3. Specify the settings that are described in the following table.

Table 51. VPN client IPSec configuration settings

Setting	Description	
VPN Client address	Either enter **0.0.0.0** as the IP address, or enter a virtual IP address that the VPN client uses in the VPN firewall's LAN; the computer (for which the VPN client opened a tunnel) appears in the LAN with this IP address.	
Address Type	Select **Subnet address** from the drop-down list. This selection defines which addresses the VPN client can communicate with after the VPN tunnel is established.	
Remote LAN address	Enter **192.168.1.0** as the remote IP address (that is, LAN network address) of the gateway that opens the VPN tunnel.	
Subnet mask	Enter **255.255.255.0** as the remote subnet mask of the gateway that opens the VPN tunnel.	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and select the **DH2 (1024)** key group from the drop-down list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure the Global Parameters

➢ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen:

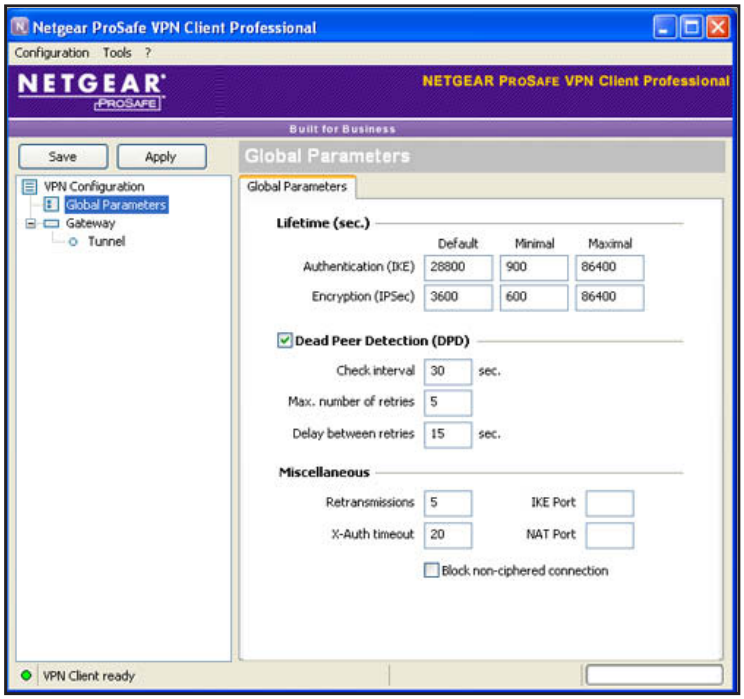

Figure 149.

2. Specify the default lifetimes in seconds:
   - **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the VPN firewall.
   - **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the VPN firewall.
3. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN firewall configuration is now complete.

Test the Connection and View Connection and Status Information

Both the NETGEAR ProSafe VPN Client and the VPN firewall provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a connection.

Test the NETGEAR VPN Client Connection

There are many ways to establish a connection. The following procedures assume that you use the default authentication phase name *Gateway* and the default IPSec configuration name *Tunnel*. If you manually set up the connection and changed the names, use *vpn_client* (or any other name that you have configured) as the authentication phase name and *netgear_platform* (or any other name that you have configured) as the IPSec configuration name.

➢ **To establish a connection, use one of the following three methods:**

- **Use the Configuration Panel screen**. In the tree list pane of the Configuration Panel screen, perform *one* of the following tasks:
  - Click the **Tunnel** IPSec configuration name, and press **Ctrl+O.**
  - Right-click the **Tunnel** IPSec configuration name, and select **Open tunnel**.

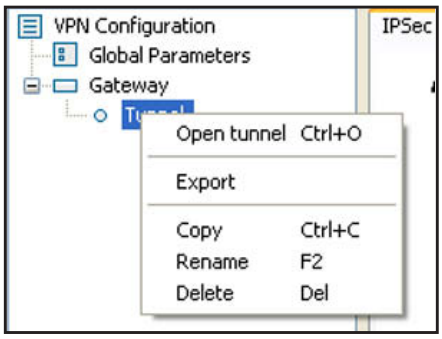

Figure 150.

- **Use the Connection Panel screen**. On the main menu of the Configuration Panel screen, select **Tools > Connection Panel** to open the Connection Panel screen. Perform *one* of the following tasks:
  - Double-click **Gateway-Tunnel**.
  - Right-click **Gateway-Tunnel**, and select **Open tunnel**.
  - Click **Gateway-Tunnel**, and press **Ctrl+O**.

Figure 151.

- **Use the system-tray icon**. Right-click the system tray icon, and select **Open tunnel 'Tunnel'**.

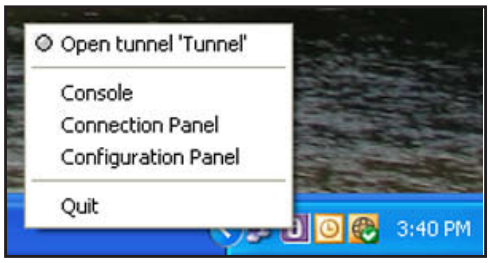

Figure 152.

Whichever way you choose to open the tunnel, when the tunnel opens successfully, the *Tunnel opened* message displays above the system tray:

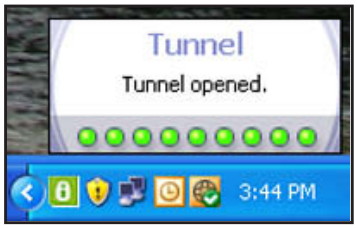

Figure 153.

After the VPN client is launched, it displays an icon in the system tray that indicates whether a tunnel is opened, using a color code:

Green icon:
at least one VPN tunnel opened

Purple icon:
no VPN tunnel opened

Figure 154.

NETGEAR VPN Client Status and Log Information

➢ **To view detailed negotiation and error information on the NETGEAR VPN client:**

Right-click the VPN client icon in the system tray, and select **Console**. The VPN Client Console Active screen displays:

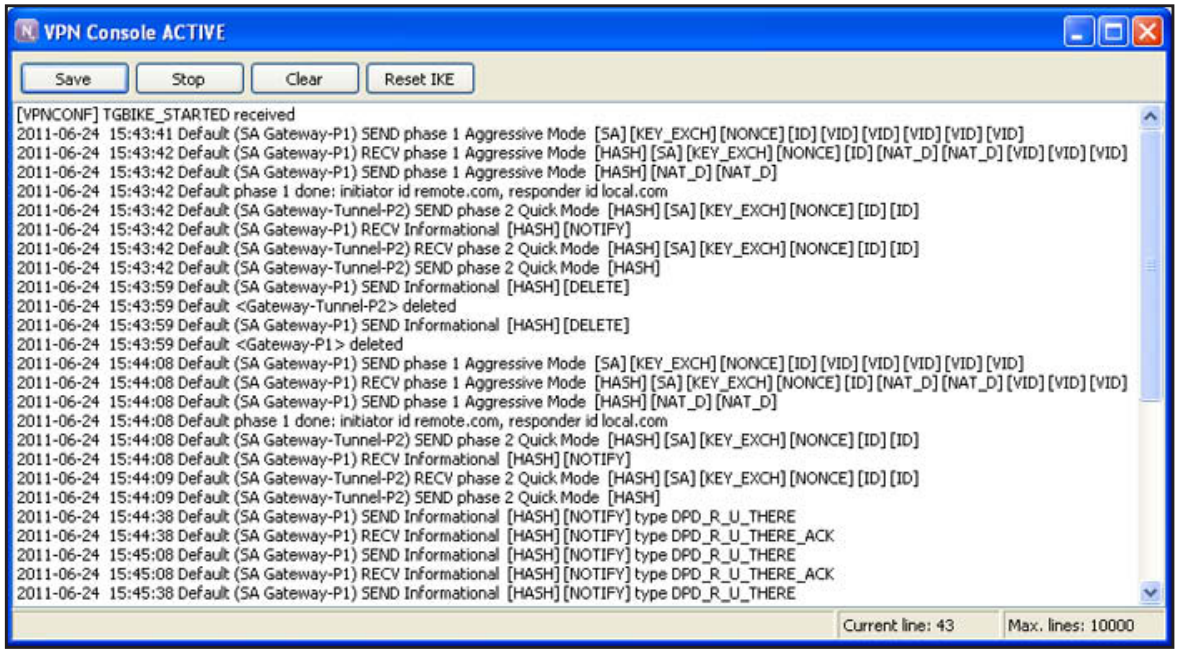

Figure 155.

View the VPN Firewall IPSec VPN Connection Status

To view the status of current IPSec VPN tunnels, select **VPN > Connection Status**. The Connection Status submenu tabs display with the IPSec VPN Connection Status screen in view. (The following figure shows an IPSec SA as an example.)

Figure 156.

The Active IPSec SA(s) table lists each active connection with the information that is described in the following table. The default poll interval is 10 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and click the **Set Interval** button. To stop polling, click the **Stop** button.

Table 52. IPSec VPN Connection Status screen information

Item	Description
Policy Name	The name of the VPN policy that is associated with this SA.
Endpoint	The IP address on the remote VPN endpoint.
Tx (KB)	The amount of data that is transmitted over this SA.
Tx (Packets)	The number of IP packets that are transmitted over this SA.
State	The status of the SA. Phase 1 is the authentication phase, and Phase 2 is key exchange phase. If there is no connection, the status is IPSec SA Not Established.
Action	Click the **Connect** table button to build the connection, or click the **Disconnect** table button to terminate the connection.

View the VPN Firewall IPSec VPN Log

➢ **To display the IPSec VPN log:**

Select **Monitoring > VPN Logs > IPSec VPN Logs.** The IPSec VPN Logs screen displays:

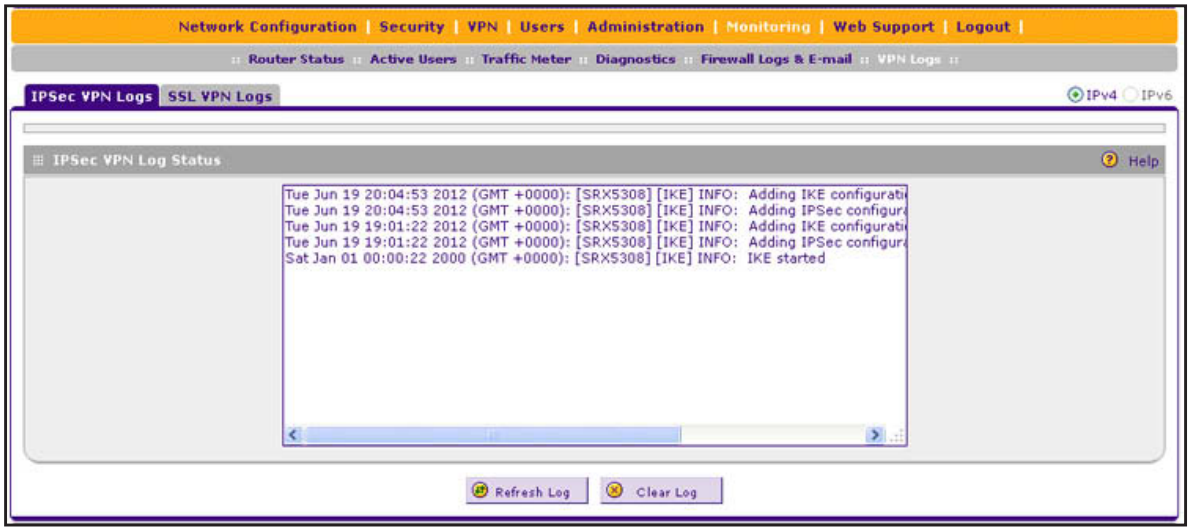

Figure 157.

Manage IPSec VPN Policies

After you have used the VPN Wizard to set up a VPN tunnel, a VPN policy and an IKE policy are stored in separate policy tables. The name that you selected as the VPN tunnel connection name during the VPN Wizard setup identifies both the VPN policy and IKE policy. You can edit existing policies, or manually add new VPN and IKE policies directly in the policy tables.

Manage IKE Policies

The Internet Key Exchange (IKE) protocol performs negotiations between the two VPN gateways and provides automatic management of the keys that are used for IPSec connections. It is important to remember that:

- An automatically generated VPN policy (auto policy) needs to use the IKE negotiation protocol.
- A manually generated VPN policy (manual policy) cannot use the IKE negotiation protocol.

IKE policies are activated when the following situations occur:

1. The VPN policy selector determines that some traffic matches an existing VPN policy of an auto policy type.
2. The IKE policy that is specified in the Auto Policy Parameters section of the Add VPN Policy screen (see *Figure 161* on page 240) for the VPN policy is used to start negotiations with the remote VPN gateway.
3. An IKE session is established, using the security association (SA) settings that are specified in a matching IKE policy:
   - Keys and other settings are exchanged.
   - An IPSec SA is established, using the settings that are specified in the VPN policy.

The VPN tunnel is then available for data transfer.

When you use the VPN Wizard to set up a VPN tunnel, an IKE policy is established and populated in the List of IKE Policies, and is given the same name as the new VPN connection name. You can also edit exiting policies or add new IKE policies from the IKE Policies screen.

IKE Policies Screen

➢ **To access the IKE Policies screen:**

Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view. In the upper right of the screen, the IPv4 radio button is selected by default. The IKE Policies screen displays the IPv4 settings. (The following figure shows some examples.) To display the IPv6 settings on the IKE Policies screen, select the **IPv6** radio button.

Figure 158.

Each policy contains the data that are described in the following table. These fields are described in more detail in *Table 54* on page 234.

Table 53. IKE Policies screen information for IPv4 and IPv6

Item	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 VPN firewall. The remote endpoint needs to have this value as its remote ID.
Remote ID	The IKE/ISAKMP identifier of the remote endpoint, which needs to have this value as its local ID.
Encr	The encryption algorithm that is used for the IKE security association (SA). This setting needs to match the setting on the remote endpoint.
Auth	The authentication algorithm that is used for the IKE SA. This setting needs to match the setting on the remote endpoint.
DH	The Diffie-Hellman (DH) group that is used when keys are exchanged. This setting needs to match the setting on the remote endpoint.

➢ **To delete one or more IKE polices:**

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

For information about how to add or edit an IKE policy, see *Manually Add or Edit an IKE Policy* on page 233.

Note: You cannot delete or edit an IKE policy for which the VPN policy is active without first disabling or deleting the VPN policy.

Manually Add or Edit an IKE Policy

➢ **To manually add an IKE policy for IPv4 or IPv6:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view (see *Figure 158* on page 232).
2. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays the IPv4 settings (see the next figure).
3. Specify the IP version for which you want to add an IKE policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 4*.
   - **IPv6**. Select the **IPv6** radio button. The Add IKE Policy screen for IPv6 displays. This screen is identical to the Add IKE Policy screen for IPv4 (see the next figure).

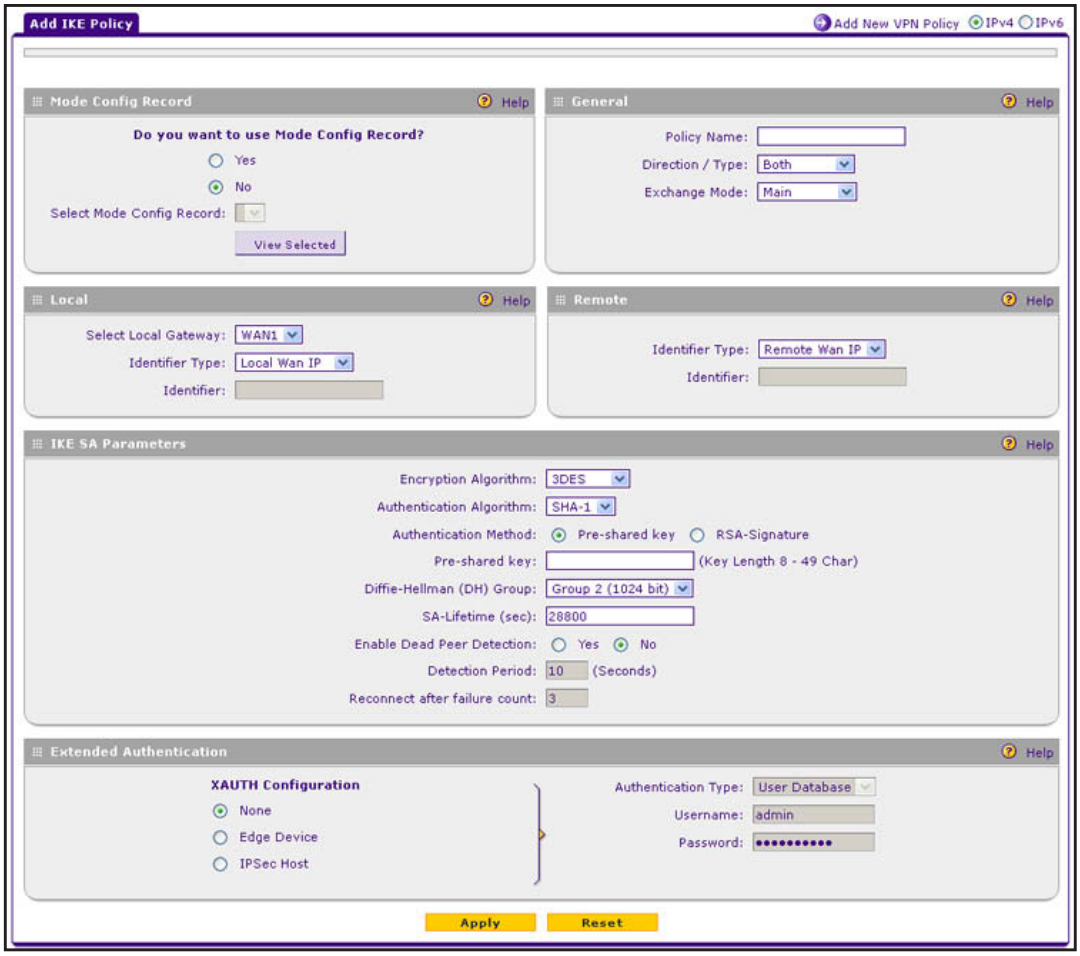

Figure 159.

4. Complete the settings as described in the following table:

Table 54. Add IKE Policy screen settings

Setting	Description	
Mode Config Record		
Do you want to use Mode Config Record?	Specify whether the IKE policy uses a Mode Config record. For information about how to define a Mode Config record, see *Mode Config Operation* on page 250. Select one of the following radio buttons: • **Yes**. IP addresses are assigned to remote VPN clients. You need to select a Mode Config record from the drop-down list. Because Mode Config functions only in Aggressive mode, selecting the Yes radio button sets the tunnel exchange mode to Aggressive mode and disables the Main mode. Mode Config also requires that both the local and remote endpoints are defined by their FQDNs. • **No**. Disables Mode Config for this IKE policy. **Note:** You can use an IPv6 IKE policy to assign IPv4 addresses to clients through a Mode Config record, but you cannot assign IPv6 addresses to clients.	
	Select Mode Config Record	From the drop-down list, select one of the Mode Config records that you defined on the Add Mode Config Record screen (see *Configure Mode Config Operation on the VPN Firewall* on page 250). **Note:** Click the **View Selected** button to open the Selected Mode Config Record Details pop-up screen.
General		
Policy Name	A descriptive name of the IKE policy for identification and management purposes. **Note:** The name is not supplied to the remote VPN endpoint.	
Direction / Type	From the drop-down list, select the connection method for the VPN firewall: • **Initiator**. The VPN firewall initiates the connection to the remote endpoint. • **Responder**. The VPN firewall responds only to an IKE request from the remote endpoint. • **Both**. The VPN firewall can both initiate a connection to the remote endpoint and respond to an IKE request from the remote endpoint.	
Exchange Mode	From the drop-down list, select the mode of exchange between the VPN firewall 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.	
Local		
Select Local Gateway	Select a WAN interface from the drop-down list to specify the WAN interface for the local gateway.	

Table 54. Add IKE Policy screen settings (continued)

Setting	Description	
Identifier	From the drop-down list, select one of the following ISAKMP identifiers to be used by the VPN firewall, and specify the identifier in the Identifier field: • **Local Wan IP**. The WAN IP address of the VPN firewall. When you select this option, the Identifier field automatically shows the IP address of the selected WAN interface. • **FQDN**. The Internet address for the VPN firewall. • **User FQDN**. The email address for a local VPN client or the VPN firewall. • **DER ASN1 DN**. A distinguished name (DN) that identifies the VPN firewall in the DER encoding and ASN.1 format.	
	Identifier	Depending on the selection of the Identifier drop-down list, enter the IP address, email address, FQDN, or distinguished name.
Remote		
Identifier	From the drop-down list, select one of the following ISAKMP identifiers to be used by the remote endpoint, and specify the identifier in the Identifier field: • **Remote Wan IP**. The WAN IP address of the remote endpoint. When you select this option, the Identifier field automatically shows the IP address of the selected WAN interface. • **FQDN**. The FQDN for a remote gateway. • **User FQDN**. The email address for a remote VPN client or gateway. • **DER ASN1 DN**. A distinguished name (DN) that identifies the remote endpoint in the DER encoding and ASN.1 format.	
	Identifier	Depending on the selection of the Identifier drop-down list, enter the IP address, email address, FQDN, or distinguished name.
IKE SA Parameters		
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.	
Authentication Algorithm	From the drop-down list, select one of the following 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.	

Table 54. Add IKE Policy screen settings (continued)

Setting	Description	
Authentication Method	Select one of the following radio buttons to specify the authentication method: • **Pre-shared key**. A secret that is shared between the VPN firewall and the remote endpoint. • **RSA-Signature**. Uses the active self-signed certificate that you uploaded on the Certificates screen (see *Manage VPN Self-Signed Certificates* on page 323). The pre-shared key is masked out when you select RSA-Signature.	
	Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote (''), single quote('), or space in the key.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following 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 occurs. The default is 28800 seconds (8 hours).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 265.	Select a radio button to specify whether Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the VPN firewall attempts to reconnect in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default is 3 failures.

Table 54. Add IKE Policy screen settings (continued)

Setting	Description	
Extended Authentication		
XAUTH Configuration **Note:** For more information about XAUTH and its authentication modes, see *Configure XAUTH for VPN Clients* on page 246.	Select one of the following radio buttons to specify whether 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 VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, or RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination.	
	Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 247). • **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 VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client and Server Configuration* on page 247. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client and Server Configuration* on page 247.
	Username	The user name for XAUTH.
	Password	The password for XAUTH.

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

➢ **To edit an IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view (see *Figure 158* on page 232).
2. Specify the IP version for which you want to edit an IKE policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.
   - **IPv6**. Select the **IPv6** radio button. The IKE Policies screen for IPv6 displays.
3. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy that you want to edit. The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen (see *Figure 159* on page 233).
4. Modify the settings that you wish to change (see the previous table).

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

Manage VPN Policies

You can create two types of VPN policies. When you use the VPN Wizard to create a VPN policy, only the Auto method is available.

- **Manual**. You manually enter all settings (including the keys) for the VPN tunnel on the VPN firewall and on the remote VPN endpoint. No third-party server or organization is involved.
- **Auto**. Some settings for the VPN tunnel are generated automatically through the use of the IKE (Internet Key Exchange) Protocol to perform negotiations between the two VPN endpoints (the local ID endpoint and the remote ID endpoint). You still need to manually enter all settings on the remote VPN endpoint (unless the remote VPN endpoint also has a VPN Wizard).

In addition, a certification authority (CA) can also be used to perform authentication (see *Manage Digital Certificates for VPN Connections* on page 320). For gateways to use a CA to perform authentication, each VPN gateway needs to have a certificate from the CA. For each certificate, there is both a public key and a private key. The public key is freely distributed, and is used by any sender to encrypt data intended for the receiver (the key owner). The receiver then uses its private key to decrypt the data (without the private key, decryption is impossible). The use of certificates for authentication reduces the amount of data entry that is required on each VPN endpoint.

VPN Policies Screen

The VPN Policies screen allows you to add additional policies—either Auto or Manual—and to manage the VPN policies already created. You can edit policies, enable or disable policies, or delete them entirely. These are the rules for VPN policy use:

- Traffic covered by a policy is automatically sent through a VPN tunnel.
- When traffic is covered by two or more policies, the first matching policy is used. (In this situation, the order of the policies is important. However, if you have only one policy for each remote VPN endpoint, the policy order is not important.)
- The VPN tunnel is created according to the settings in the security association (SA).
- The remote VPN endpoint needs to have a matching SA; otherwise, it refuses the connection.

To access the VPN Policies screen, select **VPN > IPSec VPN > VPN Policies**. In the upper right of the screen, the IPv4 radio button is selected by default. The VPN Policies screen displays the IPv4 settings. (The following figure shows some examples.) To display the IPv6 settings on the IKE Policies screen, select the **IPv6** radio button.

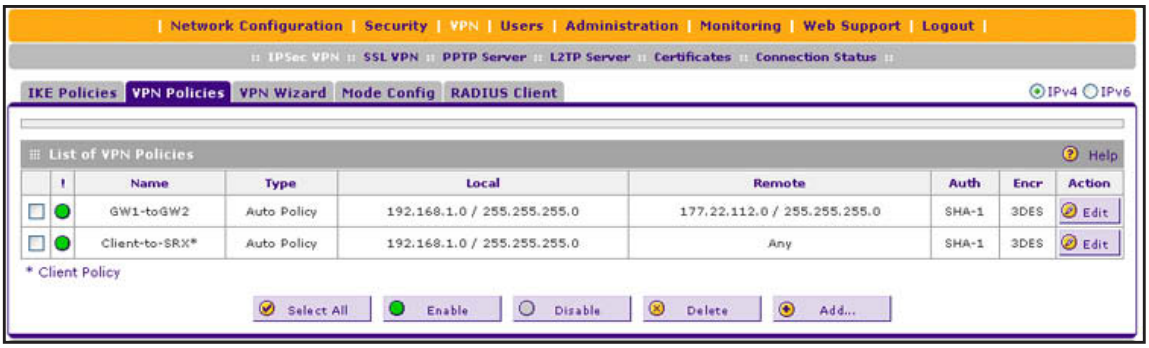

Figure 160.

Each policy contains the data that are described in the following table. These fields are described in more detail in *Table 56* on page 241.

Table 55. VPN Policies screen information for IPv4 and IPv6

Item	Description
! (Status)	Indicates whether the policy is enabled (green circle) or disabled (gray circle). To enable or disable a policy, select the check box to the left of the circle, and click the **Enable** or **Disable** table button, as appropriate.
Name	The name that identifies the VPN policy. When you use the VPN Wizard to create a VPN policy, the name of the VPN policy (and of the automatically created accompanying IKE policy) is the connection name.
Type	Auto or Manual as described previously (Auto is used during VPN Wizard configuration).
Local	IP address (either a single address, range of address, or subnet address) on your LAN. Traffic needs to be from (or to) these addresses to be covered by this policy. (The subnet address is supplied as the default IP address when you are using the VPN Wizard.)
Remote	IP address or address range of the remote network. Traffic needs to be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask.)
Auth	The authentication algorithm that is used for the VPN tunnel. This setting needs to match the setting on the remote endpoint.
Encr	The encryption algorithm that is used for the VPN tunnel. This setting needs to match the setting on the remote endpoint.

- **To delete one or more VPN polices:**

  1. Select the check box to the left of each policy that you want to delete, or click the **Select All** table button to select all VPN policies.
  2. Click the **Delete** table button.

- **To enable or disable one or more VPN policies:**

  1. Select the check box to the left of each policy that you want to enable or disable, or click the **Select All** table button to select all VPN Policies.
  2. Click the **Enable** or **Disable** table button.

For information about how to add or edit a VPN policy, see *Manually Add or Edit a VPN Policy* on this page.

Manually Add or Edit a VPN Policy

➢ **To manually add a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays the IPV4 settings (see *Figure 160* on page 239).
2. Under the List of VPN Policies table, click the **Add** table button. The Add New VPN Policy screen displays the IPv4 settings (see *Figure 161* on page 240).
3. Specify the IP version for which you want to add a VPN policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 4*.
   - **IPv6**. Select the **IPv6** radio button. The Add New VPN Policy screen for IPv6 displays (see *Figure 162* on page 241).

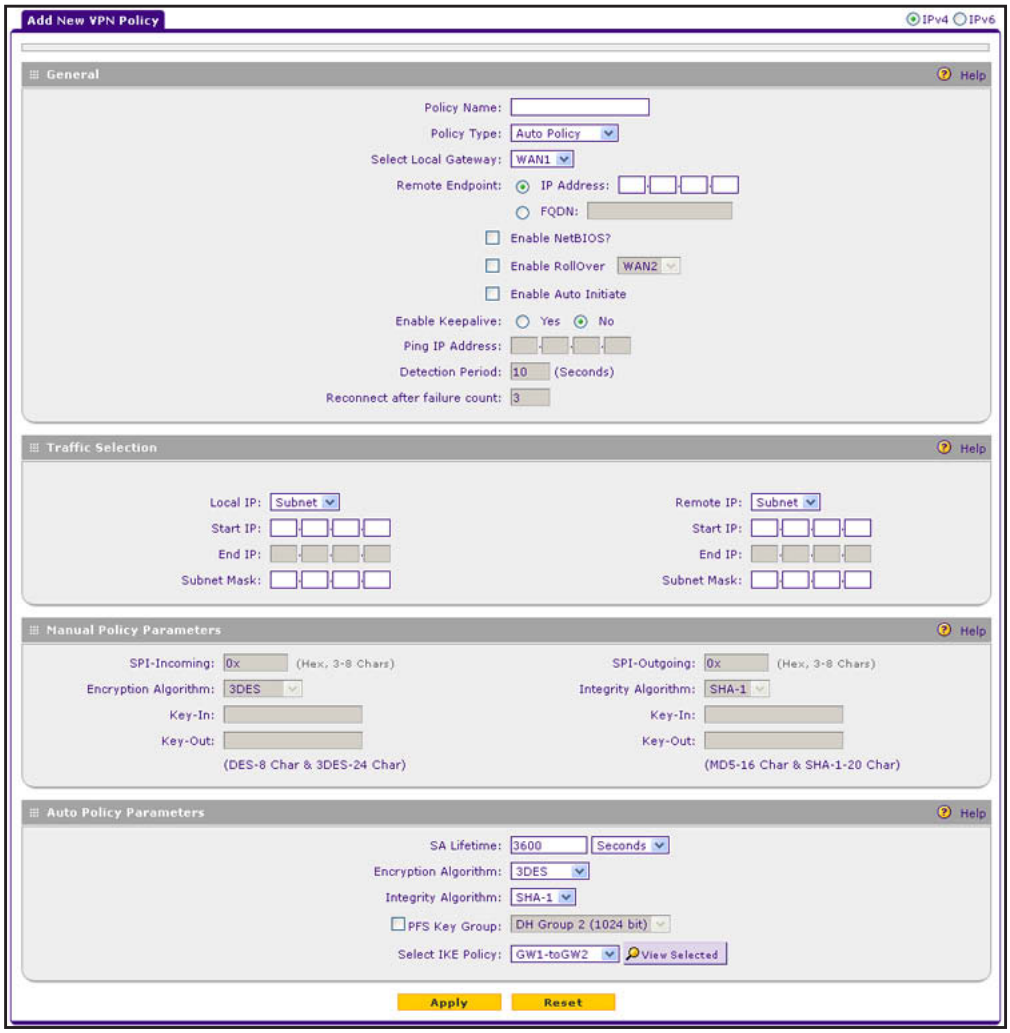

Figure 161. Add New VPN Policy screen for IPv4

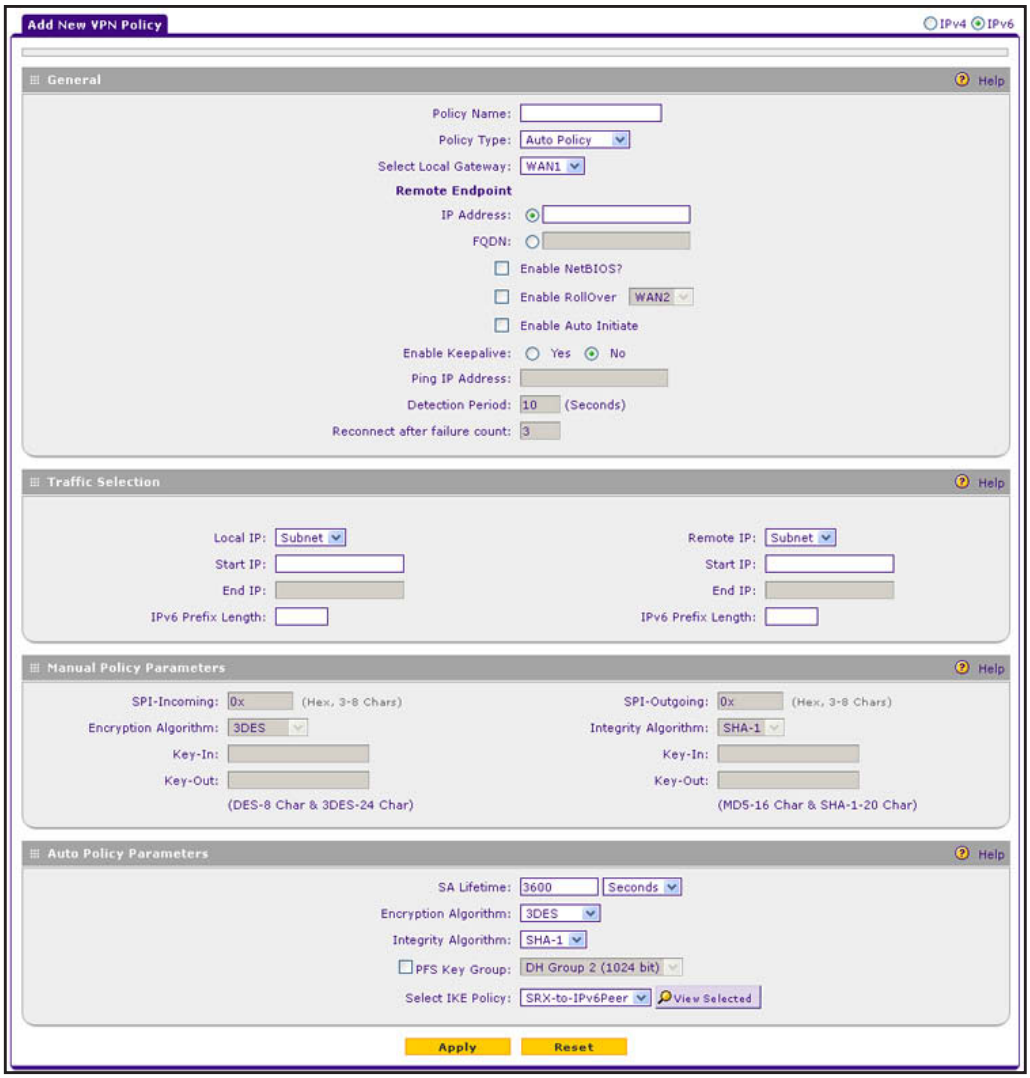

Figure 162. Add New VPN Policy screen for IPv6

4. Complete the settings as described in the following table. The only differences between IPv4 and IPv6 settings are the subnet mask (IPv4) and prefix length (IPv6).

Table 56. Add New VPN Policy screen settings for IPv4 and IPv6

Setting	Description
General	
Policy Name	A descriptive name of the VPN policy for identification and management purposes. **Note:** The name is not supplied to the remote VPN endpoint.

Table 56. Add New VPN Policy screen settings for IPv4 and IPv6 (continued)

Setting	Description	
Policy Type	From the drop-down list, select one of the following policy types: • **Auto Policy**. Some settings (the ones in the Manual Policy Parameters section of the screen) for the VPN tunnel are generated automatically. • **Manual Policy**. All settings need to be specified manually, including the ones in the Manual Policy Parameters section of the screen.	
Select Local Gateway	Select a WAN interface from the drop-down list to specify the WAN interface for the local gateway.	
Remote Endpoint	Select a radio button to specify how the remote endpoint is defined: • **IP Address**. Enter the IP address of the remote endpoint in the fields to the right of the radio button. • **FQDN**. Enter the FQDN of the remote endpoint in the field to the right of the radio button.	
Enable NetBIOS?	Select this check box to enable NetBIOS broadcasts to travel over the VPN tunnel. For more information about NetBIOS, see *Configure NetBIOS Bridging with IPSec VPN* on page 268. This feature is disabled by default.	
Enable RollOver?	Select this check box to allow the VPN tunnel to roll over to the other WAN interface when the WAN mode is set to Auto-Rollover and an actual rollover occurs. This feature is disabled by default. Select a WAN interface from the drop-down list.	
Enable Auto Initiate	Select this check box to enable the VPN tunnel to autoestablish itself without the presence of any traffic. **Note:** The direction and type of the IKE policy that is associated with this VPN policy need to be either Initiator or Both but cannot be Responder. For more information, see *Manually Add or Edit an IKE Policy* on page 233.	
Enable Keepalive **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 265.	Select a radio button to specify if keep-alive is enabled: • **Yes**. This feature is enabled: Periodically, the VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You need to specify the ping IP address in the Ping IP Address field, the detection period in the Detection Period field, and the maximum number of keep-alive requests that the VPN firewall sends in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Ping IP Address	The IP address that the VPN firewall pings. The address needs to be of a host that can respond to ICMP ping requests.
	Detection Period	The period in seconds between the keep-alive requests. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of keep-alive requests before the VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is 3 keep-alive requests.

Table 56. Add New VPN Policy screen settings for IPv4 and IPv6 (continued)

Setting	Description
Traffic Selection	
Local IP	From the drop-down list, select the address or addresses that are part of the VPN tunnel on the VPN firewall: • **Any**. All computers and devices on the network. Note that you cannot select Any for both the VPN firewall 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. In addition: - **Subnet Mask**. For IPv4 addresses on the IPv4 screen only, enter the subnet mask. - **IPv6 Prefix Length**. For IPv6 addresses on the IPv6 screen only, enter the prefix length.
Remote IP	From the drop-down list, select the address or addresses that are part of the VPN tunnel on the remote endpoint. The selections are the same as for the Local IP drop-down list.
Manual Policy Parameters **Note:** These fields apply only when you select Manual Policy as the policy type. When you specify the settings for the fields in this section, a security association (SA) is created.	
SPI-Incoming	The Security Parameters Index (SPI) for the inbound policy. Enter a hexadecimal value between 3 and 8 characters (for example, 0x1234).
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **3DES**. Triple DES. This is the default algorithm. • **None**. No encryption algorithm. • **DES**. Data Encryption Standard (DES). • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.
Key-In	The encryption key for the inbound policy. The length of the key depends on the selected encryption algorithm: • **3DES**. Enter 24 characters. • **None**. Key does not apply. • **DES**. Enter 8 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.

Table 56. Add New VPN Policy screen settings for IPv4 and IPv6 (continued)

Setting	Description
Key-Out	The encryption key for the outbound policy. The length of the key depends on the selected encryption algorithm: • **3DES**. Enter 24 characters. • **DES**. Enter 8 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.
SPI-Outgoing	The Security Parameters Index (SPI) for the outbound policy. Enter a hexadecimal value between 3 and 8 characters (for example, 0x1234).
Integrity Algorithm	From the drop-down list, select one of the following 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 the outbound policy. The length of the key depends on the selected integrity algorithm: • **MD5**. Enter 16 characters. • **SHA-1**. Enter 20 characters.
Auto Policy Parameters **Note:** These fields apply only when you select Auto Policy as the policy type.	
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. From the drop-down list, select how the SA lifetime is specified: • **Seconds**. In the SA Lifetime field, enter a period in seconds. The minimum value is 300 seconds. The default setting is 3600 seconds. • **KBytes**. In the SA Lifetime field, enter a number of kilobytes. The minimum value is 1920000 KB.
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **3DES**. Triple DES. This is the default algorithm. • **None**. No encryption algorithm. • **DES**. Data Encryption Standard (DES). • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.

Table 56. Add New VPN Policy screen settings for IPv4 and IPv6 (continued)

Setting	Description
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and select a Diffie-Hellman (DH) group from the drop-down list. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**.
Select IKE Policy	Select an existing IKE policy that defines the characteristics of the Phase-1 negotiation. To display the selected IKE policy, click the **View Selected** button.

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 > VPN Policies**. The VPN Policies screen displays the IPv4 settings (see *Figure 160* on page 239).
2. Specify the IP version for which you want to edit a VPN policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.
   - **IPv6**. Select the **IPv6** radio button. The VPN Policies screen for IPv6 displays.
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 fields as the Add New VPN Policy screen (for IPv4, see *Figure 161* on page 240; for IPv6 see *Figure 162* on page 241).
4. Modify the settings that you wish to change (see the previous table).
5. Click **Apply** to save your changes. The modified VPN policy is displayed in the List of VPN Policies table.

Configure Extended Authentication (XAUTH)

- *Configure XAUTH for VPN Clients*
- *User Database Configuration*
- *RADIUS Client and Server Configuration*

When many VPN clients connect to a VPN firewall, you might want to use a unique user authentication method beyond relying on a single common pre-shared key for all clients. Although you could configure a unique VPN policy for each user, it is more efficient to authenticate users from a stored list of user accounts. XAUTH provides the mechanism for

requesting individual authentication information from the user. A local user database or an external authentication server, such as a RADIUS server, provides a method for storing the authentication information centrally in the local network.

You can enable XAUTH when you manually add or edit an IKE policy. Two types of XAUTH are available:

- **Edge Device**. The VPN firewall is used as a VPN concentrator on which one or more gateway tunnels terminate. You need to specify the authentication type that should be used during verification of the credentials of the remote VPN gateways: the user database, RADIUS-PAP, or RADIUS-CHAP.
- **IPSec Host**. Authentication by the remote gateway through a user name and password that are associated with the IKE policy. The user name and password that are used to authenticate the VPN firewall need to be specified on the remote gateway.

Note: If a RADIUS-PAP server is enabled for authentication, XAUTH first checks the local user database for the user credentials. If the user account is not present, the VPN firewall then connects to a RADIUS server.

Configure XAUTH for VPN Clients

Once the XAUTH has been enabled, you need to establish user accounts in the user database to be authenticated against XAUTH, or you need to enable a RADIUS-CHAP or RADIUS-PAP server.

Note: You cannot modify an existing IKE policy to add XAUTH while the IKE policy is in use by a VPN policy. The VPN policy needs to be disabled before you can modify the IKE policy.

➢ **To enable and configure XAUTH:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies for IPv4 screen in view (see *Figure 158* on page 232).
2. Specify the IP version for which you want to edit an IKE policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.
   - **IPv6**. Select the **IPv6** radio button. The IKE Policies screen for IPv6 displays.
3. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy for which you want to enable and configure XAUTH. The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen (see *Figure 159* on page 233).

4. In the Extended Authentication section on the screen, complete the settings as described in the following table:

Table 57. Extended authentication settings for IPv4 and IPv6

Setting	Description
Select one of the following radio buttons to specify whether 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 VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination.	
Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 247). • **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 VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client and Server Configuration* on page 247. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client and Server Configuration* on page 247.
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 need to be authenticated either by a local user database account or by an external RADIUS server. Whether or not you use a RADIUS server, you might want some users to be authenticated locally. These users need to be added to the List of Users table on the Users screen, as described in *Configure User Accounts* on page 310.

RADIUS Client and Server Configuration

Remote Authentication Dial In User Service (RADIUS, RFC 2865) is a protocol for managing authentication, authorization, and accounting (AAA) of multiple users in a network. A RADIUS server stores a database of user information and can validate a user at the request of a gateway or server in the network when a user requests access to network resources. During the establishment of a VPN connection, the VPN gateway can interrupt the process with an XAUTH request. At that point, the remote user needs to provide authentication information such as a user name and password or some encrypted response using the 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.

Note: Even though you can configure RADIUS servers with IPv4 addresses only, the servers can be used for authentication, authorization, and accounting of both IPv4 and IPv6 users.

➢ **To configure primary and backup RADIUS servers:**

1. Select **VPN > IPSec VPN > RADIUS Client**. The RADIUS Client screen displays:

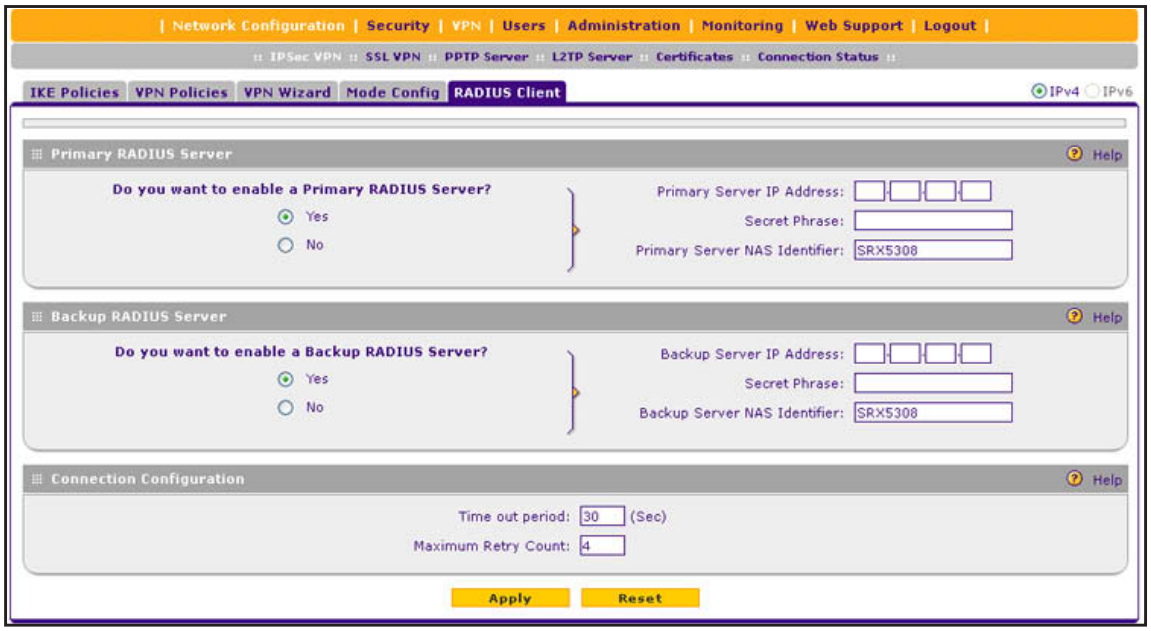

Figure 163.

2. Complete the settings as described in the following table:

Table 58. RADIUS Client screen settings

Setting	Description
Primary RADIUS Server	
To enable and configure the primary RADIUS server, select the **Yes** radio button, and enter the settings for the three fields to the right. The default setting is that the No radio button is selected.	
Primary Server IP Address	The IPv4 address of the primary RADIUS server.
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the primary RADIUS server. The same secret phrase needs to be configured on both the client and the server.

Table 58. RADIUS Client screen settings (continued)

Setting	Description
Primary Server NAS Identifier	The primary Network Access Server (NAS) identifier that needs to be present in a RADIUS request. **Note:** The VPN firewall functions as an NAS, allowing network access to external users after verification of their authentication information. In a RADIUS transaction, the NAS needs to provide some NAS identifier information to the RADIUS server. Depending on the configuration of the RADIUS server, the VPN firewall's IP address might be sufficient as an identifier, or the server might require a name, which you need to enter in this field.
Backup RADIUS Server	
To enable and configure the backup RADIUS server, select the **Yes** radio button, and enter the settings for the three fields to the right. The default setting is that the No radio button is selected.	
Backup Server IP Address	The IPv4 address of the backup RADIUS server.
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the backup RADIUS server. The same secret phrase needs to be configured on both the client and the server.
Backup Server NAS Identifier	The backup Network Access Server (NAS) identifier that needs to be present in a RADIUS request. **Note:** See the note earlier in this table for the Primary Server NAS Identifier.
Connection Configuration	
Time out period	The period in seconds that the VPN firewall waits for a response from a RADIUS server. The default setting is 30 seconds.
Maximum Retry Counts	The maximum number of times that the VPN firewall attempts to connect to a RADIUS server. The default setting is 4 retry counts.

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

Note: You can select the RADIUS authentication protocol (PAP or CHAP) on the Edit IKE Policy screen or Add IKE Policy screen (see *Configure XAUTH for VPN Clients* on page 246).

Assign IPv4 Addresses to Remote Users (Mode Config)

To simplify the process of connecting remote VPN clients to the VPN firewall, use the Mode Config feature to automatically assign IPv4 addresses to remote users, including a network access IP address, subnet mask, WINS server, and DNS address. Remote users are given IP addresses available in a secured network space so that remote users appear as seamless extensions of the network.

You can use the Mode Config feature in combination with an IPv6 IKE policy to assign IPv4 addresses to clients, but you cannot assign IPv6 addresses to clients.

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 VPN firewall. 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 165* on page 251).

Note: After configuring a Mode Config record, you need to manually configure an IKE policy and select the newly created Mode Config record from the Select Mode Config Record drop-down list (see *Configure Mode Config Operation on the VPN Firewall* on page 250). You do not need to change 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.

Configure Mode Config Operation on the VPN Firewall

To configure Mode Config on the VPN firewall, first create a Mode Config record, and then select the Mode Config record for an IKE policy.

➢ **To configure Mode Config on the VPN firewall:**

1. Select **VPN > IPSec VPN > Mode Config**. The Mode Config screen displays:

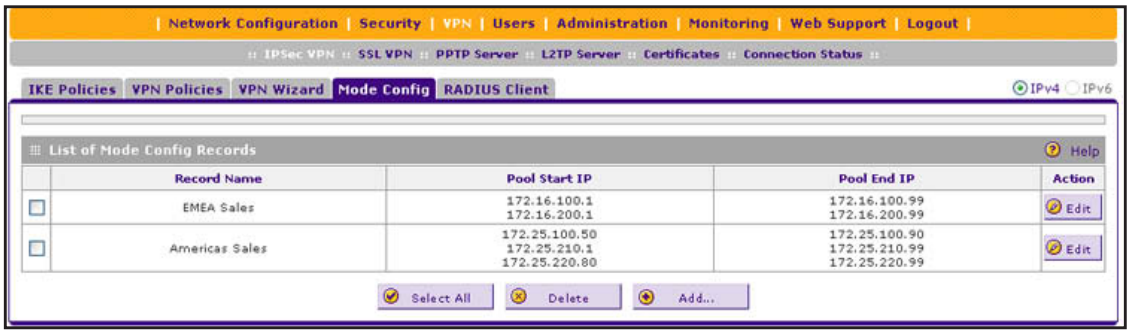

Figure 164.

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

- For EMEA Sales, a first pool (172.16.100.1 through 172.16.100.99) and second pool (172.16.200.1 through 172.16.200.99) are shown.
- For Americas Sales, a first pool (172.25.100.50 through 172.25.100.99), a second pool (172.25.210.1 through 172.25.210.99), and a third pool (172.25.220.80 through 172.25.220.99) are shown.

2. Under the List of Mode Config Records table, click the **Add** table button. The Add Mode Config Record screen displays:

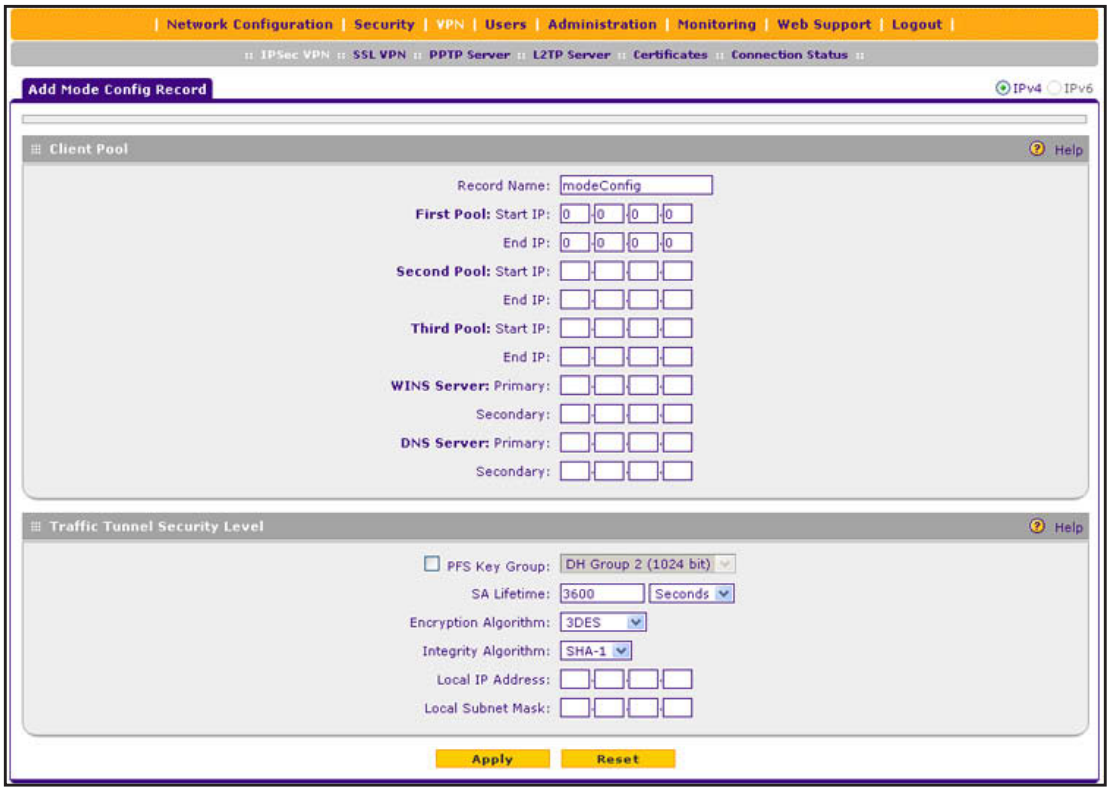

Figure 165.

3. Complete the settings as described in the following table:

Table 59. Add Mode Config Record screen settings

Setting	Description
Client Pool	
Record Name	A descriptive name of the Mode Config record for identification and management purposes.
First Pool	Assign at least one range of IP pool addresses in the First Pool fields to enable the VPN firewall to allocate these to remote VPN clients. The Second Pool and Third Pool fields are optional. To specify any client pool, enter the starting IP address for the pool in the Starting IP field, and enter the ending IP address for the pool in the Ending IP field. **Note:** No IP pool should be within the range of the local network IP addresses. Use a different range of private IP addresses such as 172.16.xxx.xx.
Second Pool	
Third Pool	
WINS Server	If there is a WINS server on the local network, enter its IP address in the Primary field. You can enter the IP address of a second WINS server in the Secondary field.
DNS Server	Enter the IP address of the DNS server that is used by remote VPN clients in the Primary field. You can enter the IP address of a second DNS server in the Secondary field.
Traffic Tunnel Security Level **Note:** Generally, the default settings work well for a Mode Config configuration.	
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and select a Diffie-Hellman (DH) group from the drop-down list. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)** • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. From the drop-down list, select how the SA lifetime is specified: • **Seconds**. In the SA Lifetime field, enter a period in seconds. The minimum value is 300 seconds. The default setting is 3600 seconds. • **KBytes**. In the SA Lifetime field, enter a number of kilobytes. The minimum value is 1920000 KB.
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **None**. No encryption. • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.

Table 59. Add Mode Config Record screen settings (continued)

Setting	Description
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.
Local IP Address	The local IP address to which remote VPN clients have access. If you do not specify a local IP address, the VPN firewall's default LAN IP address is used (by default, 192.168.1.1).
Local Subnet Mask	The local subnet mask. Typically, this is 255.255.255.0. **Note:** If you do not specify a local IP address, you do not need to specify a subnet either.

4. Click **Apply** to save your settings. The new Mode Config record is added to the List of Mode Config Records table.

   Continue the Mode Config configuration procedure by configuring an IKE policy.

5. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 158* on page 232).
6. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays the IPv4 settings (see the next figure).
7. Specify the IP version for which you want to add an IKE policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 8*.
   - **IPv6**. Select the **IPv6** radio button. The Add IKE Policy screen for IPv6 displays. This screen is identical to the Add IKE Policy screen for IPv4 (see the next figure).

Note: You can configure an IPv6 IKE policy to assign IPv4 addresses to clients, but you cannot assign IPv6 addresses to clients.

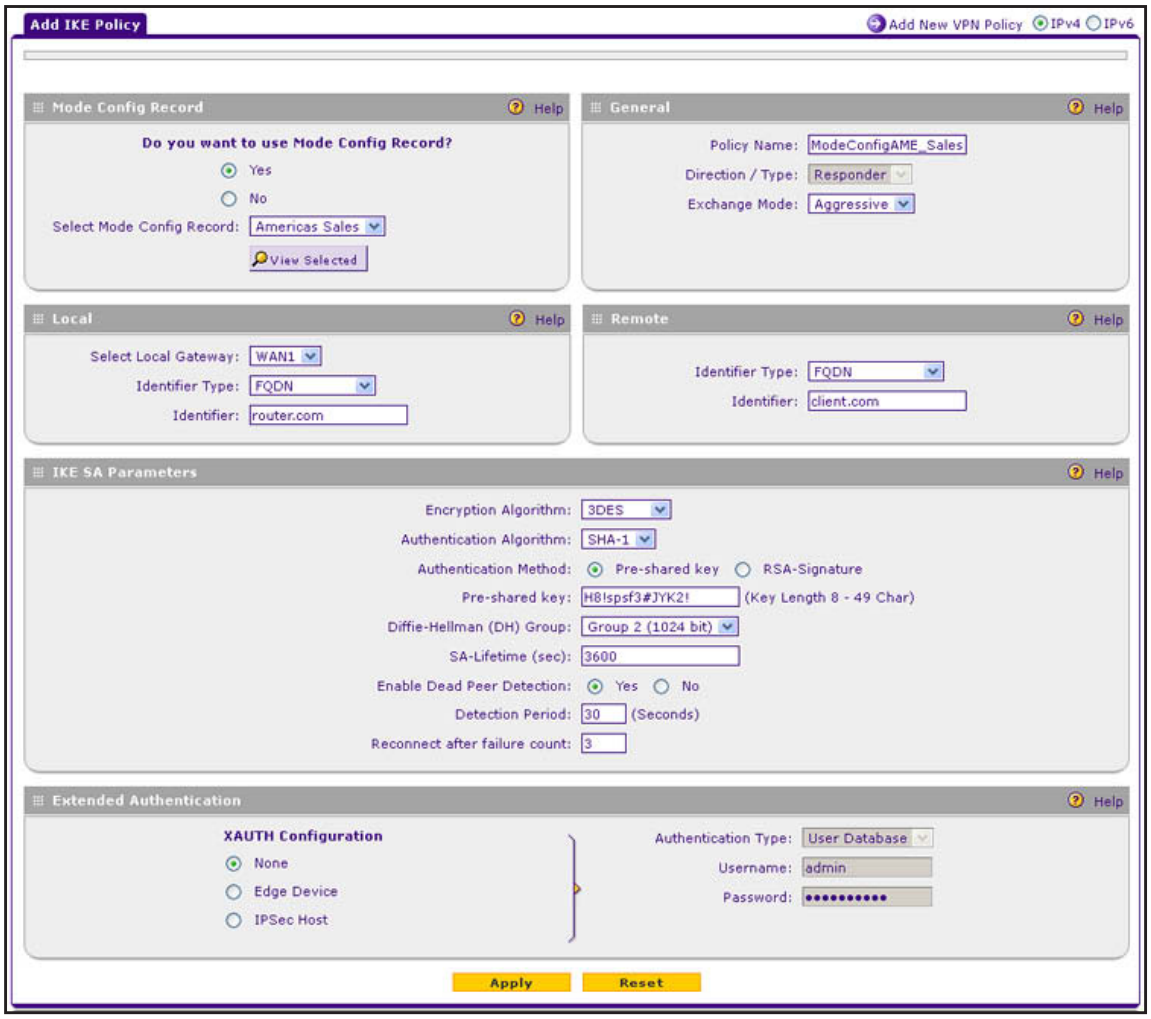

Figure 166.

8. On the Add IKE Policy screen, complete the settings as described in the following table.

Note: The IKE policy settings that are described in the following table are specifically for a Mode Config configuration. *Table 54* on page 234 explains the general IKE policy settings.

Table 60. Add IKE Policy screen settings for a Mode Config configuration

Setting	Description	
Mode Config Record		
Do you want to use Mode Config Record?	Select the **Yes** radio button. **Note:** Because Mode Config functions only in Aggressive mode, selecting the Yes radio button sets the tunnel exchange mode to Aggressive mode. Mode Config also requires that both the local and remote endpoints are defined by their FQDNs.	
	Select Mode Config Record	From the drop-down list, select the Mode Config record that you created in *Step 4* on page 253. This example uses NA Sales.
General		
Policy Name	A descriptive name of the IKE policy for identification and management purposes. This example uses ModeConfigAME_Sales. **Note:** The name is not supplied to the remote VPN endpoint.	
Direction / Type	Responder is automatically selected when you select the Mode Config record in the Mode Config Record section of the screen. This ensures that the VPN firewall responds to an IKE request from the remote endpoint but does not initiate one.	
Exchange Mode	Aggressive mode is automatically selected when you select the Mode Config record in the Mode Config Record section of the screen.	
Local		
Select Local Gateway	Select a WAN interface from the drop-down list to specify the WAN interface for the local gateway.	
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the VPN firewall (that is, the local endpoint) is defined by an FQDN.	
	Identifier	Enter an FQDN for the VPN firewall. This example uses router.com.
Remote		
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the remote endpoint is defined by an FQDN.	
	Identifier	Enter the FQDN for the remote endpoint. This needs to be an FQDN that is not used in any other IKE policy. This example uses client.com.

Table 60. Add IKE Policy screen settings for a Mode Config configuration (continued)

Setting	Description	
IKE SA Parameters **Note:** Generally, the default settings work well for a Mode Config configuration.		
Encryption Algorithm	To negotiate the security association (SA), from the drop-down list, select the **3DES** algorithm.	
Authentication Algorithm	From the drop-down list, select the **SHA-1** algorithm to be used in the VPN header for the authentication process.	
Authentication Method	Select **Pre-shared key** as the authentication method, and enter a key in the Pre-shared key field.	
	Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote ("), single quote('), or space in the key. This example uses H8!spsf3#JYK2!.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. From the drop-down list, select **Group 2 (1024 bit)**.	
SA-Lifetime (sec)	The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying occurs. The default setting is 28800 seconds (8 hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (1 hour).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 265.	Select a radio button to specify whether Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the VPN firewall attempts to reconnect in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds. This example uses 30 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default setting is 3 failures.

Table 60. Add IKE Policy screen settings for a Mode Config configuration (continued)

Setting	Description	
Extended Authentication		
XAUTH Configuration **Note:** For more information about XAUTH and its authentication modes, see *Configure XAUTH for VPN Clients* on page 246.	Select one of the following radio buttons to specify whether 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 VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination.	
	Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 247). • **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 VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client and Server Configuration* on page 247. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client and Server Configuration* on page 247.
	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.

Configure the ProSafe VPN Client for Mode Config Operation

When the Mode Config feature is enabled, the following information is negotiated between the VPN client and the VPN firewall during the authentication phase:

- Virtual IP address of the VPN client
- DNS server address (optional)
- WINS server address (optional)

The virtual IP address that is issued by the VPN firewall is displayed in the VPN Client Address field on the VPN client's IPSec pane.

Note: Perform these tasks from a computer that has the NETGEAR ProSafe VPN Client installed.

To configure the VPN client for Mode Config operation, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and specify the global parameters.

Configure the Mode Config Authentication Settings (Phase 1 Settings)

➢ **To create new authentication settings:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays:

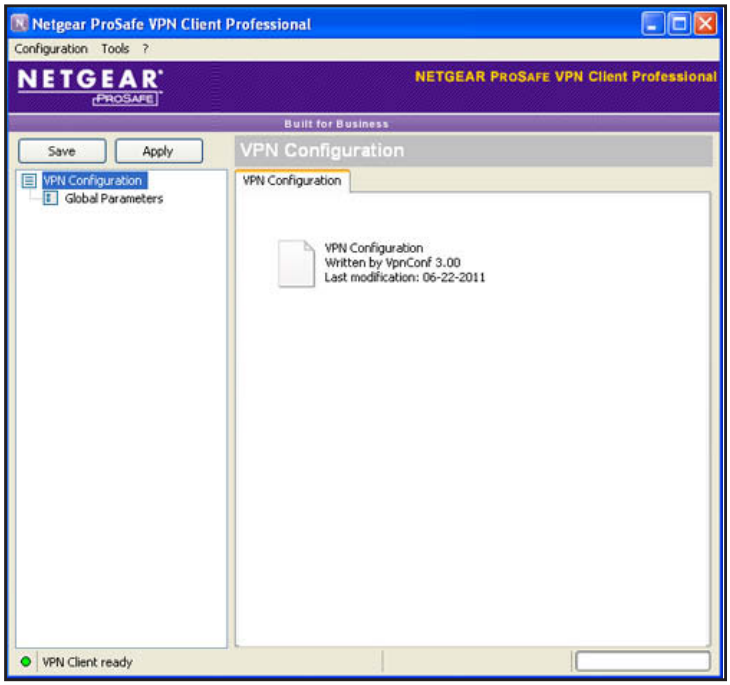

Figure 167.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.

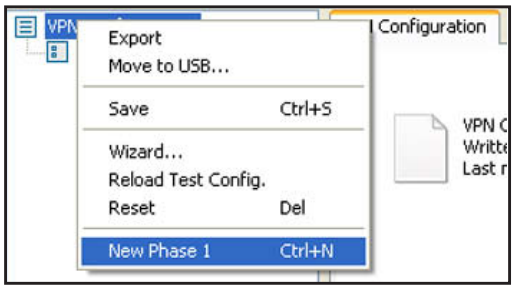

Figure 168.

3. Change the name of the authentication phase (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Type **GW_ModeConfig**.
   d. Click anywhere in the tree list pane.

   Note: *This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

   The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default:

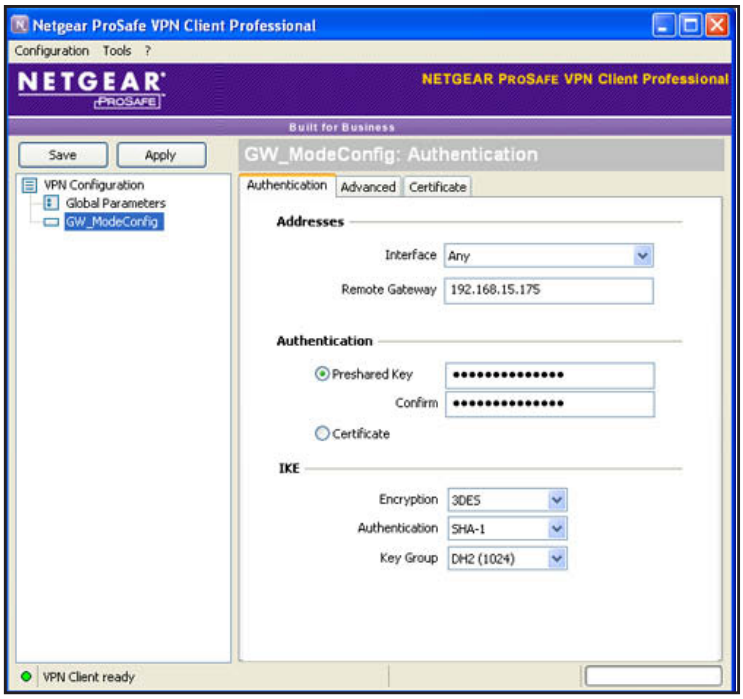

Figure 169.

4. Specify the settings that are described in the following table.

Table 61. VPN client authentication settings (Mode Config)

Setting	Description
Interface	Select **Any** from the drop-down list.
Remote Gateway	Enter the remote IP address or DNS name of the VPN firewall. For example, enter **192.168.15.175**.
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **H8!spsf3#JYK2!**. Confirm the key in the Confirm field.

Table 61. VPN client authentication settings (Mode Config) (continued)

Setting	Description	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.
6. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays:

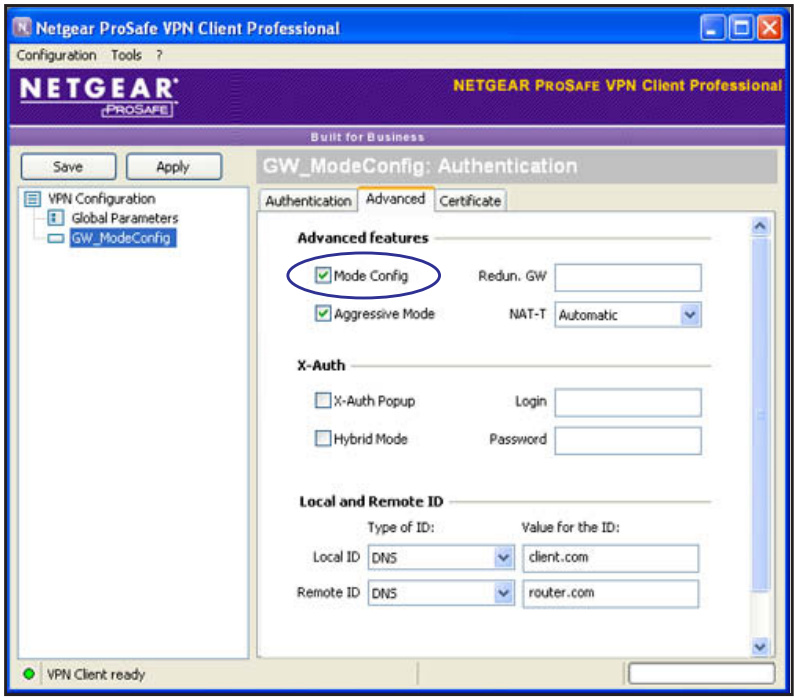

Figure 170.

7. Specify the settings that are described in the following table.

Table 62. VPN client advanced authentication settings (Mode Config)

Setting	Description
Advanced features	
Mode Config	Select this check box to enable Mode Config.
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the VPN firewall.

Table 62. VPN client advanced authentication settings (Mode Config) (continued)

Setting	Description
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **client.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **router.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the Mode Config IPSec Configuration (Phase 2 Settings)

Note: On the VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **GW_ModeConfig** authentication phase name, and select **New Phase 2**.
2. Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Type **Tunnel_ModeConfig**.
   d. Click anywhere in the tree list pane.

Note: *This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default:

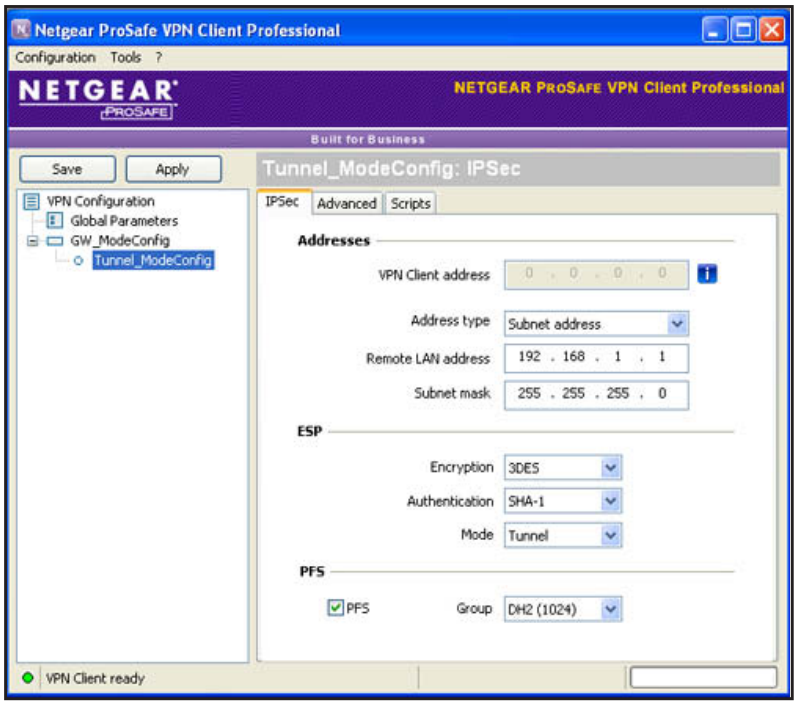

Figure 171.

3. Specify the settings that are described in the following table.

Table 63. VPN client IPSec configuration settings (Mode Config)

Setting	Description
VPN Client address	This field is masked out because Mode Config is selected. After an IPSec connection is established, the IP address that is issued by the VPN firewall displays in this field (see *Figure 176* on page 266).
Address Type	Select **Subnet address** from the drop-down list.
Remote host address	The address that you need to enter depends on whether you have specified a LAN IP network address in the Local IP Address field on the Add Mode Config Record screen of the VPN firewall: • If you left the Local IP Address field blank, enter the VPN firewall's default LAN IP address as the remote host address that opens the VPN tunnel. For example, enter **192.168.1.1**. • If you specified a LAN IP network address in the Local IP Address field, enter the address that you specified as the remote host address that opens the VPN tunnel.
Subnet mask	Enter **255.255.255.0** as the remote subnet mask of the VPN firewall that opens the VPN tunnel. This is the LAN IP subnet mask that you specified in the Local Subnet Mask field on the Add Mode Config Record screen of the VPN firewall. If you left the Local Subnet Mask field blank, enter the VPN firewall's default IP subnet mask.

Table 63. VPN client IPSec configuration settings (Mode Config) (continued)

Setting	Description	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and select the **DH2 (1024)** key group from the drop-down list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure the Mode Config Global Parameters

➢ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen:

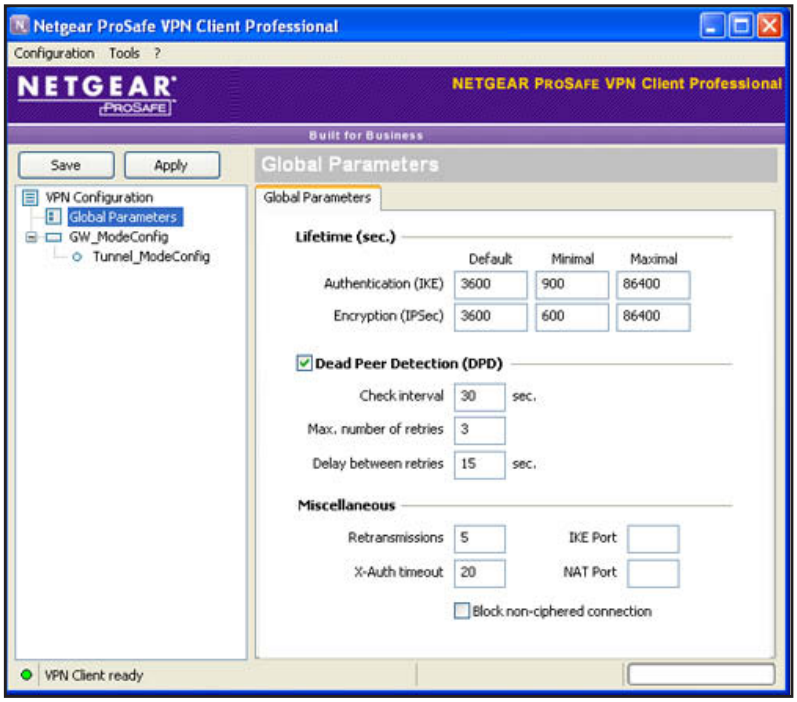

Figure 172.

2. Specify the following default lifetimes in seconds to match the configuration on the VPN firewall:
   - **Authentication (IKE)**, **Default**. Enter **3600** seconds.

     Note: *The default setting is 28800 seconds (8 hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (1 hour).*

   - **Encryption (IPSec)**, **Default**. Enter **3600** seconds.
3. Select the **Dead Peer Detection (DPD)** check box, and configure the following DPD settings to match the configuration on the VPN firewall:
   - **Check Interval**. Enter **30** seconds.
   - **Max. number of entries**. Enter **3** retries.
   - **Delay between entries**. Leave the default delay setting of 15 seconds.
4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The Mode Config configuration of the VPN client is now complete.

Test the Mode Config Connection

➢ **To test the Mode Config connection from the VPN client to the VPN firewall:**

1. Right-click the system tray icon, and select **Open tunnel 'Tunnel_ModeConfig'**.

Figure 173.

When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray, and the VPN client displays a green icon in the system tray.

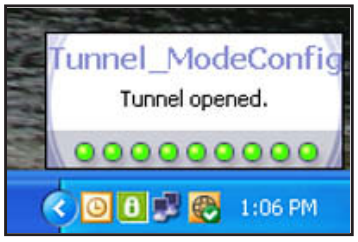

Figure 174.

2. Verify that the VPN firewall issued an IP address to the VPN client. This IP address displays in the VPN Client address field on the IPSec pane of the VPN client. (The following figure shows the upper part of the IPSec pane only.)

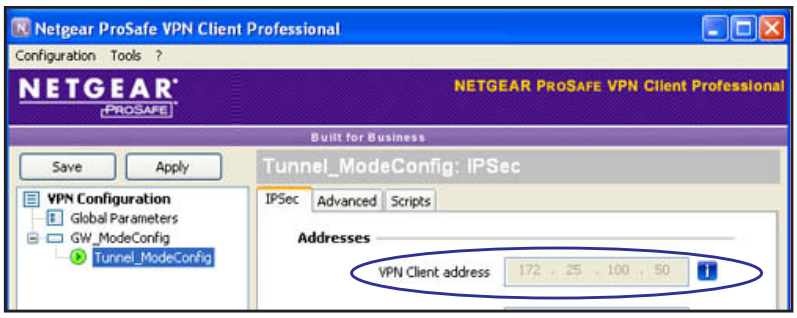

Figure 175.

3. From the client computer, ping a computer on the VPN firewall LAN.

Modify or Delete a Mode Config Record

Note: Before you modify or delete a Mode Config record, make sure that it is not used in an IKE policy.

➢ **To edit a Mode Config record:**

1. On the Mode Config screen (see *Figure 164* on page 251), click the **Edit** button in the Action column for the record that you want to modify. The Edit Mode Config Record screen displays. This screen is identical to the Add Mode Config Record screen (see *Figure 165* on page 251).
2. Modify the settings as described in *Table 59* on page 252.
3. Click **Apply** to save your settings.

➢ **To delete one or more Mode Config records:**

1. On the Mode Config screen (see *Figure 164* on page 251), select the check box to the left of each record that you want to delete, or click the **Select All** table button to select all records.
2. Click the **Delete** table button.

Configure Keep-Alives and Dead Peer Detection

- *Configure Keep-Alives*
- *Configure Dead Peer Detection*

In some cases, you might not want a VPN tunnel to be disconnected when traffic is idle, for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require a VPN tunnel to remain connected, you can use the

keep-alive and Dead Peer Detection (DPD) features to prevent the tunnel from being disconnected and to force a reconnection if the tunnel disconnects for any reason.

For DPD to function, the peer VPN device on the other end of the tunnel also needs to support DPD. Keep-alive, though less reliable than DPD, does not require any support from the peer device.

Configure Keep-Alives

The keep-alive feature maintains the IPSec SA by sending periodic ping requests to a host across the tunnel and monitoring the replies.

➢ **To configure the keep-alive feature on a configured VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays the IPv4 settings (see *Figure 160* on page 239).
2. Specify the IP version for which you want to edit a VPN policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.
   - **IPv6**. Select the **IPv6** radio button. The VPN Policies screen for IPv6 displays.
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. (The following figure shows only the top part with the General section of the Edit VPN Policy screen for IPv6.)

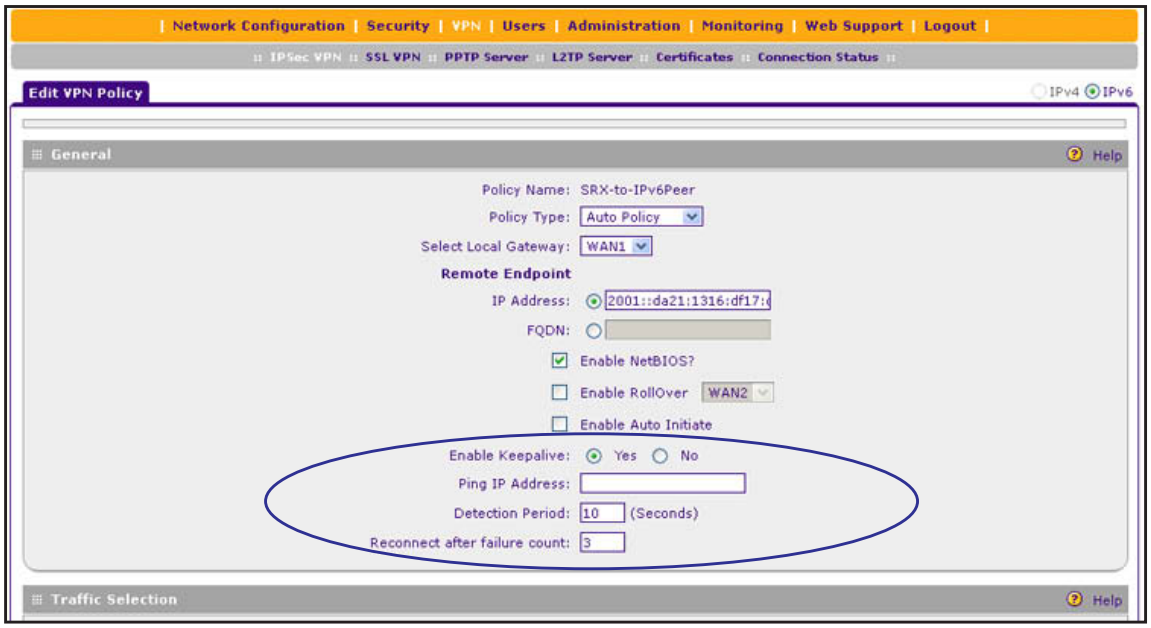

Figure 176.

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

Table 64. Keep-alive settings

Setting	Description	
General		
Enable Keepalive	Select the **Yes** radio button to enable the keep-alive feature. Periodically, the VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You need to specify the ping IP address in the Ping IP Address field, the detection period in the Detection Period field, and the maximum number of keep-alive requests that the VPN firewall sends in the Reconnect after failure count field.	
	Ping IP Address	The IP address that the VPN firewall pings. The address should be of a host that can respond to ICMP ping requests.
	Detection Period	The period in seconds between the keep-alive requests. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of keep-alive requests before the VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is 3 keep-alive requests.

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

Configure Dead Peer Detection

The Dead Peer Detection (DPD) feature lets the VPN firewall maintain the IKE SA by exchanging periodic messages with the remote VPN peer.

➢ **To configure DPD on a configured IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view (see *Figure 158* on page 232).
2. Specify the IP version for which you want to edit an IKE policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.
   - **IPv6**. Select the **IPv6** radio button. The IKE Policies screen for IPv6 displays.
3. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy that you want to edit. The Edit IKE Policy screen displays. (The following figure shows only the IKE SA Parameters section of the screen).

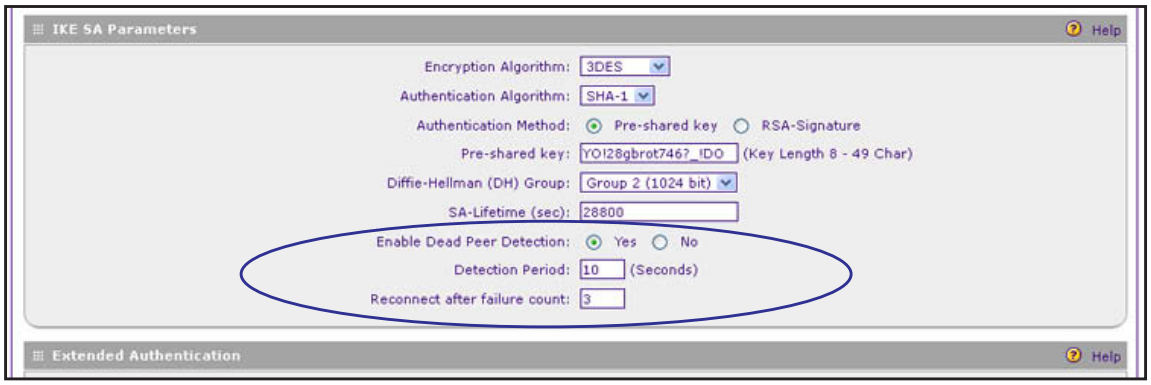

Figure 177.

4. In the IKE SA Parameters section of the screen, locate the DPD fields, and complete the settings as described the following table:

Table 65. Dead Peer Detection settings

Setting	Description	
IKE SA Parameters		
Enable Dead Peer Detection	Select the **Yes** radio button to enable DPD. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the VPN firewall attempts to reconnect in the Reconnect after failure count field.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default setting is 3 failures.

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

Configure NetBIOS Bridging with IPSec VPN

Windows networks use the Network Basic Input/Output System (NetBIOS) for several basic network services such as naming and neighborhood device discovery. Because VPN routers do not usually pass NetBIOS traffic, these network services do not function for hosts on opposite ends of a VPN connection. To solve this problem, you can configure the VPN firewall to bridge NetBIOS traffic over the VPN tunnel.

➢ **To enable NetBIOS bridging on a configured VPN tunnel:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 160* on page 239).

2. Specify the IP version for which you want to edit a VPN policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.
   - **IPv6**. Select the **IPv6** radio button. The VPN Policies screen for IPv6 displays.
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. (The following figure shows only the top part with the General section of the Edit VPN Policy screen for IPv6.)

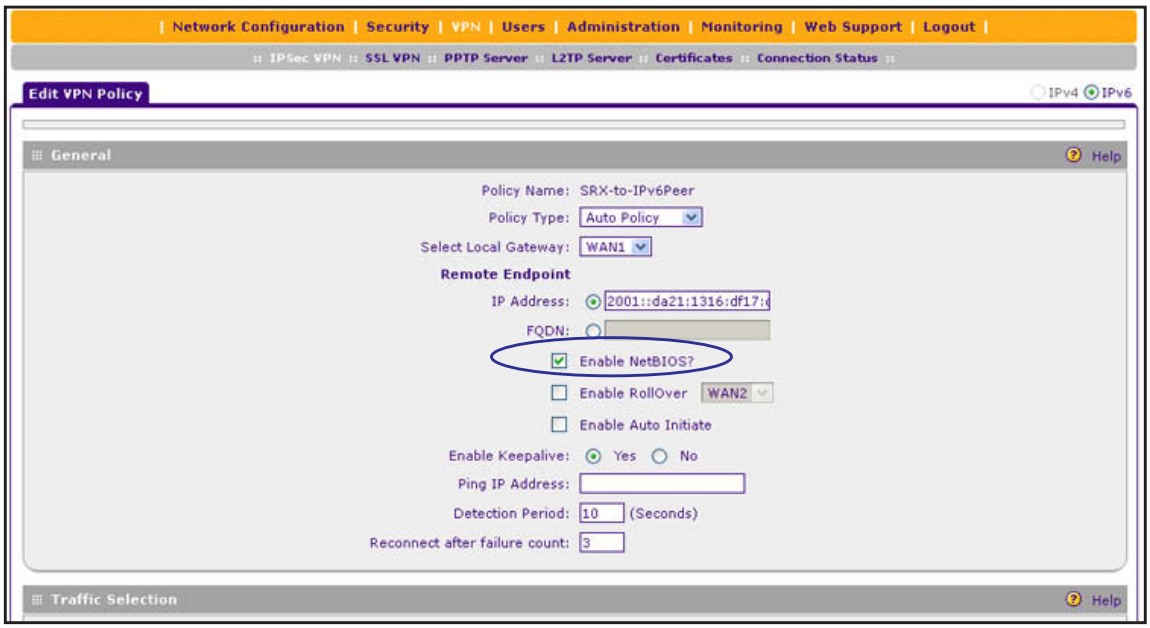

Figure 178.

4. Select the **Enable NetBIOS?** check box.
5. Click **Apply** to save your settings.

Configure the PPTP Server

As an alternate solution to IPSec VPN and L2TP tunnels, you can configure a Point-to-Point Tunnel Protocol (PPTP) server on the VPN firewall to allow users to access PPTP clients over PPTP tunnels. A maximum of 25 simultaneous PPTP user sessions are supported. (The very first IP address of the PPTP address pool is used for distribution to the VPN firewall.)

A PPTP user typically initiates a tunnel request; the PPTP server accommodates the tunnel request and assigns an IP address to the user. After a PPTP tunnel is established, the user can connect to a PPTP client that is located behind the VPN firewall.

You need to enable the PPTP server on the VPN firewall, specify a PPTP server address pool, and create PPTP user accounts. (PPTP users are authenticated through local authentication with geardomain.) For information about how to create PPTP user accounts, see *Configure User Accounts* on page 310.

➢ **To enable the PPTP server and configure the PPTP server pool, authentication, and encryption:**

1. Select **VPN > PPTP Server**. The PPTP Server screen displays. (The following figure contains an example.)

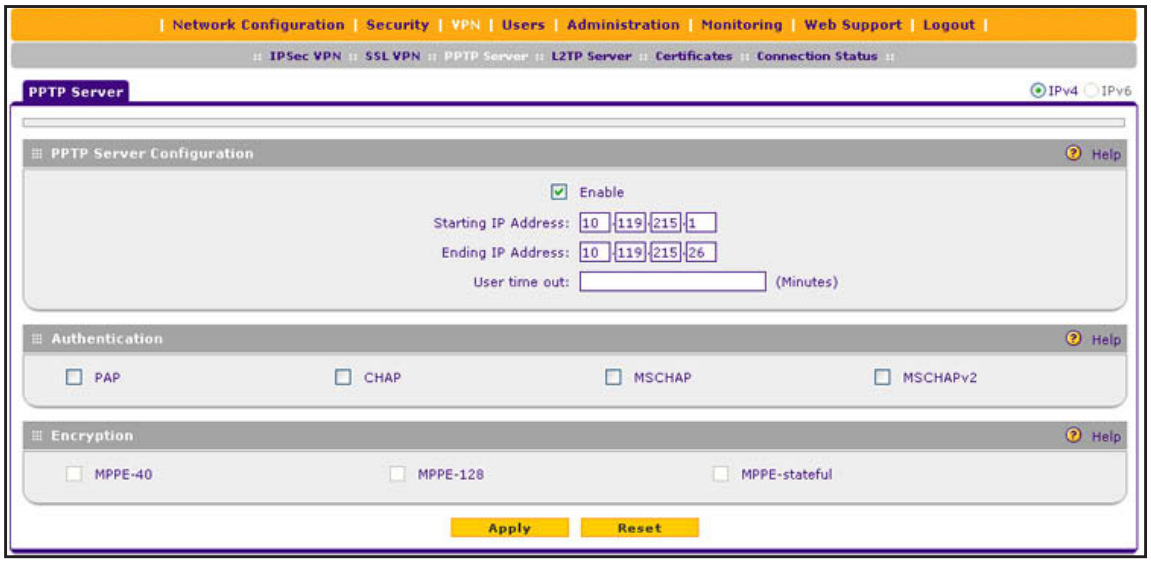

Figure 179.

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

Table 66. PPTP Server screen settings

Setting	Description
PPTP Server	
Enable	To enable the PPTP server, select the **Enable** check box.
Start IP Address	Type the first IP address of the address pool.
End IP Address	Type the last IP address of the address pool. A maximum of 26 contiguous addresses can be part of the pool. (The first address of the pool cannot be assigned to a user.)
User time out	Enter the time-out period in seconds, from 0 to 999 seconds. The default is 0 seconds. If there is no traffic from a user, the connection is disconnected after the specified period.
Authentication	
Select one or more of the following authentication methods to authenticate PPTP users: • **PAP**. RADIUS-Password Authentication Protocol (PAP). • **CHAP**. RADIUS-Challenge Handshake Authentication Protocol (CHAP). • **MSCHAP**. RADIUS-Microsoft CHAP (MSCHAP). • **MSCHAPv2**. RADIUS-Microsoft CHAP version 2 (MSCHAPv2).	

Table 66. PPTP Server screen settings (continued)

Setting	Description
Encryption	
If the authentication is MSCHAP or MSCHAPv2, the PPTP server can support Microsoft Point-to-Point Encryption (MPPE). Select one or more of the following types of MPPE: • **MPPE-40**. MPPE 40-bit encryption. • **MPPE-128**. MPPE 128-bit encryption. This is the most secure type of MPPE encryption. • **MPPE-stateful**. Stateful MPPE encryption. This is the least secure type of MPPE encryption.	

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

View the Active PPTP Users

➢ **To view the active PPTP tunnel users:**

Select **Monitoring > Active Users & VPNs > PPTP Active Users**. The PPTP Active Users screen displays. (The following figure does not show any active users.)

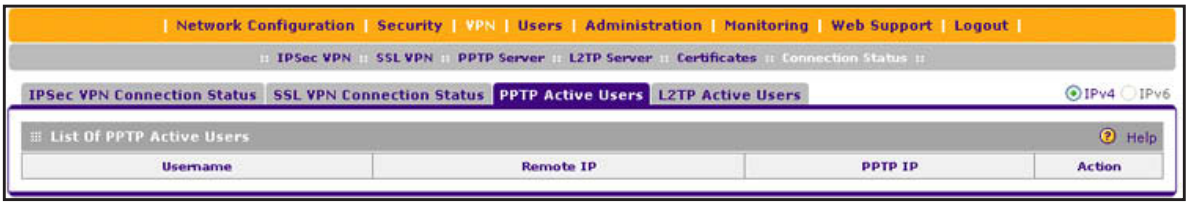

Figure 180.

The List of PPTP Active Users table lists each active connection with the information that is described in the following table.

Table 67. PPTP Active Users screen information

Item	Description
Username	The name of the PPTP user that you have defined (see *Configure User Accounts* on page 310).
Remote IP	The remote client's IP address.
PPTP IP	The IP address that is assigned by the PPTP server on the VPN firewall.
Action	Click the **Disconnect** table button to terminate the connection. (This button is displayed only when there an active connection.)

The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and click the **Set Interval** button. To stop polling, click the **Stop** button.

Configure the L2TP Server

As an alternate solution to IPSec VPN tunnels, you can configure a Layer 2 Tunneling Protocol (L2TP) server on the VPN firewall to allow users to access L2TP clients over L2TP tunnels. A maximum of 25 simultaneous L2TP user sessions are supported. (The very first IP address of the L2TP address pool is used for distribution to the VPN firewall.)

An L2TP Access Concentrator (LAC) typically initiates a tunnel to fulfill a connection request from an L2TP user; the L2TP server accommodates the tunnel request. After an L2TP tunnel is established, the L2TP user can connect to an L2TP client that is located behind the VPN firewall.

Note: IPSec VPN provides stronger authentication and encryption than L2TP. (Packets that traverse the L2TP tunnel are not encapsulated by IPSec.)

You need to enable the L2TP server on the VPN firewall, specify an L2TP server address pool, and create L2TP user accounts. (L2TP users are authenticated through local authentication with geardomain.) For information about how to create L2TP user accounts, see *Configure User Accounts* on page 310.

➢ **To enable the L2TP server and configure the L2TP server pool:**

1. Select **VPN > L2TP Server**. The L2TP Server screen displays. (The following figure contains an example.)

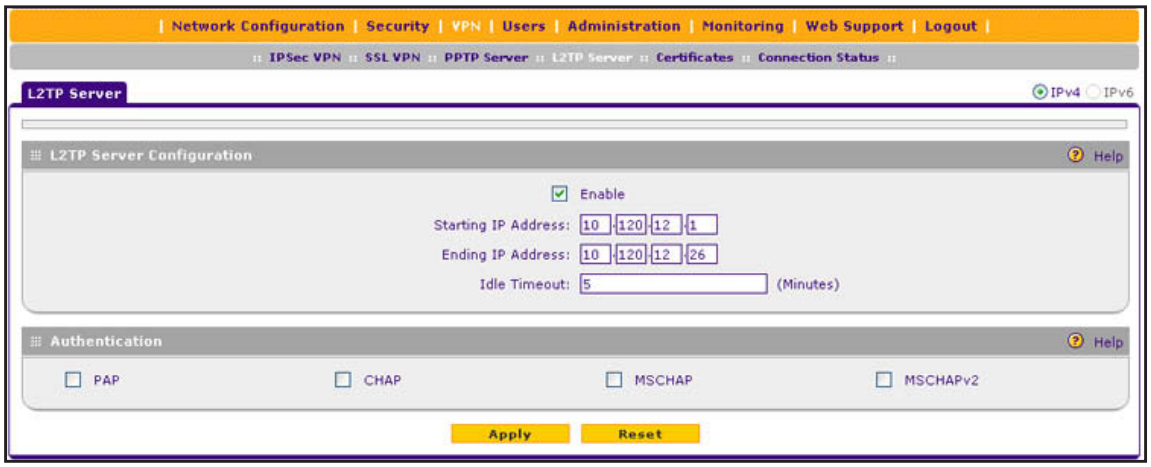

Figure 181.

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

Table 68. L2TP Server screen settings

Setting	Description
L2TP Server Configuration	
Enable	To enable the L2TP server, select the **Enable** check box.
Starting IP Address	The first IP address of the pool. This address is used for distribution to the VPN firewall.
Ending IP Address	The last IP address of the pool. A maximum of 26 contiguous addresses is supported. (The first address of the pool cannot be assigned to a user.)
Idle Timeout	The period after which an idle user is automatically logged out of the L2TP server. The default idle time-out period is 5 minutes.
Authentication	
Select one or more of the following authentication methods to authenticate L2TP users: • **PAP**. RADIUS-Password Authentication Protocol (PAP). • **CHAP**. RADIUS-Challenge Handshake Authentication Protocol (CHAP). • **MSCHAP**. RADIUS-Microsoft CHAP (MSCHAP). • **MSCHAPv2**. RADIUS-Microsoft CHAP version 2 (MSCHAPv2).	

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

View the Active L2TP Users

To view the active L2TP tunnel users, select **VPN > Connection Status > L2TP Active Users**. The L2TP Active Users screen displays. (The following figure does not show any active users.)

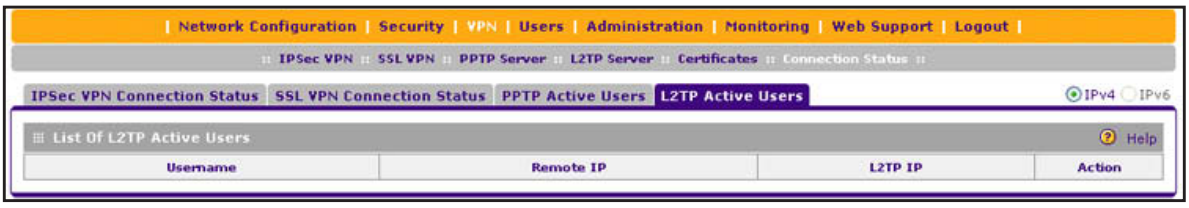

Figure 182.

The List of L2TP Active Users table lists each active connection with the information that is described in the following table.

Table 69. L2TP Active Users screen information

Item	Description
Username	The name of the L2TP user that you have defined (see *Configure User Accounts* on page 310).
Remote IP	The client's IP address on the remote L2TP Access Concentrator (LAC).

Table 69. L2TP Active Users screen information (continued)

Item	Description
L2TP IP	The IP address that is assigned by the L2TP server on the VPN firewall.
Action	Click the **Disconnect** table button to terminate the L2TP connection.

Virtual Private Networking Using SSL Connections

6

The VPN firewall provides a hardware-based SSL VPN solution designed specifically to provide remote access for mobile users to their corporate resources, bypassing the need for a preinstalled VPN client on their computers. Using the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, the VPN firewall can authenticate itself to an SSL-enabled client, such as a standard web browser. Once the authentication and negotiation of encryption information are completed, the server and client can establish an encrypted connection. With support for up to five dedicated SSL VPN tunnels, the VPN firewall allows users to easily access the remote network for a customizable, secure, user portal experience from virtually any available platform.

This chapter contains the following sections:

SSL VPN Portal Options

The VPN firewall's SSL VPN portal can provide two levels of SSL service to the remote user:

- **SSL VPN tunnel**. The VPN firewall 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 VPN firewall. Upon successful connection, an ActiveX-based SSL VPN client is downloaded to the remote computer 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 VPN firewall, and a virtual network interface is created on the user's computer. The VPN firewall assigns the computer an IP address and DNS server IP addresses, allowing the remote computer to access network resources in the same manner as if it were connected directly to the corporate network, subject to any policy restrictions that you configure.

- **SSL port forwarding**. Like an SSL VPN tunnel, port forwarding is a web-based client that is installed transparently and then creates a virtual, encrypted tunnel to the remote network. However, port forwarding differs from an SSL VPN tunnel in several ways:
  - Port forwarding supports only TCP connections, not UDP connections, or connections using other IP protocols.
  - Port forwarding detects and reroutes individual data streams on the user's computer 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.

Overview of the SSL Configuration Process

To configure and activate SSL connections, perform the following six basic steps in the order that they are presented:

1. create an SSL portal (see *Create the Portal Layout* on page 277).

   When remote users log in to the VPN firewall, they see a portal page that you can customize to present the resources and functions that you choose to make available.

2. Create authentication domains, user groups, and user accounts (see *Configure Domains, Groups, and Users* on page 281).)

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

      When remote users log in to the VPN firewall, they need to specify a domain to which their login account belongs. The domain determines the authentication method that is used and the portal layout that is presented, which in turn determines the network

resources to which the users are granted access. Because you need to assign a portal layout when creating a domain, the domain is created after you have created the portal layout.

b. Create one or more groups for your SSL VPN users.

When you define the SSL VPN policies that determine network resource access for your SSL VPN users, you can define global policies, group policies, or individual policies. Because you need to assign an authentication domain when creating a group, the group is created after you have created the domain.

c. Create one or more SSL VPN user accounts.

Because you need to assign a group when creating an SSL VPN user account, the user account is created after you have created the group.

3. For port forwarding, define the servers and services (see *Configure Applications for Port Forwarding* on page 282).

   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 VPN firewall resolves the names to the servers using the list you have created.

4. For SSL VPN tunnel service, configure the virtual network adapter (see *Configure the SSL VPN Client* on page 284).

   For the SSL VPN tunnel option, the VPN firewall creates a virtual network adapter on the remote computer that then functions as if it were on the local network. Configure the portal's SSL VPN client to define a pool of local IP addresses to be issued to remote clients, as well as DNS addresses. Declare static routes or grant full access to the local network, subject to additional policies.

5. To simplify policies, define network resource objects (see *Use Network Resource Objects to Simplify Policies* on page 288).

   Network resource objects are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies.

6. Configure the SSL VPN policies (see *Configure User, Group, and Global Policies* on page 291).

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

Create the Portal Layout

The Portal Layouts screen that you can access from the SSL VPN configuration menu allows you to create a custom screen that remote users see when they log in to the portal. Because the log-in screen is 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 log-in screen is also suited as a starting screen for restricted users; if mobile users or business partners are permitted to access only a few resources, the log-in screen that you create presents only the resources that are relevant to these users.

You apply portal layouts by selecting one from the available portal layouts in the configuration of a domain. When you have completed your portal layout, you can apply the portal layout to one or more authentication domains (see *Configure Domains* on page 303). You can also make the new portal the default portal for the SSL VPN gateway by selecting the default radio button next to the portal layout name.

The VPN firewall's default portal address is https://<IP_address>/portal/SSL-VPN, in which the IP address can be either an IPv4 or an IPv6 address. Both types of addresses are supported simultaneously. The default domain geardomain is assigned to the default SSL-VPN portal.

You can define individual layouts for the SSL VPN portal. The layout configuration includes the menu layout, theme, portal pages to display, and web cache control options. The default portal layout is the SSL-VPN portal. You can add additional portal layouts. You can also make any portal the default portal for the VPN firewall by clicking the **Default** button in the Action column of the List of Layouts table, to the right of the desired portal layout.

➢ **To create an SSL VPN portal layout:**

1. Select **VPN > SSL VPN > Portal Layouts**. The Portal Layouts screen displays the IPv4 settings. (The following figure shows an additional layout in the List of Layouts table as an example.)
2. Specify the IP version for which you want to add a portal layout:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.

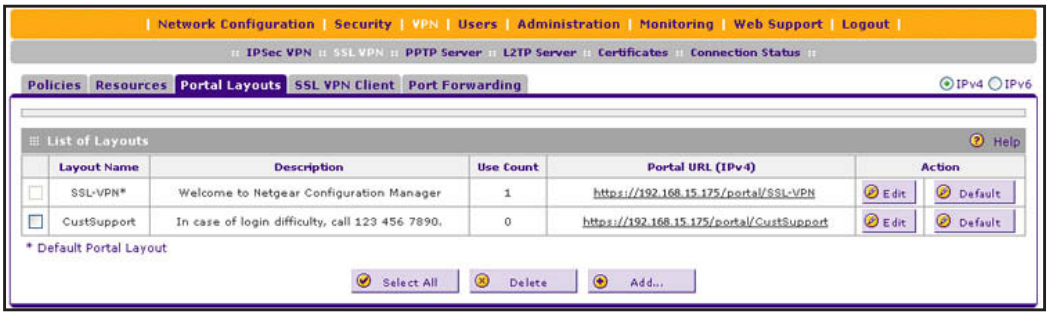

Figure 183. Portal Layouts screen for IPv4

   - **IPv6**. Select the **IPv6** radio button. The Portal Layouts screen displays the IPv6 settings. (The following figure shows an additional layout in the List of Layouts table as an example.)

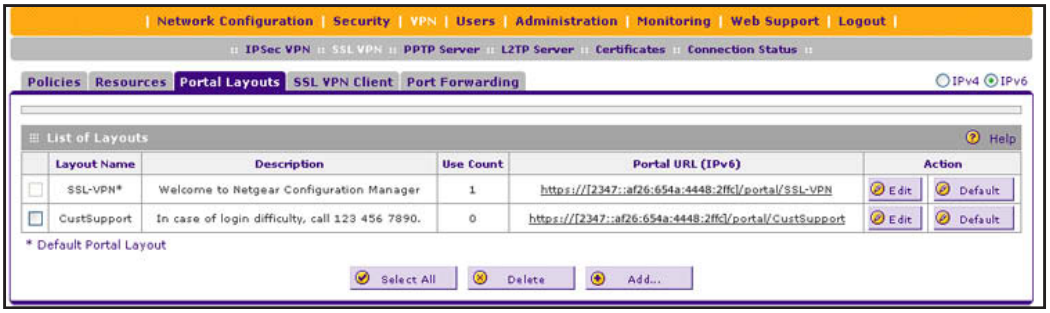

Figure 184. Portal Layouts screen for IPv6

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 196* on page 298).
- **Use Count**. The number of authentication domains that use the portal.
- **Portal URL:**
  - **Portal URL (IPv4)**. The IPv4 URL at which the portal can be accessed. The IPv4 address in the URL is the public WAN address of the VPN firewall (see *Configure the IPv4 Internet Connection and WAN Settings* on page 29). Both the IPv4 URL and the IPv6 URL can be active simultaneously.
  - **Portal URL (IPv6)**. The IPv6 URL at which the portal can be accessed. The IPv6 address in the URL is the public WAN address of the VPN firewall (see *Configure the IPv6 Internet Connection and WAN Settings* on page 52). Both the IPv6 URL and the IPv4 URL can be active simultaneously.
- **Action**. The table buttons, which allow you to edit the portal layout or set it as the default.

3. Under the List of Layouts table, click the **Add** table button. The Add Portal Layout screen displays. (The following figure shows an example.)

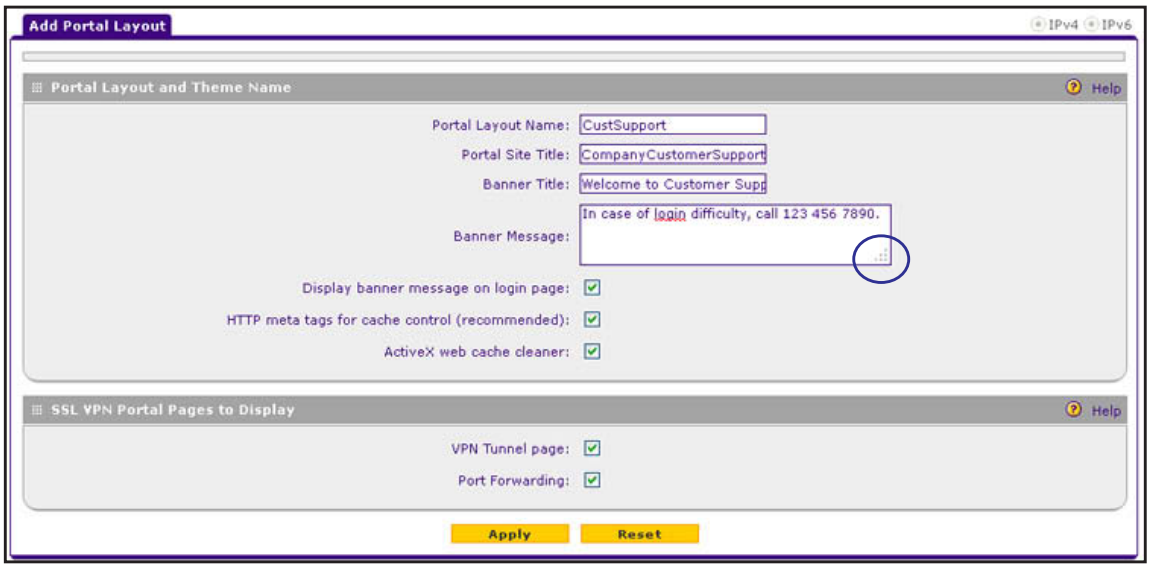

Figure 185.

4. Complete the settings as described in the following table:

Table 70. Add Portal Layout screen settings

Setting	Description
Portal Layout and Theme Name	
Portal Layout Name	A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL. **Note:** Custom portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at https://vpn.company.com, and you create a portal layout named CustomerSupport, users access the website at https://vpn.company.com/portal/CustomerSupport. **Note:** Only alphanumeric characters, hyphens (-), and underscores (_) are accepted in the Portal Layout Name field. If you enter other types of characters or spaces, the layout name is truncated before the first nonalphanumeric character. **Note:** Unlike most other URLs, this name is case-sensitive.
Portal Site Title	The title that displays at the top of the user's web browser window, for example, *Company Customer Support*.
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 196* on page 298. The banner title text is displayed in the orange header bar.
Banner Message	The text of a banner message that users see before they log in to the portal, for example, *In case of login difficulty, call 123-456-7890*. Enter a plain text message, or include HTML and JavaScript tags. The maximum length of the login screen message is 4096 characters. **Note:** You can enlarge the field (that is, the text box) by manipulating the lower right corner of the field (see the blue circle in the previous figure). **Note:** For an example, see *Figure 196* on page 298. The banner message text is displayed in the gray header bar.
Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen as shown in *Figure 196* on page 298.
HTTP meta tags for cache control (recommended)	Select this check box to apply cache control directives for the HTTP meta tags to this portal layout. Cache control directives include: <meta http-equiv="pragma" content="no-cache"> <meta http-equiv="cache-control" content="no-cache"> <meta http-equiv="cache-control" content="must-revalidate"> **Note:** NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user's web browser cache.

Table 70. Add Portal Layout screen settings (continued)

Setting	Description
ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to delete all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. The ActiveX web cache control is ignored by web browsers that do not support ActiveX.
SSL VPN Portal Pages to Display	
VPN Tunnel page	To provide full network connectivity, select this check box.
Port Forwarding	To specific defined network services, select this check box to provide access. **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. For information about how to display the new portal layout, see *Access the New SSL Portal Login Screen* on page 297.

➢ **To edit a portal layout:**

1. On the Portal Layouts screen (for IPv4, see *Figure 183* on page 278; for IPv6, see *Figure 184* on page 278), click the **Edit** button in the Action column for the portal layout that you want to modify. The Edit Portal Layout screen displays. This screen is identical to the Add Portal Layout screen (see the previous figure).
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more portal layouts:**

1. On the Portal Layouts screen (for IPv4, see *Figure 183* on page 278; for IPv6, see *Figure 184* on page 278), select the check box to the left of each portal layout that you want to delete, or click the **Select All** table button to select all layouts. (You cannot delete the SSL-VPN default portal layout.)
2. Click the **Delete** table button.

Configure Domains, Groups, and Users

Remote users connecting to the VPN firewall through an SSL VPN portal need to be authenticated before they are granted access to the network. The login screen that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines both the authentication method and the portal layout that are used.

You need to create name and password accounts for the SSL VPN users. When you create a user account, you need to specify a group. Groups are used to simplify the application of access policies. When you create a group, you need to specify a domain. Therefore, you should create any domains first, then groups, and then user accounts.

For information about how to configure domains, groups, and users, see *Configure Authentication Domains, Groups, and Users* on page 303.

Configure Applications for Port Forwarding

Port forwarding provides access to specific defined network services. To define these services, you need to specify the internal server addresses and port numbers for TCP applications that are intercepted by the port forwarding client on the user's computer. This client reroutes the traffic to the VPN firewall.

Note: SSL VPN port forwarding is supported for IPv4 connections only.

Add Servers and Port Numbers

To configure port forwarding, you need to define the IP addresses of the internal servers and the port number for TCP applications that are available to remote users.

➢ **To add a server and a port number:**

1. Select **VPN > SSL VPN > Port Forwarding**. The Port Forwarding screen displays. (The following figure shows an example.)

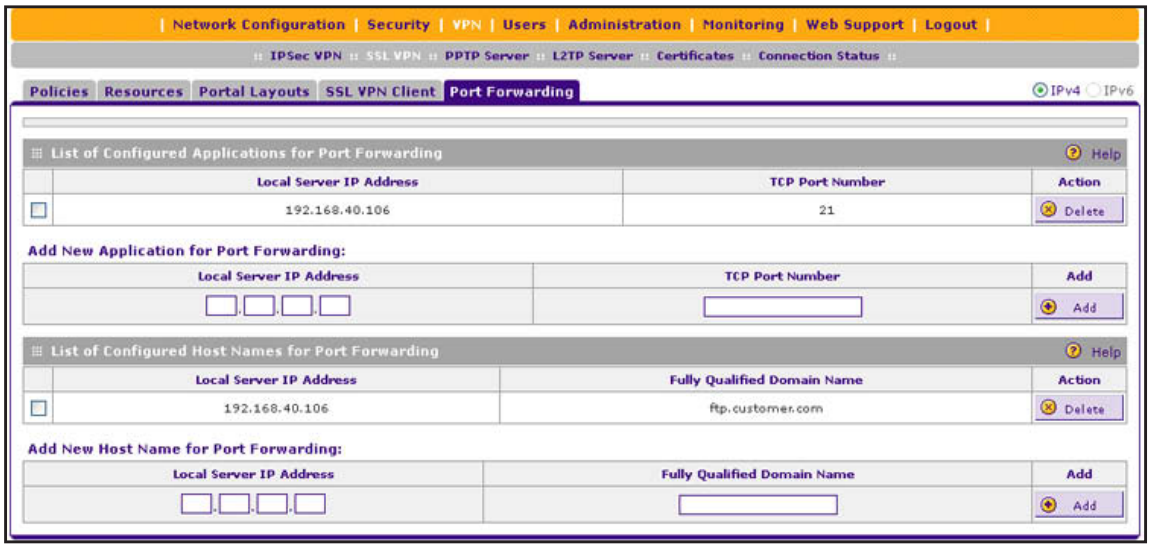

Figure 186.

2. In the Add New Application for Port Forwarding section of the screen, specify information in the following fields:
   - **IP Address**. The IP address of an internal server or host computer that a remote user has access to.
   - **TCP Port**. The TCP port number of the application that is accessed through the SSL VPN tunnel. The following table lists some commonly used TCP applications and port numbers.

Table 71. Port forwarding applications/TCP port numbers

TCP Application	Port Number
FTP data (usually not needed)	20
FTP Control Protocol	21
SSH	22[a]
Telnet	23[a]
SMTP (send mail)	25
HTTP (web)	80
POP3 (receive mail)	110
NTP (Network Time Protocol)	123
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

a. Users can specify the port number together with the host name or IP address.

3. Click the **Add** table button. The new application entry is added to the List of Configured Applications for Port Forwarding table. Remote users can now securely access network applications once they have logged in to the SSL VPN portal and launched port forwarding.

➢ **To delete an application from the List of Configured Applications for Port Forwarding table:**

1. Select the check box to the left of the application that you want to delete.
2. Click the **Delete** table button in the Action column.

Add a New Host Name

After you have configured port forwarding by defining the IP addresses of the internal servers and the port number for TCP applications that are available to remote users, you then can also specify host-name-to-IP-address resolution for the network servers as a convenience for users. Host name resolution allows users to access TCP applications at familiar addresses such as mail.*example*.com or ftp.*customer*.com rather than by IP addresses.

➢ **To add servers and host names for client name resolution:**

1. Select **VPN > SSL VPN > Port Forwarding**. The Port Forwarding screen displays (see *Figure 186* on page 282).
2. In the Add New Host Name for Port Forwarding section of the screen, specify information in the following fields:
   - **Local Server IP Address**. The IP address of an internal server or host computer that you want to name.
   - **Fully Qualified Domain Name**. The full server name.

Note: If the server or host computer that you want to name does not display in the List of Configured Applications for Port Forwarding table, you need to add it before you can rename it.

3. Click the **Add** table button. The new application entry is added to the List of Configured Host Names for Port Forwarding table.

➢ **To delete a name from the List of Configured Host Names for Port Forwarding table:**

1. Select the check box to the left of the name that you want to delete.
2. Click the **Delete** table button in the Action column.

Configure the SSL VPN Client

- *Configure the Client IP Address Range*
- *Add Routes for VPN Tunnel Clients*

The SSL VPN client on the VPN firewall 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 assigned to devices on the local network, 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 VPN firewall. (For example, if your computer has a network interface IP address of 10.0.0.45, you cannot contact a server on the remote network that also has the IP address 10.0.0.45.)

- Select whether you want to enable full-tunnel or split-tunnel support based on your bandwidth:
  - A full tunnel sends all of the client's traffic across the VPN tunnel.
  - A split tunnel sends only traffic that is destined for the local network based on the specified client routes. All other traffic is sent to the Internet. A split tunnel allows you to manage bandwidth by reserving the VPN tunnel for local traffic only.
- If you enable split-tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you need to add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel.

Configure the Client IP Address Range

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

➢ **To define the client IP address range:**

1. Select **VPN > SSL VPN > SSL VPN Client**. The SSL VPN Client screen displays the IPv4 settings (the following screen shows some examples).
2. Specify the IP version for which you want to configure the SSL VPN client:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.

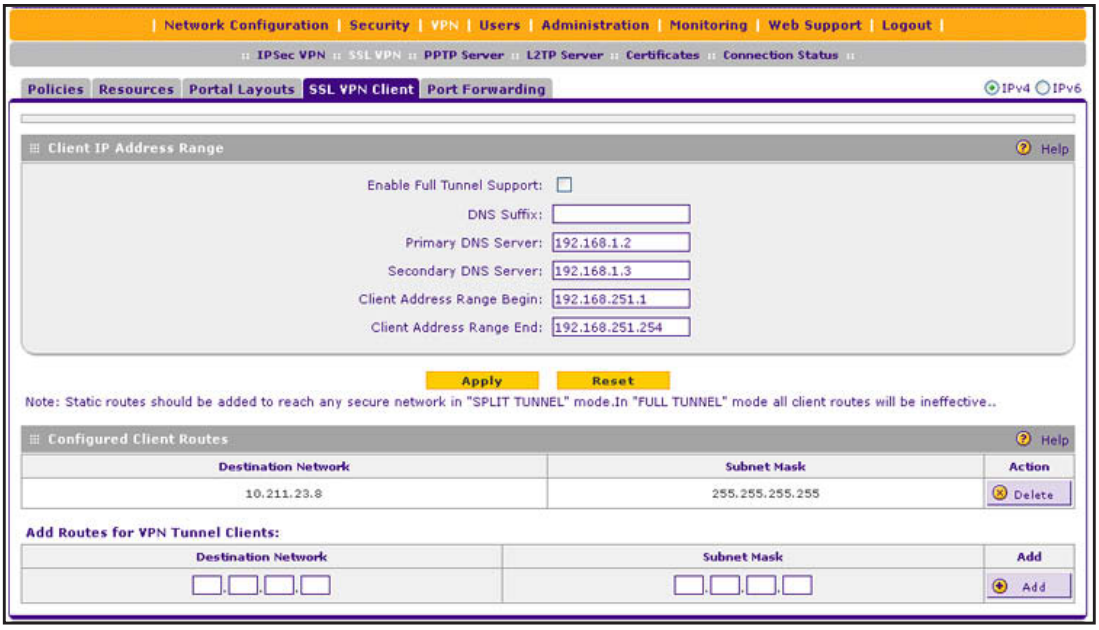

Figure 187. SSL VPN Client screen for IPv4

   - **IPv6**. Select the **IPv6** radio button. The SSL VPN Client screen displays the IPv6 settings (the following screen shows some examples).

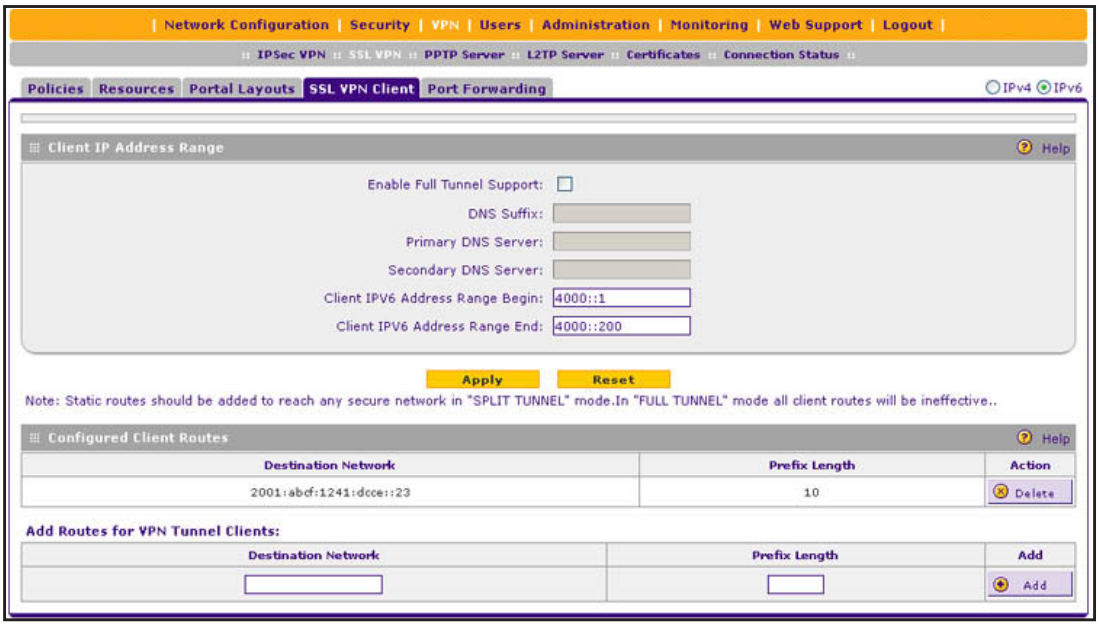

Figure 188. SSL VPN Client screen for IPv6

3. Complete the settings as described in the following table:

Table 72. SSL VPN Client screen settings for IPv4 and IPv6

Setting	Description	
Client IP Address Range		
Enable Full Tunnel Support	Select this check box to enable full-tunnel support. If you leave this check box cleared (which is the default setting), full-tunnel support is disabled but split-tunnel support is enabled, and you need to add client routes (see *Add Routes for VPN Tunnel Clients* on page 287). **Note:** When full-tunnel support is enabled, client routes are not operable.	
IPv4 screen only	DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
	Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the SSL VPN client after a VPN tunnel has been established.
	Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.
	Client Address Range Begin	The first IP address of the IPv4 address range that you want to assign to the VPN tunnel clients. By default, the first IPv4 address is 192.168.251.1.

Table 72. SSL VPN Client screen settings for IPv4 and IPv6 (continued)

Setting	Description	
IPv4 screen only (continued)	Client Address Range End	The last IP address of the IPv4 address range that you want to assign to the VPN tunnel clients. By default, the last IPv4 address is 192.168.251.254.
IPv6 screen only	Client IPv6 Address Range Begin	The first IP address of the IPv6 address range that you want to assign to the VPN tunnel clients. By default, the first IPv6 address is 4000::1.
	Client IPv6 Address Range End	The last IP address of the IPv6 address range that you want to assign to the VPN tunnel clients. By default, the last IPv6 address is 4000::200.

4. Click **Apply** to save your settings. VPN tunnel clients are now able to connect to the VPN firewall and receive a virtual IP address in the client address range.

Add Routes for VPN Tunnel Clients

The VPN tunnel clients assume that the following networks are located across the VPN-over-SSL tunnel:

- The subnet that contains the client IP address (that is, PPP interface), as determined by the class of the address (Class A, B, or C).
- Subnets that are specified in the Configured Client Routes table on the SSL VPN Client screen.

If the assigned client IP address range is in a different subnet from the local network, or if the local network has multiple subnets, or if you select split-tunnel operation, you need to define client routes.

➢ **To add an SSL VPN tunnel client route:**

1. Select **VPN > SSL VPN > SSL VPN Client**. The SSL VPN Client screen for IPv4 displays (see *Figure 187* on page 285).
2. Specify the IP version for which you want to add a route:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.
   - **IPv6**. Select the **IPv6** radio button. The SSL VPN Client screen displays the IPv6 settings (see *Figure 188* on page 286).
3. In the Add Routes for VPN Tunnel Clients section of the screen, specify information in the following fields:
   - **Destination Network**. The destination network IPv4 or IPv6 address of a local network or subnet. For example, for an IPv4 route, enter 10.211.23.8.
   - **Subnet Mask / Prefix Length**. For an IPv4 route, the address of the appropriate subnet mask; for an IPv6 route, the prefix length.
4. Click the **Add** table button. The new client route is added to the Configured Client Routes table.

If VPN tunnel clients are already connected, disconnect and then reconnect the clients on the SSL VPN Connection Status screen (see *View the SSL VPN Connection Status and SSL VPN Log* on page 299). Doing so allows the clients to 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, you can delete it.

Use Network Resource Objects to Simplify Policies

- *Add New Network Resources*
- *Edit Network Resources to Specify Addresses*

Network resources are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies. You do not need to redefine the same set of IP addresses or address ranges when you configure the same access policies for multiple users.

Defining network resources is optional; smaller organizations can choose to create access policies using individual IP addresses or IP networks rather than predefined network resources. But for most organizations, NETGEAR recommends that you use network resources. If your server or network configuration changes, you can perform an update quickly by using network resources instead of individually updating all of the user and group policies.

Add New Network Resources

The resource name and service are independent of the IP version. However, the resource definition (see *Edit Network Resources to Specify Addresses* on page 289) is dependent on the IP version because you can assign either an IPv4 or an IPv6 address or network.

➢ **To define a network resource:**

1. Select **VPN > SSL VPN > Resources**. The Resources screen displays. (The following figure shows some resources in the List of Resources table as an example.)

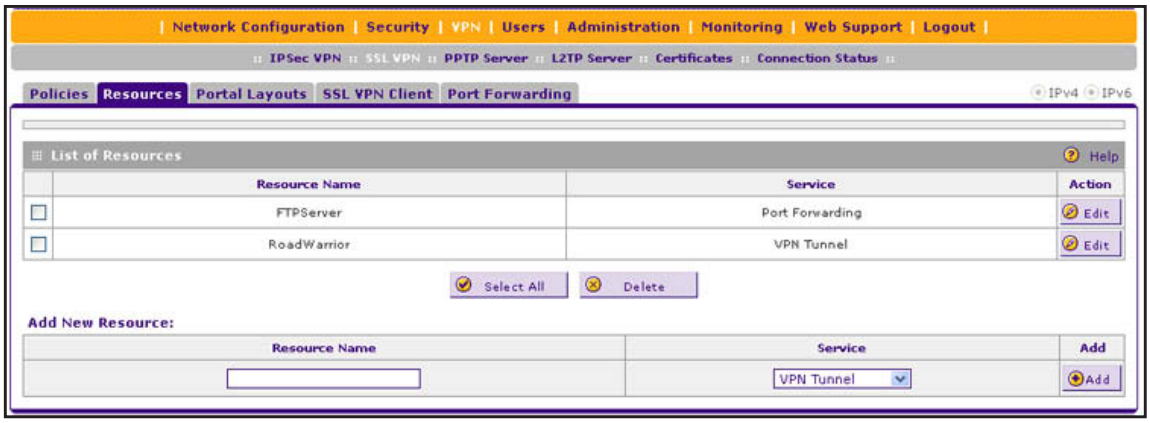

Figure 189.

2. In the Add New Resource section of the screen, specify information in the following fields:
   - **Resource Name**. A descriptive name of the resource for identification and management purposes.
   - **Service**. From the Service drop-down list, select the type of service to which the resource applies:
     - **VPN Tunnel**. The resource applies only to a VPN tunnel.
     - **Port Forwarding**. The resource applies only to port forwarding.
     - **All**. The resource applies both to a VPN tunnel and to port forwarding.
3. Click the **Add** table button. The new resource is added to the List of Resources table.

➢ **To delete one or more network resources:**

1. Select the check box to the left of each network resource that you want to delete, or click the **Select All** table button to select all network resources.
2. Click the **Delete** table button.

Edit Network Resources to Specify Addresses

➢ **To edit network resources:**

1. Select **VPN > SSL VPN > Resources**. The Resources screen displays (see the previous figure, which shows some examples).
2. In the List of Resources table, to the right of the new resource in the Action column, click the **Edit** table button. A new screen that lets you edit the resource displays the IPv4 settings. (The following figure shows some examples.)
3. Specify the IP version for which you want to add a portal layout:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 4*.
   - **IPv6**. Select the **IPv6** radio button. The screen that lets you edit the resource displays the IPv6 settings. Except for the Mask Length, which is Prefix Length on the screen for IPv6, this screen is identical to the screen for IPv4 (see the next figure, which shows some examples).

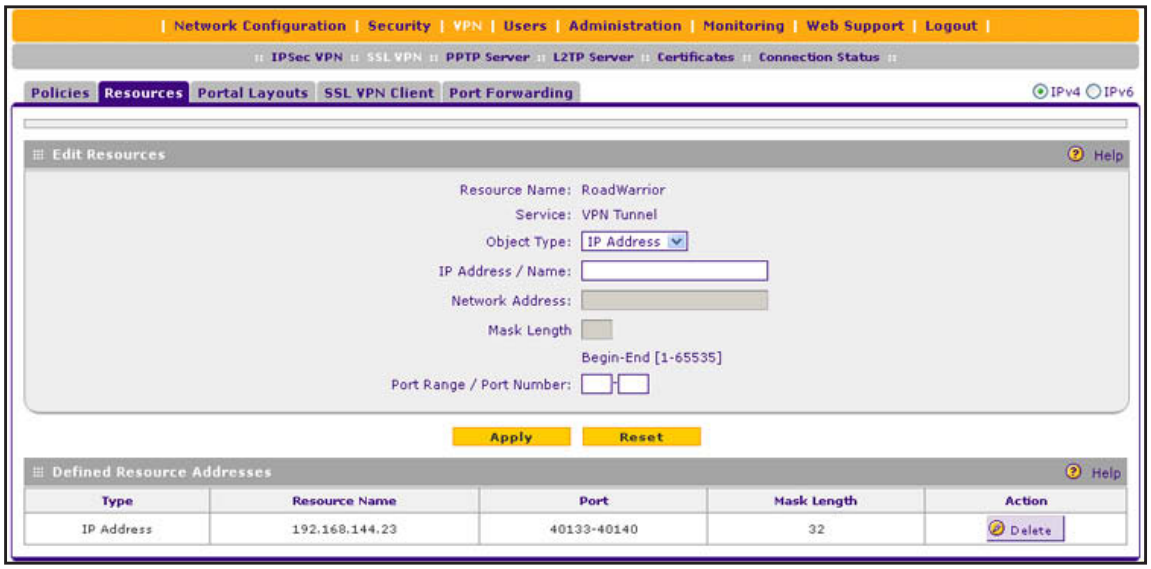

Figure 190.

4. Complete the settings as described in the following table:

Table 73. Resources screen settings to edit a resource

Setting	Description	
Add Resource Addresses		
Resource Name	The unique identifier for the resource. You cannot modify the resource name after you have created it on the first Resources screen.	
Service	The SSL service that is assigned to the resource. You cannot modify the service after you have assigned it to the resource on the first Resources screen.	
Object Type	From the drop-down list, select one of the following options: • **IP Address**. The object is an IPv4 or IPv6 address. You need to enter the IP address or the FQDN in the IP Address / Name field. • **IP Network**. The object is an IPv4 or IPv6 network. You need to enter the network IP and the network mask length (for IPv4) or prefix length (for IPv6) 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. You also need to enter the mask length (IPv4 only) or prefix length (IPv6 only):

Table 73. Resources screen settings to edit a resource (continued)

Setting	Description	
Object Type (continued)	IPv4 screen only: Mask Length	Enter the network mask (0–31) for the locations that are permitted to use this resource.
	IPv6 screen only: Prefix Length	Enter the prefix length 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.

Configure User, Group, and Global Policies

You can define and apply user, group, and global policies to predefined network resource objects, IP addresses, address ranges, or all IP addresses, and to different SSL VPN services. A specific hierarchy is invoked over which policies take precedence. The VPN firewall policy hierarchy is defined as follows:

- User policies take precedence over group policies.
- Group policies take precedence over global policies.
- If two or more user, group, or global policies are configured, the *most specific* policy takes precedence.

For example, a policy that is configured for a single IP address takes precedence over a policy that is configured for a range of addresses. And a policy that applies to a range of IP addresses takes precedence over a policy that is applied to all IP addresses. If two or more IP address ranges are configured, the smallest address range takes precedence. Host names are treated the same as individual IP addresses.

Network resources are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire network resource.

For example, assume the following global policy configuration:

- Policy 1. A Deny rule has been configured to block all services to the IP address range 10.0.0.0–10.0.0.255.
- Policy 2. A Deny rule has been configured to block FTP access to 10.0.1.2–10.0.1.10.
- Policy 3. A Permit rule has been configured to allow FTP access to the predefined network resource with the name FTP Servers. The FTP Servers network resource

includes the following addresses: 10.0.0.5–10.0.0.20 and the FQDN ftp.*company*.com, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies have been configured, if a user attempted to access FTP servers at the following addresses, the actions listed would occur:

- 10.0.0.1. The user would be blocked by Policy 1.
- 10.0.1.5. The user would be blocked by Policy 2.
- 10.0.0.10. The user would be granted access by Policy 3. The IP address range 10.0.0.5–10.0.0.20 is more specific than the IP address range that is defined in Policy 1.
- ftp.*company*.com. The user would be granted access by Policy 3. A single host name is more specific than the IP address range that is configured in Policy 2.

Note: The user would not be able to access ftp.*company*.com using its IP address 10.0.1.3. The VPN firewall's policy engine does not perform reverse DNS lookups.

View Policies

➢ **To view the existing SSL VPN policies:**

1. Select **VPN > SSL VPN**. The SSL VPN submenu tabs display, with the Policies screen in view. (The following figure shows some examples.)

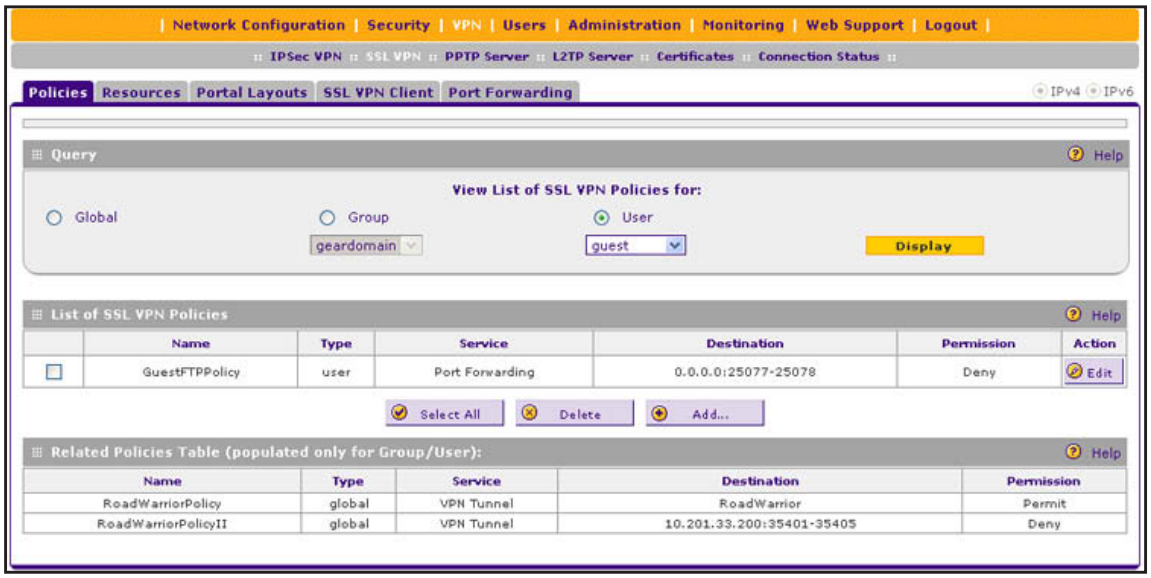

Figure 191.

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

Add an IPv4 or IPv6 SSL VPN Policy

➢ **To add an SSL VPN policy:**

1. Select **VPN > SSL VPN**. The SSL VPN submenu tabs display, with the Policies screen in view (see the previous figure).
2. Under the List of SSL VPN Policies table, click the **Add** table button. The Add SSL VPN Policy screen displays the IPv4 settings (see the next figure).
3. Specify the IP version for which you want to add an SSL VPN policy:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 4*.

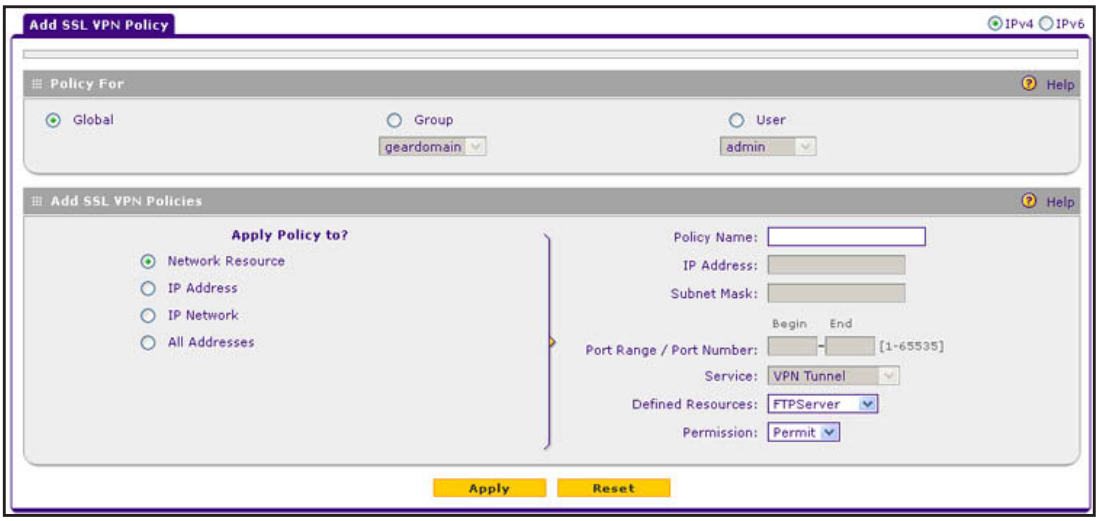

Figure 192. Add SSL VPN Policy screen for IPv4

   - **IPv6**. Select the **IPv6** radio button. The Add SSL VPN Policy screen displays the IPv6 settings:

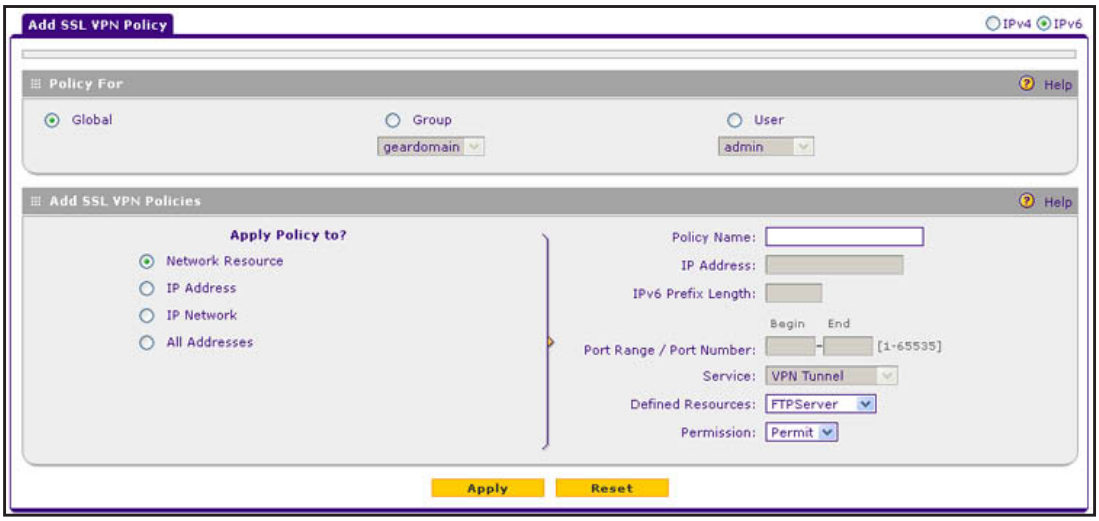

Figure 193. Add SSL VPN Policy screen for IPv6

4. Complete the settings as described in the following table:

Table 74. Add SSL VPN Policy screen settings

Setting	Description
Policy For	
Select one of the following radio buttons to specify the type of SSL VPN policy: • **Global**. The new policy is global and includes all groups and users. • **Group**. The new policy needs to be limited to a single group. From the drop-down list, select a group name. For information about how to create groups, see *Configure Groups* on page 307. • **User**. The new policy needs to be limited to a single user. From the drop-down list, select a user name. For information about how to create user accounts, see *Configure User Accounts* on page 310.	
Add SSL VPN Policies	
Apply Policy to?	Select one of the following radio buttons to specify how the policy is applied. When you select a radio button, the fields and drop-down lists that apply to your selection (see explanations later in this table) unmask onscreen. • **Network Resource**. The policy is applied to a network resource that you have defined on the Resources screen (see *Use Network Resource Objects to Simplify Policies* on page 288). • **IP Address**. The policy is applied to a single IP address. • **IP Network**. The policy is applied to a network address. • **All Addresses**. The policy is applied to all addresses.

Table 74. Add SSL VPN Policy screen settings (continued)

Setting	Description			
Apply Policy to? (continued)	Network Resource	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.	
		Defined Resources	From the drop-down list, select a network resource that you have defined on the Resources screen (see *Use Network Resource Objects to Simplify Policies* on page 288).	
		Permission	From the drop-down list, select **Permit** or **Deny** to specify whether the policy permits or denies access.	
	IP Address	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.	
		IP Address	The IPv4 or IPv6 address to which the SSL VPN policy is applied.	
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.	
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.	
		Permission	From the drop-down list, select **Permit** or **Deny** to specify whether the policy permits or denies access.	
	IP Network	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.	
		IP Address	The network IPv4 or IPv6 network address to which the SSL VPN policy is applied.	
		IPv4 screen only	Subnet Mask	The IPv4 network subnet mask to which the SSL VPN policy is applied.
		IPv6 screen only	IPv6 Prefix Length	The IPv6 prefix length that apples to the network to which the SSL VPN policy is applied.
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.	

Table 74. Add SSL VPN Policy screen settings (continued)

Setting	Description		
Apply Policy to? (continued)	IP Network (continued)	Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select **Permit** or **Deny** to specify whether the policy permits or denies access.
	All Addresses	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select **Permit** or **Deny** to specify whether the policy permits or denies access.

5. Click **Apply** to save your settings. The policy is added to the List of SSL VPN Policies table on the Policies screen. The new policy goes into effect immediately.

Note: If you have configured SSL VPN user policies, make sure that secure HTTP remote management is enabled (see *Configure Remote Management Access* on page 338). If secure HTTP remote management is not enabled, all SSL VPN user connections are disabled.

➢ **To edit an SSL VPN policy:**

1. On the Policies screen (see *Figure 191* on page 292), click the **Edit** button in the Action column for the SSL VPN policy that you want to modify. The Edit SSL VPN Policy screen displays. This screen is identical to the Add SSL VPN Policy screen (see the previous figure).
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more SSL VPN policies:**

1. On the Policies screen (see *Figure 191* on page 292), select the check box to the left of each SSL VPN policy that you want to delete, or click the **Select All** table button to select all policies.
2. Click the **Delete** table button.

Access 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 in the upper right of the screen, above the menu bars (User Portal).

When you click the **User Portal** link, the SSL VPN default portal opens (see *Figure 197* on page 298). This user portal is not the same as the new SSL portal login screen that you defined in *Create the Portal Layout* on page 277.

➢ **To open the new SSL portal login screen:**

1. Select **VPN > SSL VPN > Portal Layouts**.
2. Specify the IP version for which you want to open the SSL portal login screen:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.

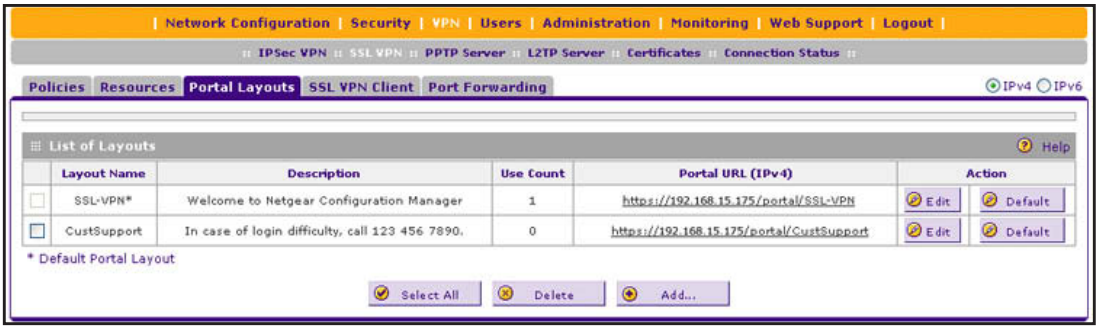

Figure 194. Portal Layouts screen for IPv4

   - **IPv6**. Select the **IPv6** radio button. The Portal Layouts screen displays the IPv6 settings. (The following figure shows an additional layout in the List of Layouts table as an example.)

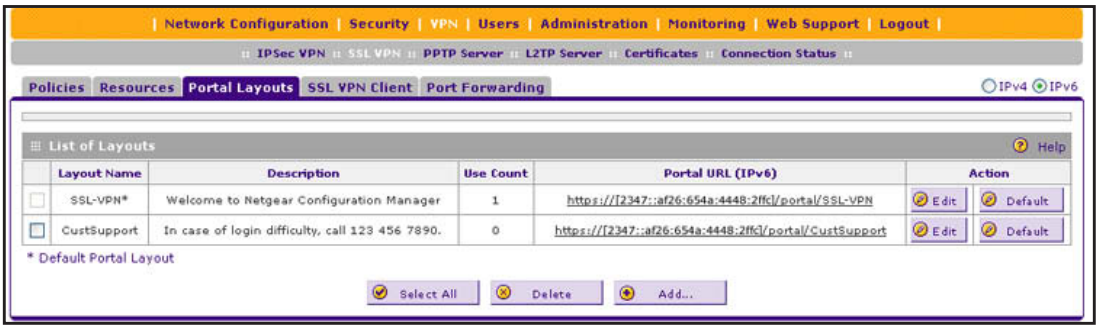

Figure 195. Portal Layouts screen for IPv6

3. In the Portal URL field of the List of Layouts table, click the URL that corresponds to the SSL portal login screen that you want to open. The SSL portal login screen displays. (The following figure shows the CustSupport layout that was defined in *Create the Portal Layout* on page 277.)

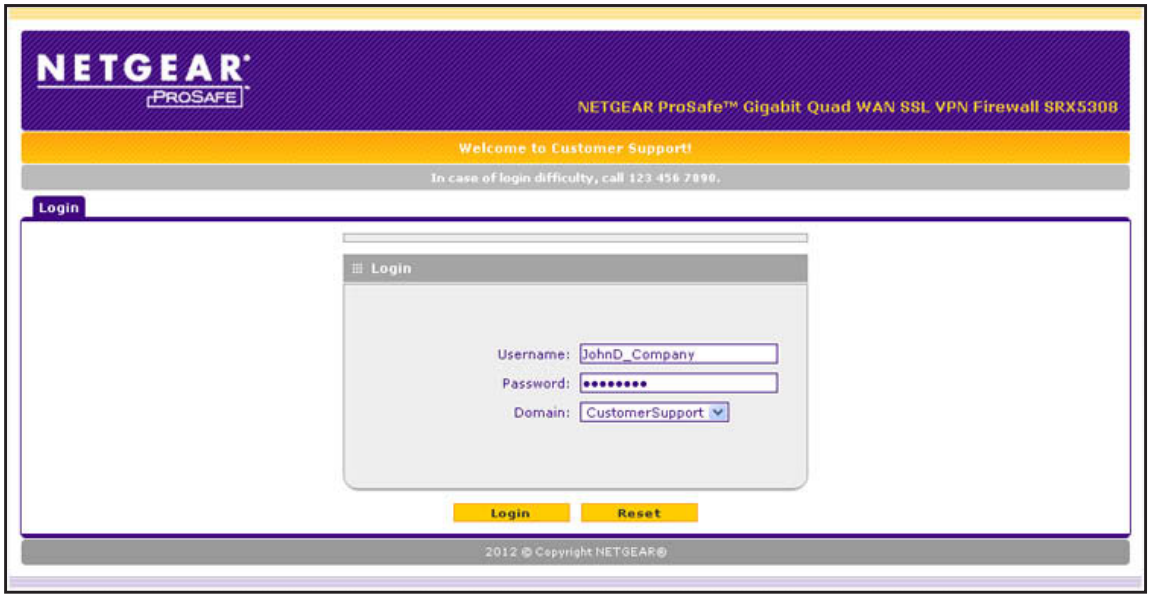

Figure 196.

4. Enter a user name and password that are associated with a domain, that, in turn, is associated with the portal. For information about creating login credentials to access a portal, see *Configure Domains, Groups, and Users* on page 281.
5. Click **Login**. The User Portal screen displays. The format of the User Portal screen depends on the settings that you selected on the Add Portal Layout screen (see *Create the Portal Layout* on page 277):
   - *Figure 197* shows the VPN Tunnel icon.
   - *Figure 198* on page 299 show the Port Forwarding icon.

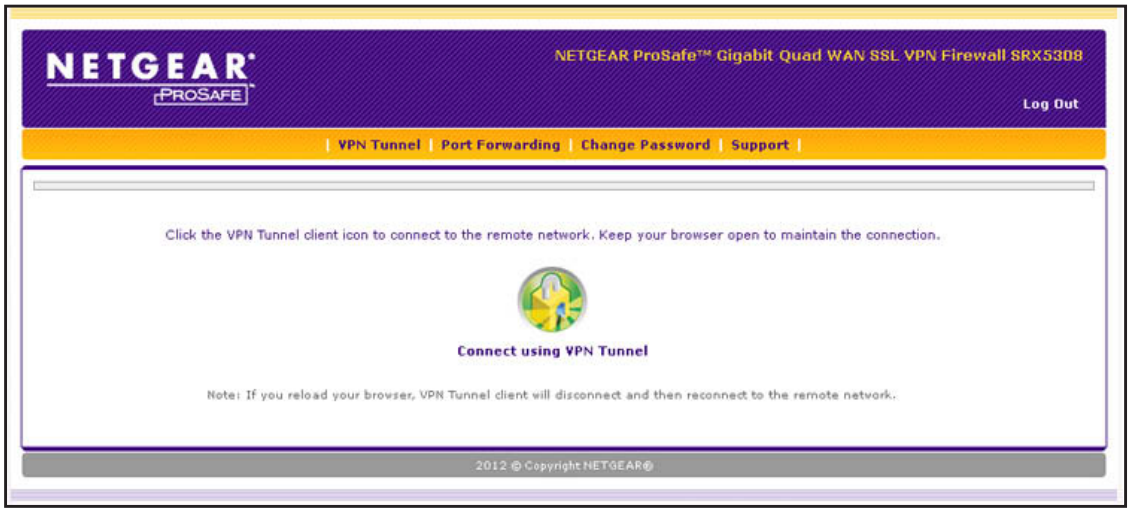

Figure 197.

Figure 198.

The User Portal screen displays a simple menu that, depending on the resources allocated, provides the SSL user with the following menu selections:

- **VPN Tunnel**. Provides full network connectivity.
- **Port Forwarding**. Provides access to the network services that you defined as described in *Configure Applications for Port Forwarding* on page 282.
- **Change Password**. Allows the user to change the password.
- **Support**. Provides access to the NETGEAR website.

Note: The first time that a user attempts to connect through the VPN tunnel, the NETGEAR SSL VPN tunnel adapter is installed; the first time that a user attempts to connect through the port forwarding tunnel, the NETGEAR port forwarding engine is installed.

View the SSL VPN Connection Status and SSL VPN Log

➢ **To view the status of current SSL VPN tunnels:**

Select **VPN > Connection Status > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:

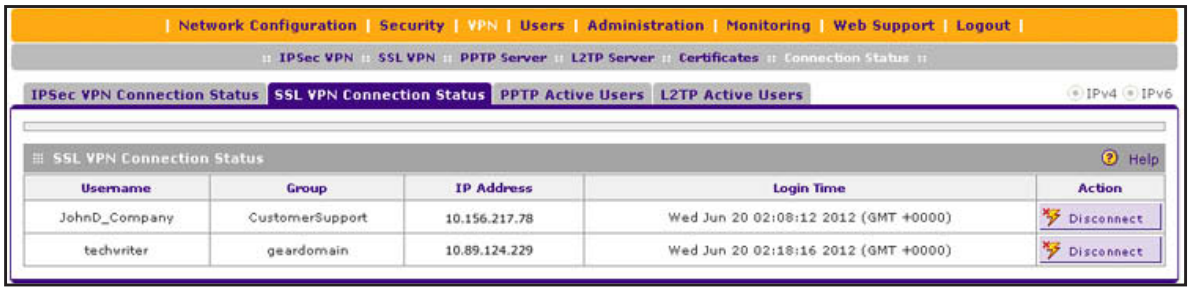

Figure 199.

The active user's name, group, and IP address are listed in the table with a time stamp indicating the time and date that the user connected.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

- **To display the SSL VPN log:**

  Select **Monitoring > VPN Logs > SSL VPN Logs.** The SSL VPN Logs screen displays:

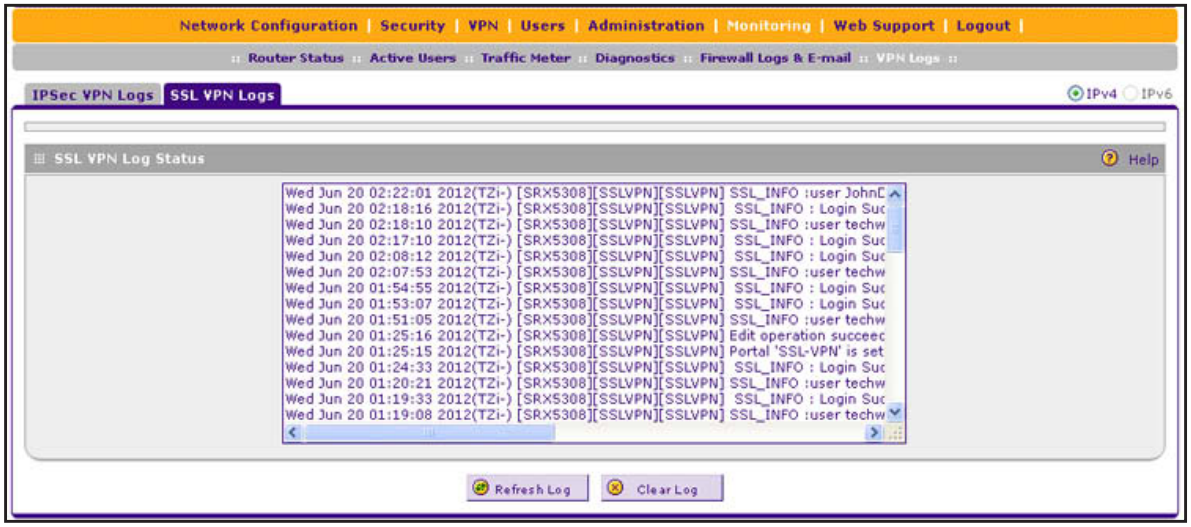

Figure 200.

7. Manage Users, Authentication, and VPN Certificates

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

- *The VPN Firewall's Authentication Process and Options*
- *Configure Authentication Domains, Groups, and Users*
- *Manage Digital Certificates for VPN Connections*

The VPN Firewall's Authentication Process and Options

Users are assigned to a group, and a group is assigned to a domain. Therefore, you should first create any domains, then groups, then user accounts.

Note: Do not confuse the authentication groups with the LAN groups that are described in *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 96.

You need to create name and password accounts for all users who need to be able to connect to the VPN firewall. This includes administrators, guests, and SSL VPN clients. Accounts for IPSec VPN clients are required only if you have enabled extended authentication (XAUTH) in your IPSec VPN configuration.

Users connecting to the VPN firewall need to be authenticated before being allowed to access the VPN firewall or the VPN-protected network. The login screen that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines the authentication method that is used and, for SSL connections, the portal layout that is presented.

Note: IPSec VPN, L2TP, and PPTP users do not belong to a domain and are not assigned to a group.

Except in the case of IPSec VPN users, when you create a user account, you need to specify a group. When you create a group, you need to specify a domain.

The following table summarizes the external authentication protocols and methods that the VPN firewall supports.

Table 75. External authentication protocols and methods

Authentication Protocol or Method	Description
PAP	Password Authentication Protocol (PAP) is a simple protocol in which the client sends a password in clear text.
CHAP	Challenge Handshake Authentication Protocol (CHAP) executes a three-way handshake in which the client and server trade challenge messages, each responding with a hash of the other's challenge message that is calculated using a shared secret value.
RADIUS	A network-validated PAP or CHAP password-based authentication method that functions with Remote Authentication Dial In User Service (RADIUS).

Table 75. External authentication protocols and methods (continued)

Authentication Protocol or Method	Description
MIAS	A network-validated PAP or CHAP password-based authentication method that functions with Microsoft Internet Authentication Service (MIAS), which is a component of Microsoft Windows 2003 Server.
WiKID	WiKID Systems is a PAP or CHAP key-based two-factor authentication method that functions with public key cryptography. The client sends an encrypted PIN to the WiKID server and receives a one-time passcode with a short expiration period. The client logs in with the passcode. See *Appendix 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.
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.

Configure Authentication Domains, Groups, and Users

- *Configure Domains*
- *Configure Groups*
- *Configure User Accounts*
- *Set User Login Policies*
- *Change Passwords and Other User Settings*

Configure Domains

The domain determines the authentication method to be used for associated users. For SSL connections, the domain also determines the portal layout that is presented, which in turn determines the network resources to which the associated users have access. The default domain of the VPN firewall is named geardomain. You cannot delete the default domain.

Create Domains

➢ **To create a domain:**

1. Select **Users > Domains**. The Domains screen displays. (The following figure shows the VPN firewall's default domain—geardomain—and, as an example, other domains in the List of Domains table.)

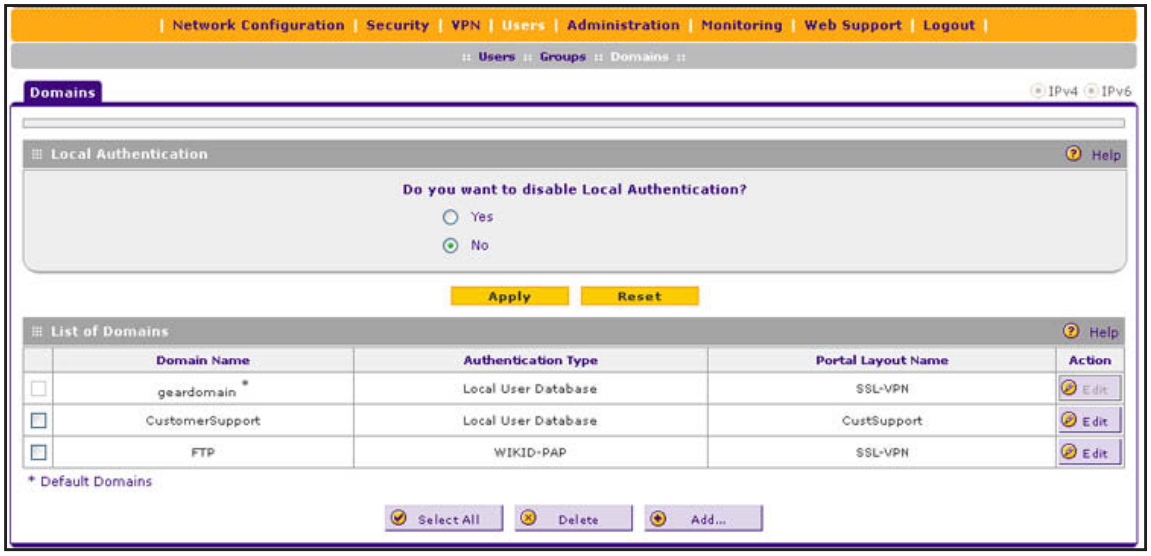

Figure 201.

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

- **Check box**. Allows you to select the domain in the table.
- **Domain Name**. The name of the domain. The name of the default domain (geardomain) to which the default SSL-VPN portal is assigned is appended by an asterisk.
- **Authentication Type**. The authentication method that is assigned to the domain.
- **Portal Layout Name**. The SSL portal layout that is assigned to the domain.
- **Action**. The Edit table button, which provides access to the Edit Domain screen.

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

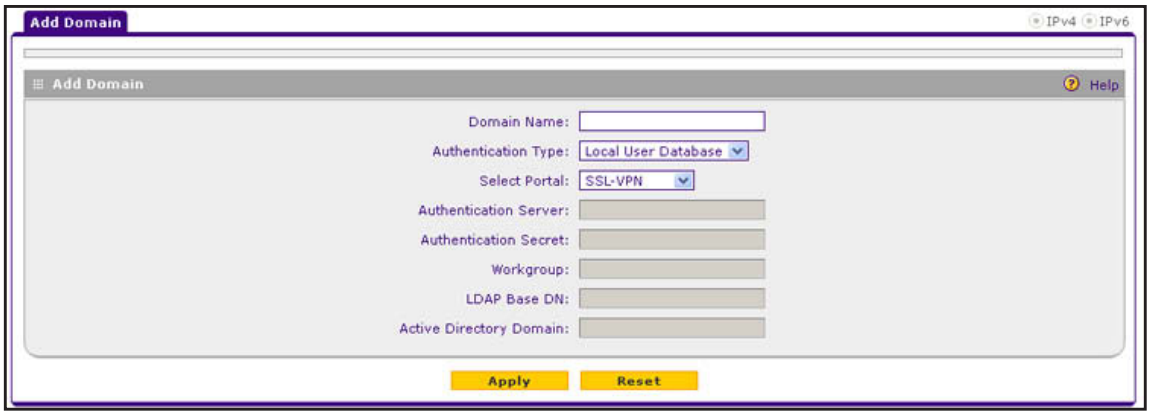

Figure 202.

3. Complete the settings as described in the following table:

Table 76. Add Domain screen settings

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type **Note:** If you select any type of RADIUS authentication, make sure that one or more RADIUS servers are configured (see *RADIUS Client and Server Configuration* on page 247).	From the drop-down list, select the authentication method that the VPN firewall applies: • **Local User Database (default)**. Users are authenticated locally on the VPN firewall. This is the default setting. You do not need to complete any other fields on this screen. • **Radius-PAP**. RADIUS Password Authentication Protocol (PAP). Complete the following fields: - Authentication Server - Authentication Secret • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the following fields: - Authentication Server - Authentication Secret • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the following fields: - Authentication Server - Authentication Secret • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the following fields: - Authentication Server - Authentication Secret • **WIKID-PAP**. WiKID Systems PAP. Complete the following fields: - Authentication Server - Authentication Secret • **WIKID-CHAP**. WiKID Systems CHAP. Complete the following fields: - Authentication Server - Authentication Secret

Table 76. Add Domain screen settings (continued)

Setting	Description
Authentication Type (continued) **Note:** If you select any type of RADIUS authentication, make sure that one or more RADIUS servers are configured (see *RADIUS Client and Server Configuration* on page 247).	• **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the following fields: - Authentication Server - Authentication Secret • **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the following fields: - Authentication Server - Authentication Secret • **NT Domain**. Microsoft Windows NT Domain. Complete the following fields: - Authentication Server - Workgroup • **Active Directory**. Microsoft Active Directory. Complete the following fields, and make a selection from the LDAP Encryption drop-down list: - Authentication Server - Active Directory Domain • **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the following fields, and make a selection from the LDAP Encryption drop-down list: - Authentication Server - LDAP Base DN
Select Portal	The portal that is assigned to this domain and that is presented to the user to enter credentials. The default portal is SSL-VPN.
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 distinguished name (DN) that is required to access the LDAP authentication server. This should be a user in the LDAP directory who has read access to all the users that you would like to import into the VPN firewall. The Bind DN field accepts two formats: • **A display name in the DN format**. For example: cn=Jamie Hanson,cn=users,dc=test,dc=com. • **A Windows login account name in email format**. For example: jhanson@testAD.com. This last type of bind DN can be used only for a Windows LDAP server.
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: in the Local Authentication section of the Domain screen (see *Figure 201* on page 304), select the **No** radio button.

Note: A combination of local and external authentication is supported.

WARNING:

If you disable local authentication, make sure that there is at least one external administrative user; otherwise, access to the VPN firewall is blocked.

6. If you do change local authentication, click **Apply** in the Domain screen to save your settings.

➢ **To delete one or more domains:**

1. In the List of Domains table, select the check box to the left of each domain that you want to delete, or click the **Select All** table button to select all domains.
2. Click the **Delete** table button.

Note: You cannot delete the geardomain default domain.

Edit Domains

➢ **To edit a domain:**

1. Select **Users > Domains**. The Domains screen displays (see *Figure 201* on page 304).
2. In the Action column of the List of Domains table, click the **Edit** table button for the domain that you want to edit. The Edit Domains screen displays. This screen is similar to the Add Domains screen (see the previous figure).
3. Modify the settings as described in the previous table. (You cannot modify the Domain Name and Authentication Type fields.)
4. Click **Apply** to save your changes. The modified domain is displayed in the List of Domains table.

Note: You cannot edit the geardomain default domain.

Configure Groups

The use of groups simplifies the configuration of VPN policies when different sets of users have different restrictions and access controls. It also simplifies the configuration of web access exception rules. Like the default domain of the VPN firewall, the default group is also named geardomain. The default group geardomain is assigned to the default domain geardomain. You cannot delete the default domain geardomain, nor its associated default group geardomain.

IMPORTANT:

When you create a domain on the Domains screen (see the previous section), a group with the same name as the new domain is created automatically. You cannot delete such a group. However, when you delete the domain with which it is associated, the group is deleted automatically.

Note: IPSec VPN, L2TP, and PPTP users do not belong to a domain and are not assigned to a group.

Note: Groups that are defined on the Groups screen are used for setting SSL VPN policies. These groups should not be confused with LAN groups that are defined on the IPv4 LAN Groups screen and that are used to simplify firewall policies. For information about LAN groups, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 96.

Create Groups

➢ **To create a VPN group:**

1. Select **Users > Groups**. The Groups screen displays. (The following figure shows the VPN firewall's default group—geardomain—and, as an example, several other groups in the List of Groups table.)

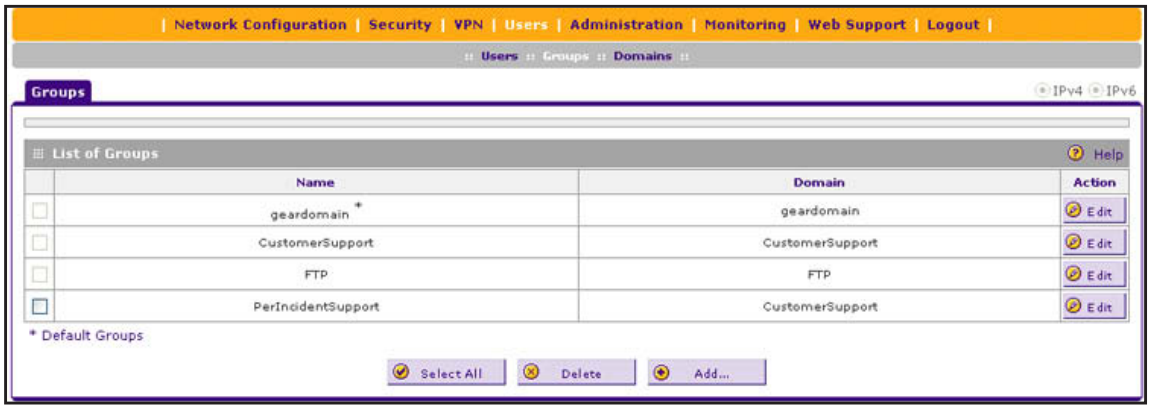

Figure 203.

The List of Groups table displays the VPN groups with the following fields:

- **Check box**. Allows you to select the group in the table.
- **Name**. The name of the group. The name of the default group (geardomain) that is assigned to the default domain (also geardomain) is appended by an asterisk.

Note: *When you create a domain on the Domains screen, a group with the same name as the new domain is created automatically. You cannot delete such a group on the Groups screen. However, when you delete the domain with which the group is associated, the group is deleted automatically.*

- **Domain**. The name of the domain to which the group is assigned.
- **Action**. The Edit table button, which provides access to the Edit Group screen.

2. Under the List of Groups table, click the **Add** table button. The Add Group screen displays:

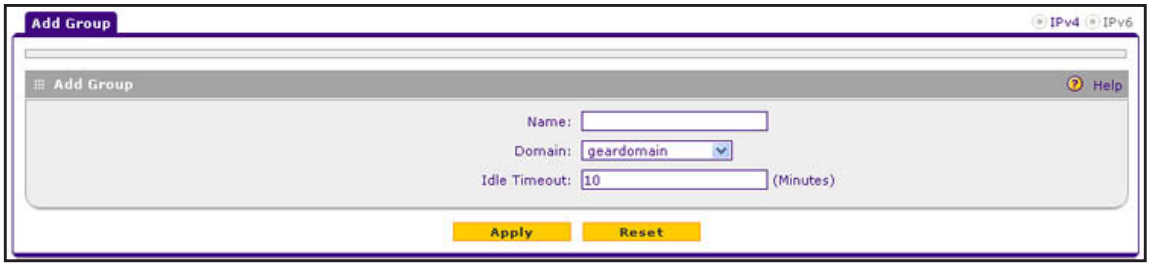

Figure 204.

3. Complete the settings as described in the following table:

Table 77. Add Group screen settings

Setting	Description
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.
Domain	The drop-down list shows the domains that are listed on the Domain screen. From the drop-down list, select the domain with which the group is associated. For information about how to configure domains, see *Configure Domains* on page 303.
Idle Timeout	The period after which an idle user is automatically logged out of the VPN firewall's web management interface. The default idle time-out period is 10 minutes.

4. Click **Apply** to save your changes. The new group is added to the List of Groups table.

➢ **To delete one or more groups:**

1. In the List of Groups table, select the check box to the left of each group that you want to delete, or click the **Select All** table button to select all groups.
2. Click the **Delete** table button.

Note: You can delete only groups that you created on the Groups screen. Groups that were automatically created when you created a domain cannot be deleted on the Groups screen. See the Important note at the beginning of this section.

Edit Groups

For groups that were automatically created when you created a domain, you can modify only the idle time-out settings but not the group name or associated domain.

For groups that you created on the Add Groups screen, you can modify the domain and the idle time-out settings but not the group name.

➢ **To edit a VPN group:**

1. Select **Users > Groups**. The Groups screen displays (see *Figure 203* on page 308).
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. This screen is identical to the Add Groups screen.
3. Modify the settings as described in the previous table.
4. Click **Apply** to save your changes. The modified group is displayed in the List of Groups table.

Configure User Accounts

When you create a user account, you need to assign the user to a user group. When you create a group, you need to assign the group to a domain that specifies the authentication method. Therefore, you should first create any domains, then groups, and then user accounts.

Note: IPSec VPN, L2TP, and PPTP users do not belong to a domain and are not assigned to a group.

There are two default user accounts:

- A user with the name **admin** and the password **password**. This is a user who has read/write access, is associated with the domain geardomain, and is denied login from the WAN interface by default. The user name is appended by an asterisk. You cannot delete this user account.
- A user with the name **guest** and the password **password**. This is a user who has read-only access, is associated with the domain geardomain, and is denied login from the WAN interface by default. The user name is appended by an asterisk. You cannot delete this user account.

You can create five different types of user accounts by applying one of the predefined user types:

- **SSL VPN user**. A user who can log in only to the SSL VPN portal.
- **Administrator**. A user who has full access and the capacity to change the VPN firewall configuration (that is, read-write access).

- **Guest user**. A user who can only view the VPN firewall configuration (that is, read-only access).
- **IPSec VPN user**. A user who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 245).
- **L2TP user**. A user who can connect over an L2TP connection to an L2TP client that is located behind the VPN firewall.
- **PPTP user**. A user who can connect over a PPTP connection to a PPTP client that is located behind the VPN firewall.

➢ **To create a user account:**

1. Select **Users > Users**. The Users screen displays. (The following figure shows the VPN firewall's default users—admin and guest—and, as an example, several other users in the List of Users table.)

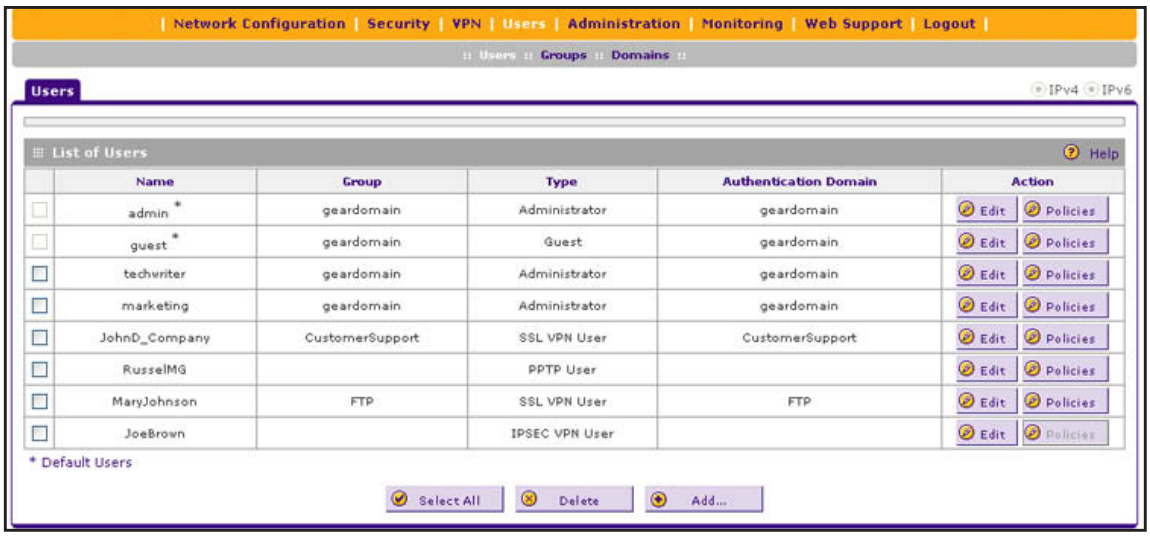

Figure 205.

The List of Users table displays the users and has the following fields:

- **Check box**. Allows you to select the user in the table.
- **Name**. The name of the user. If the user name is appended by an asterisk, the user is a default user that is preconfigured on the VPN firewall and cannot be deleted.
- **Group**. The group to which the user is assigned.
- **Type**. The type of access credentials that are assigned to the user.
- **Authentication Domain**. The authentication domain to which the user is assigned.
- **Action**. The Edit table button, which provides access to the Edit User screen; the Policies table button, which provides access to the policy screens.

2. Under the List of Users table, click the **Add** table button. The Add Users screen displays:

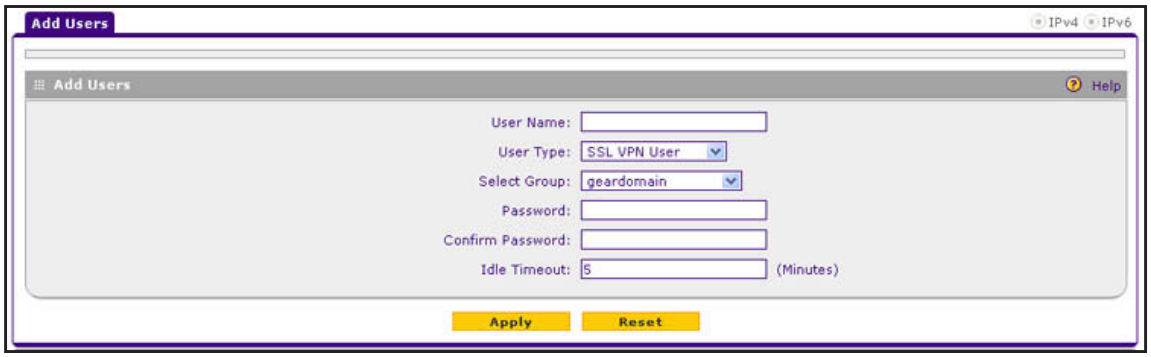

Figure 206.

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

Table 78. Add Users screen settings

Setting	Description
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	From the drop-down list, select one of the predefined user types that determines the access credentials: • **SSL VPN User**. A user who can log in only to the SSL VPN portal. • **Administrator**. A user who has full access and the capacity to change the VPN firewall configuration (that is, read/write access). • **Guest (readonly)**. A user who can only view the VPN firewall configuration (that is, read-only access). • **IPSEC VPN User**. A user who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 245). • **L2TP User**. A user who can connect over an L2TP connection to an L2TP client that is located behind the VPN firewall. • **PPTP User**. A user who can connect over a PPTP connection to a PPTP client that is located behind the VPN firewall.
Select Group	The drop-down list shows the groups that are listed on the Group screen. From the drop-down list, select the group to which the user is assigned. For information about how to configure groups, see *Configure Groups* on page 307. **Note:** The user is assigned to the domain that is associated with the selected group.
Password	The password that the user needs to enter to gain access to the VPN firewall.
Confirm Password	This field needs to be identical to the password that you entered in the Password field.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes.

4. Click **Apply** to save your settings. The user is added to the List of Users table.

➢ **To delete one or more user accounts:**

1. In the List of Users table, select the check box to the left of each user account that you want to delete, or click the **Select All** table button to select all accounts. You cannot delete a default user account.
2. Click the **Delete** table button.

Note: You cannot delete the default admin or guest user.

Set User Login Policies

You can restrict the ability of defined users to log in to the VPN firewall's web management interface. You can also require or prohibit logging in from certain IP addresses or from particular browsers. This section consists of the following subsections:

- *Configure Login Policies*
- *Configure Login Restrictions Based on IPv4 Addresses*
- *Configure Login Restrictions Based on IPv6 Addresses*
- *Configure Login Restrictions Based on Web Browser*

Configure Login Policies

➢ **To configure user login policies:**

1. Select **Users > Users**. The Users screen displays (see *Figure 205* on page 311).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view:

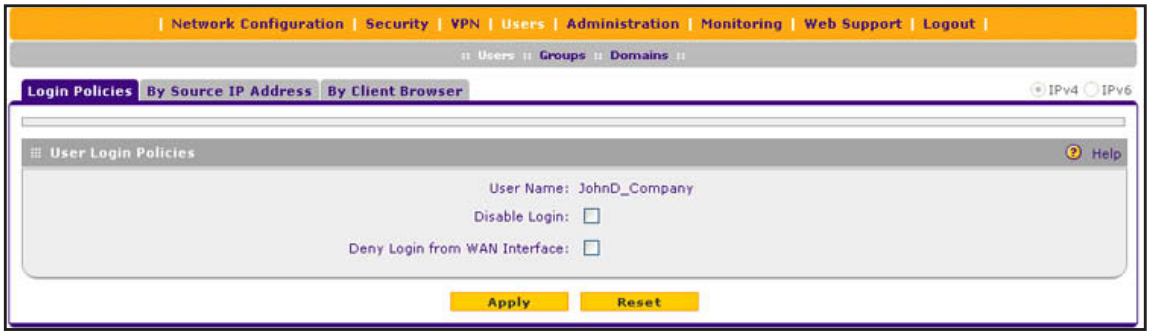

Figure 207.

3. Make the following optional selections:
   - To prohibit the user from logging in to the VPN firewall, select the **Disable Login** check box.
   - To prohibit the user from logging in from the WAN interface, select the **Deny Login from WAN Interface** check box. In this case, the user can log in only from the LAN interface.

Note: For security reasons, the Deny Login from WAN Interface check box is selected by default for guests and administrators. The Disable Login check box is disabled (masked out) for administrators.

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

Configure Login Restrictions Based on IPv4 Addresses

➢ **To restrict logging in based on IPv4 addresses:**

1. Select **Users > Users**. The Users screen displays (see *Figure 205* on page 311).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view.
3. Click the **By Source IP Address** submenu tab. In the upper right of the screen, the IPv4 radio button is selected by default. The By Source IP Address screen displays the IPv4 settings. (The following figure shows an IP address in the Defined Addresses table as an example.)

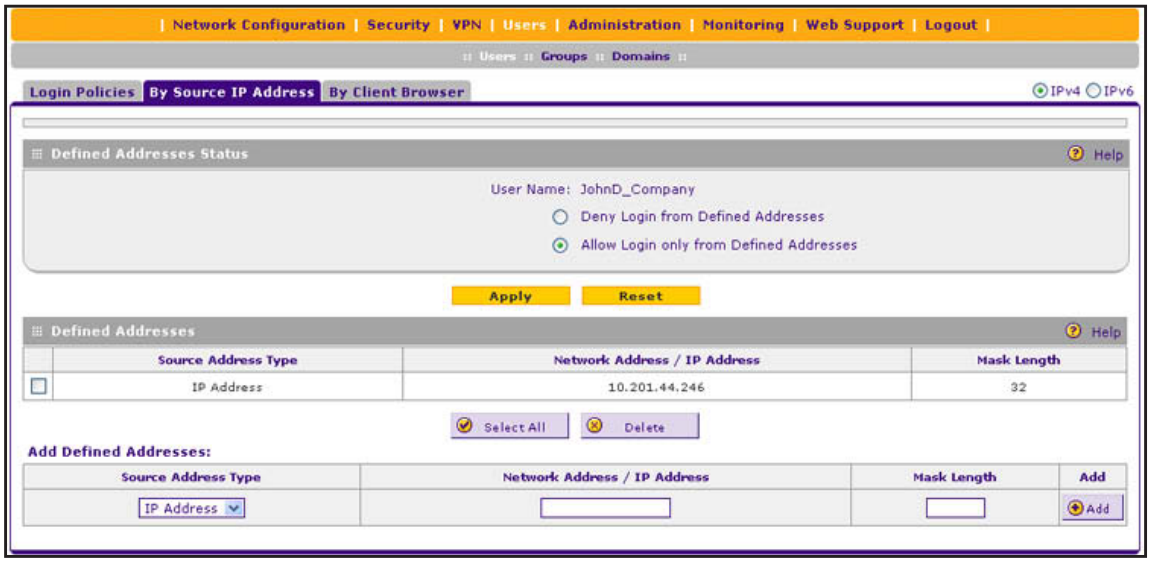

Figure 208.

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 described in the following table:

Table 79. Defined addresses settings for IPv4

Setting	Description
Source Address Type	Select the type of address from the drop-down list: • **IP Address**. A single IPv4 address. • **IP Network**. A subnet of IPv4 addresses. You need to enter a netmask length in the Mask Length field.
Network Address / IP Address	Depending on your selection from the Source Address Type drop-down list, enter the IP address or the network address.
Mask Length	For a network address, enter the netmask length (0–32). **Note:** By default, a single IPv4 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 IPv4 addresses:**

1. In the Defined Addresses table, select the check box to the left of each address that you want to delete, or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Configure Login Restrictions Based on IPv6 Addresses

➢ **To restrict logging in based on IPv6 addresses:**

1. Select **Users > Users**. The Users screen displays (see *Figure 205* on page 311).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view.
3. Click the **By Source IP Address** submenu tab.
4. In the upper right of the screen, select the **IPv6** radio button. The By Source IP Address screen displays the IPv6 settings. (The following figure shows an IP address in the Defined Addresses table as an example.)

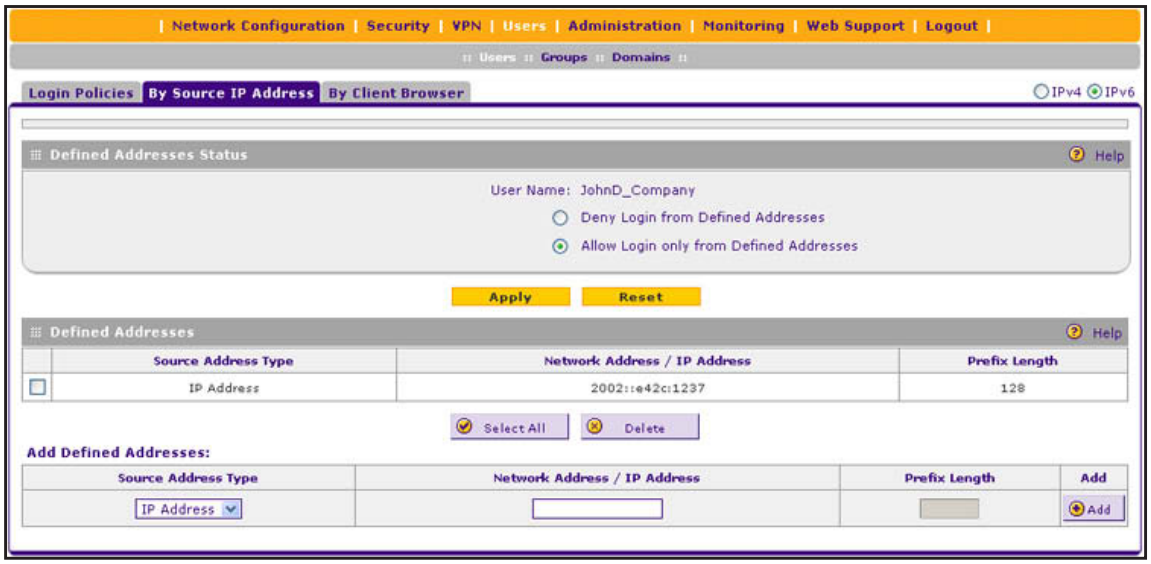

Figure 209.

5. 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.
6. Click **Apply** to save your settings.
7. In the Add Defined Addresses section of the screen, add an address to the Defined Addresses table by entering the settings as described in the following table:

Table 80. Defined addresses settings for IPv6

Setting	Description
Source Address Type	Select the type of address from the drop-down list: • **IP Address**. A single IPv6 address. • **IP Network**. A subnet of IPv6 addresses. You need to enter a prefix length in the Prefix Length field.
Network Address / IP Address	Depending on your selection from the Source Address Type drop-down list, enter the IP address or the network address.
Prefix Length	For a network address, enter the prefix length (0–64). **Note:** By default, a single IPv6 address is assigned a prefix length of 64.

8. Click the **Add** table button. The address is added to the Defined Addresses table.
9. Repeat *Step 7* and *Step 8* for any other addresses that you want to add to the Defined Addresses table.

➢ **To delete one or more IPv6 addresses:**

1. In the Defined Addresses table, select the check box to the left of each address that you want to delete, or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Configure Login Restrictions Based on Web Browser

➢ **To restrict logging in based on the user's browser:**

1. Select **Users > Users**. The Users screen displays (see *Figure 205* on page 311).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view.
3. Click the **By Client Browser** submenu tab. The By Client Browser screen displays. (The following figure shows a browser in the Defined Browsers table as an example.)

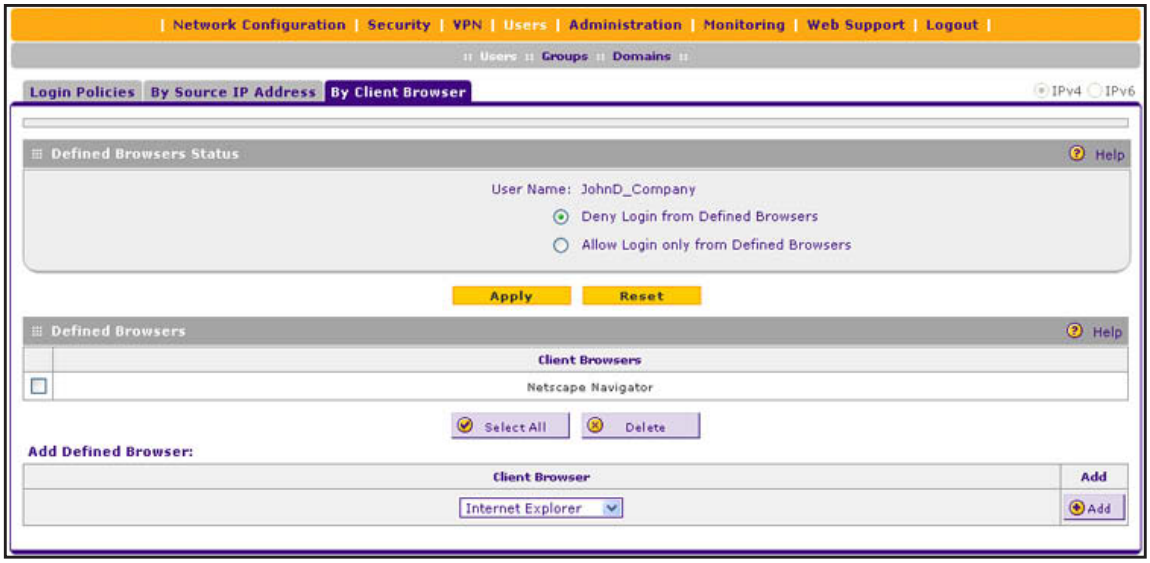

Figure 210.

4. In the Defined Browsers Status section of the screen, select one of the following radio buttons:
   - **Deny Login from Defined Browsers**. Deny logging in from the browsers in the Defined Browsers table.
   - **Allow Login only from Defined Browsers**. Allow logging in from the browsers in the Defined Browsers table.
5. Click **Apply** to save your settings.
6. In the Add Defined Browser section of the screen, add a browser to the Defined Browsers table by selecting one of the following browsers from the drop-down list:
   - **Internet Explorer**.
   - **Opera**.
   - **Netscape Navigator**.

- **Firefox**. Mozilla Firefox.
- **Mozilla**. Other Mozilla browsers.

7. Click the **Add** table button. The browser is added to the Defined Browsers table.
8. Repeat *Step 6* and *Step 7* for any other browsers that you want to add to the Defined Browsers table.

➢ **To delete one or more browsers:**

1. In the Defined Browsers table, select the check box to the left of each browser that you want to delete, or click the **Select All** table button to select all browsers.
2. Click the **Delete** table button.

Change Passwords and Other User Settings

For any user, you can change the password, user type, and idle time-out settings. Only administrators have read/write access. All other users have read-only access.

Note: The default administrator and default guest passwords for the web management interface are both **password**. NETGEAR recommends that you change the password for the administrator account to a more secure password, and that you configure a separate secure password for the guest account.

Note: The most secure password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 32 characters.

Note: After a factory defaults reset, the password and time-out value are changed back to **password** and 5 minutes, respectively.

➢ **To modify user settings, including passwords:**

1. Select **Users > Users**. The Users screen displays (see *Figure 205* on page 311).
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 Users screen displays:

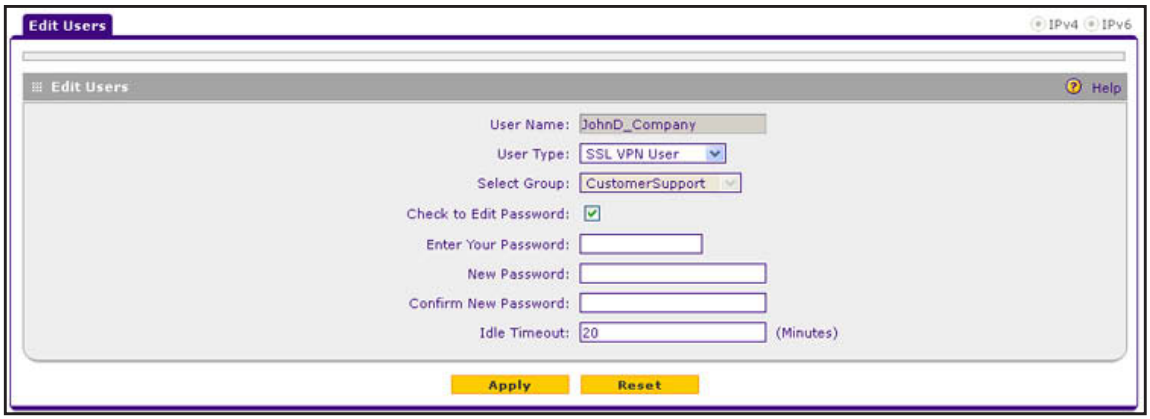

Figure 211.

3. Change the settings as described in the following table:

> **Note:** Once established, you cannot change the user name or the group. If you need to change the user name or the group, delete the user account and recreate it with the correct name or group.

Table 81. Edit User screen settings

Setting	Description	
Select User Type	From the drop-down list, select one of the predefined user types that determines the access credentials: • **SSL VPN User**. User who can log in only to the SSL VPN portal. • **Administrator**. User who has full access and the capacity to change the VPN firewall configuration (that is, read/write access). • **Guest (readonly)**. User who can only view the VPN firewall configuration (that is, read-only access). • **IPSEC VPN User**. You cannot change an existing user from the IPSEC VPN User type to another type or from another type to the IPSEC VPN User type. • **L2TP User**. You cannot change an existing user from the L2TP User type to another type or from another type to the L2TP User type. • **PPTP User**. You cannot change an existing user from the PPTP User type to another type or from another type to the PPTP User type.	
Check to Edit Password	Select this check box to make the password fields accessible to modify the password.	
	Enter Your Password	Enter the password with which you have logged in.
	New Password	Enter the new password.
	Confirm New Password	Reenter the new password for confirmation.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes.	

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

Manage Digital Certificates for VPN Connections

The VPN firewall 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:

- On the VPN firewall, you can enter a digital certificate on the IKE Policies screen, on which the certificate is referred to as an RSA signature (see *Figure 159* on page 233 and *Authentication Method* on page 236).
- On the VPN Client, you can enter a digital certificate on the Authentication pane in the Configuration Panel screen (see *Figure 146* on page 222).

Digital certificates are extended for secure web access connections over HTTPS (that is, SSL connections).

Digital certificates either can be self-signed or can be issued by certification authorities (CAs) such as an internal Windows server or an external organization such as Verisign or Thawte.

However, if the digital certificate contains the extKeyUsage extension, the certificate needs to be used for one of the purposes defined by the extension. For example, if the digital certificate contains the extKeyUsage extension that is defined for SNMPv2, the same certificate cannot be used for secure web management. The extKeyUsage would govern the certificate acceptance criteria on the VPN firewall when the same digital certificate is being used for secure web management.

On the VPN firewall, the uploaded digital certificate is checked for validity and purpose. The digital certificate is accepted when it passes the validity test and the purpose matches its use. The check for the purpose needs to correspond to its use for IPSec VPN, SSL VPN, or both. If the defined purpose is for IPSec VPN and SSL VPN, the digital certificate is uploaded to both the IPSec VPN certificate repository and the SSL VPN certificate repository. However, if the defined purpose is for IPSec VPN only, the certificate is uploaded only to the IPSec VPN certificate repository.

The VPN firewall uses digital certificates to authenticate connecting VPN gateways or clients, and to be authenticated by remote entities. A digital certificate that authenticates a server, for example, is a file that contains the following elements:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

You can obtain a digital certificate from a well-known commercial certification authority (CA) such as Verisign or Thawte, or you can generate and sign your own digital certificate.

Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity. A self-signed digital certificate triggers a warning from most browsers because it provides no protection against identity theft of the server.

The VPN firewall contains a self-signed digital certificate from NETGEAR. This certificate can be downloaded from the VPN firewall login screen for browser import. However, NETGEAR recommends that you replace this digital certificate with a digital certificate from a well-known commercial CA before you deploy the VPN firewall in your network.

VPN Certificates Screen

To display the Certificates screen, select **VPN > Certificates**. Because of the large size of this screen, and because of the way the information is presented, the Certificates screen is divided and presented in this manual in three figures (*Figure 212* on page 322, *Figure 214* on page 324, and *Figure 216* on page 327).

The Certificates screen lets you view the loaded digital certificates, upload a new digital certificate, and generate a certificate signing request (CSR). The VPN firewall typically holds two types of digital certificates:

- CA certificates. Each CA issues its own digital certificate to validate communication with the CA and to verify the validity of digital certificates that are signed by the CA.
- Self-signed certificates. The digital certificates that are issued to you by a CA to identify your device.

The Certificates screen contains four tables that are described 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 *Manage VPN CA Certificates* on this page).
- **Active Self Certificates table**. Contains the self-signed certificates that were issued by CAs and that you uploaded (see *Manage VPN Self-Signed Certificates* on page 323).
- **Self Certificate Requests table**. Contains the self-signed certificate requests that you generated. These requests might or might not have been submitted to CAs, and CAs might or might not have issued digital certificates for these requests. Only the self-signed certificates in the Active Self Certificates table are active on the VPN firewall (see *Manage VPN Self-Signed Certificates* on page 323).
- **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 *Manage the VPN Certificate Revocation List* on page 326).

Manage VPN CA Certificates

➢ **To view and upload trusted certificates:**

Select **VPN > Certificates**. The Certificates screen displays. (The following figure shows the top section of the screen with the trusted certificate information and an example certificate in the Trusted Certificates [CA Certificate] table.)

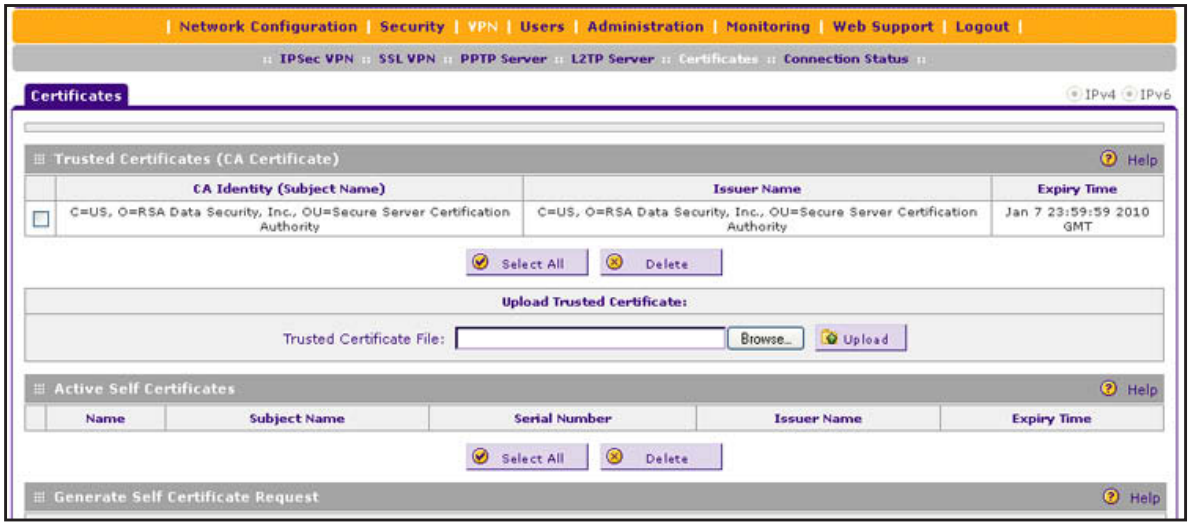

Figure 212. Certificates, screen 1 of 3

The Trusted Certificates (CA Certificate) table lists the digital certificates of CAs and contains the following fields:

- **CA Identity (Subject Name)**. The organization or person to whom the digital certificate is issued.
- **Issuer Name**. The name of the CA that issued the digital certificate.
- **Expiry Time**. The date after which the digital certificate becomes invalid.

➢ **To upload a digital certificate of a trusted CA on the VPN firewall:**

1. Download a digital certificate file from a trusted CA and store it on your computer.
2. In the Upload Trusted Certificates section of the screen, click the **Browse** button and navigate to the trusted digital certificate file that you downloaded on your computer.
3. Click the **Upload** table button. If the verification process on the VPN firewall approves the digital certificate for validity and purpose, the digital certificate is added to the Trusted Certificates (CA Certificates) table.

➢ **To delete one or more digital certificates:**

1. In the Trusted Certificates (CA Certificate) table, select the check box to the left of each digital certificate that you want to delete, or click the **Select All** table button to select all digital certificates.
2. Click the **Delete** table button.

Manage VPN Self-Signed Certificates

Instead of obtaining a digital certificate from a CA, you can generate and sign your own digital certificate. However, a self-signed digital certificate triggers a warning from most browsers because it provides no protection against identity theft of the server. (The following figure shows an image of a browser security alert.)

There can be three reasons why a security alert is generated for a security certificate:

- The security certificate was issued by a company you have not chosen to trust.
- The date of the security certificate is invalid.
- The name on the security certificate is invalid or does not match the name of the site.

When a security alert is generated, the user can decide whether to trust the host.

Figure 213.

Generate a CSR and Obtain a Self-Signed Certificate from a CA

To use a self-signed certificate, you first need to request the digital certificate from a CA, and then download and activate the digital certificate on the VPN firewall. To request a self-signed certificate from a CA, you need to generate a certificate signing request (CSR) for and on the VPN firewall. The CSR is a file that contains information about your company and about the device that holds the certificate. Refer to the CA for guidelines about the information that you need to include in your CSR.

➢ **To generate a new CSR file, obtain a digital certificate from a CA, and upload it to the VPN firewall:**

1. Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the middle section of the screen with the Active Self Certificates section, Generate Self Certificate Request section, and Self Certificate Requests section. (The Self Certificate Requests table contains an example certificate.)

Figure 214. Certificates, screen 2 of 3

2. In the Generate Self Certificate Request section of the screen, enter the settings as described in the following table:

Table 82. Generate self-signed certificate request settings

Setting	Description
Name	A descriptive name of the domain for identification and management purposes.
Subject	The name that other organizations see as the holder (owner) of the certificate. In general, use your registered business name or official company name for this purpose. **Note:** Generally, all of your certificates should have the same value in the Subject field.
Hash Algorithm	From the drop-down list, select one of the following hash algorithms: • **MD5**. A 128-bit (16-byte) message digest, slightly faster than SHA-1. • **SHA-1**. A 160-bit (20-byte) message digest, slightly stronger than MD5.
Signature Algorithm	Although this seems to be a drop-down list, the only possible selection is RSA. In other words, RSA is the default to generate a CSR.
Signature Key Length	From the drop-down list, select one of the following signature key lengths in bits: • **512** • **1024** • **2048** **Note:** Larger key sizes might improve security, but might also decrease performance.

Table 82. Generate self-signed certificate request settings (continued)

Setting	Description	
Optional Fields	IP Address	Enter your fixed (static) IP address. If your IP address is dynamic, leave this field blank.
	Domain Name	Enter your Internet domain name, or leave this field blank.
	E-mail Address	Enter the email address of a technical contact in your company.

3. Click the **Generate** table button. A new SCR is created and added to the Self Certificate Requests table.
4. In the Self Certificate Requests table, click the **View** table button in the Action column to view the new SCR. The Certificate Request Data screen displays:

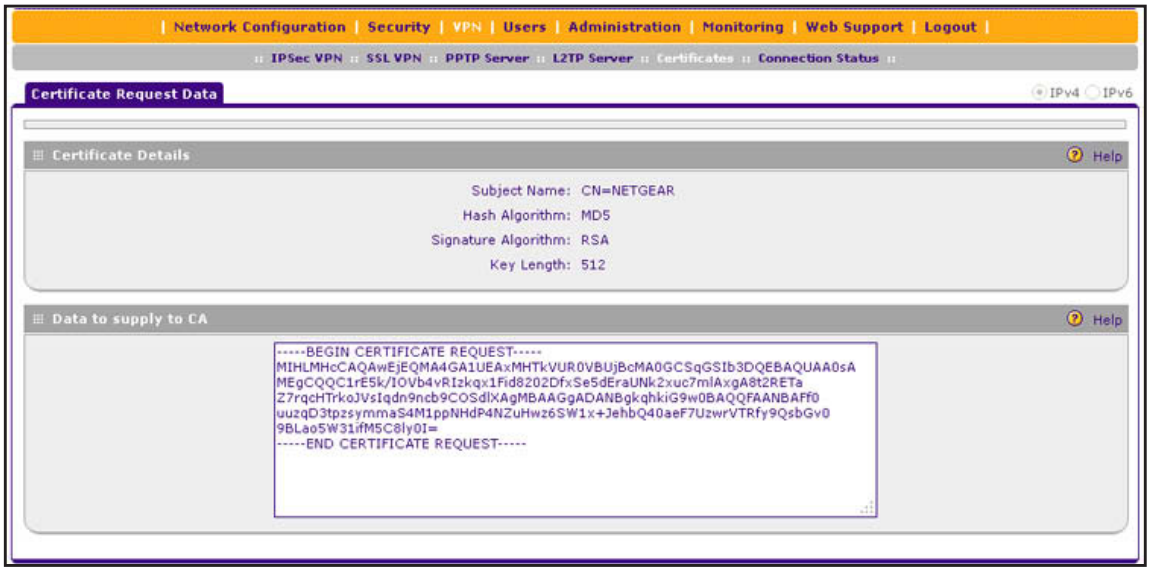

Figure 215.

5. Copy the contents of the Data to supply to CA text field into a text file, including all of the data contained from "-----BEGIN CERTIFICATE REQUEST-----" to "-----END CERTIFICATE REQUEST-----."
6. Submit your SCR to a CA:
   a. Connect to the website of the CA.
   b. Start the SCR procedure.
   c. When prompted for the requested data, copy the data from your saved text file (including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----").
   d. Submit the CA form. If no problems ensue, the digital certificate is issued by the CA.
7. Download the digital certificate file from the CA, and store it on your computer.
8. Return to the Certificates screen (see *Figure 214* on page 324) and locate the Self Certificate Requests section.

9. Select the check box next to the self-signed certificate request.
10. Click the **Browse** button and navigate to the digital certificate file from the CA that you just stored on your computer.
11. Click the **Upload** table button. If the verification process on the VPN firewall approves the digital certificate for validity and purpose, the digital certificate is added to the Active Self Certificates table.

➢ **To delete one or more SCRs:**

1. In the Self Certificate Requests table, select the check box to the left of each SCR that you want to delete, or click the **Select All** table button to select all SCRs.
2. Click the **Delete** table button.

View and Manage Self-Signed Certificates

The Active Self Certificates table on the Certificates screen (see *Figure 214* on page 324) shows the digital certificates issued to you by a CA and available for use. For each self-signed certificate, the table lists the following information:

- **Name**. The name that you used to identify this 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 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-signed certificates:**

1. In the Active Self Certificates table, select the check box to the left of each self-signed certificate that you want to delete, or click the **Select All** table button to select all self-signed certificates.
2. Click the **Delete** table button.

Manage the VPN Certificate Revocation List

A Certificate Revocation List (CRL) file shows digital certificates that have been revoked and are no longer valid. Each CA issues its own CRLs. It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

➢ **To view the loaded CRLs and upload a new CRL:**

1. Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the bottom section of the screen with the Certificate Revocation Lists (CRL) table. (There is one example certificate in the table.)

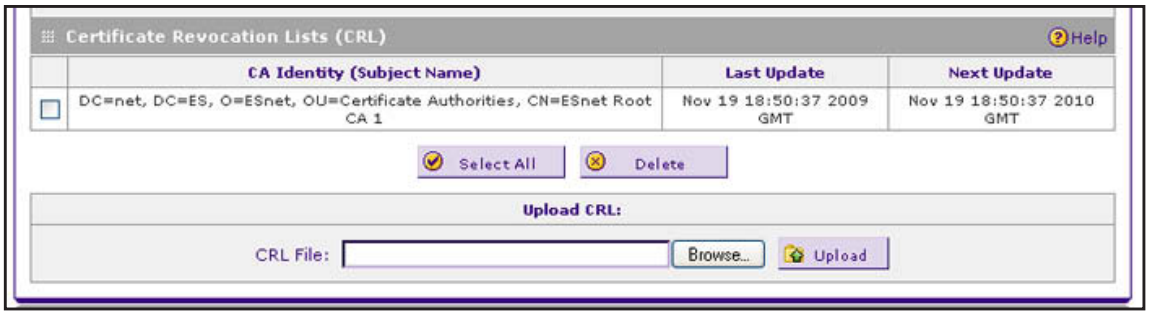

Figure 216. Certificates, screen 3 of 3

The Certificate Revocation Lists (CRL) table lists the active CAs and their critical release dates:

- **CA Identity**. The official name of the CA that issued the CRL.
- **Last Update**. The date when the CRL was released.
- **Next Update**. The date when the next CRL will be released.

2. In the Upload CRL section, click the **Browse** button and navigate to the CLR file that you previously downloaded from a CA.
3. Click the **Upload** table button. If the verification process on the VPN firewall approves the CRL, the CRL is added to the Certificate Revocation Lists (CRL) table.

Note: If the table already contains a CRL from the same CA, the old CRL is deleted when you upload the new CRL.

➢ **To delete one or more CRLs:**

1. In the Certificate Revocation Lists (CRL) table, select the check box to the left of each CRL that you want to delete, or click the **Select All** table button to select all CRLs.
2. Click the **Delete** table button.

8. 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 VPN firewall. The chapter contains the following sections:

- *Performance Management*
- *System Management*

Performance Management

Performance management consists of controlling the traffic through the VPN firewall so that the necessary traffic gets through when there is a bottleneck. You can either reduce unnecessary traffic or reschedule some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

The maximum bandwidth capacity of the VPN firewall in each direction is as follows:

- LAN side. 4000 Mbps (four LAN ports at 1000 Mbps each)
- WAN side
  - Load balancing mode. 4000 Mbps (four WAN ports at 1000 Mbps each)
  - Auto-rollover mode. 1000 Mbps (one active WAN port at 1000 Mbps)
  - Single WAN port mode. 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. 6 Mbps (four WAN ports at 1.5 Mbps each)
- Auto-rollover mode. 1.5 Mbps (one active WAN port at 1.5 Mbps)
- Single WAN port mode. 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 VPN firewall is the limiting factor to throughput for most installations.

Using four WAN ports in load balancing mode increases the bandwidth capacity of the WAN side of the VPN firewall, but there is no backup if one of the WAN ports fails. When such a failure occurs, the traffic that would have been sent on the failed WAN port is diverted to another 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 VPN firewall 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. Any outbound rule that you create restricts outgoing traffic and therefore decreases the traffic load on the WAN side.

On the LAN WAN screen, if you have not defined any rules, only the default rule is listed. The default LAN WAN outbound rule allows all outgoing traffic.

WARNING:

Incorrect configuration of outbound firewall rules can cause serious connection problems.

Each rule lets you specify the desired action for the connections that are covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise allow
- ALLOW always
- ALLOW by schedule, otherwise block

The following section summarizes the various criteria that you can apply to outbound rules in order to reduce traffic. For more information about outbound rules, see *Outbound Rules (Service Blocking)* on page 137. For detailed procedures on how to configure outbound rules, see *Configure LAN WAN Rules* on page 145 and *Configure DMZ WAN Rules* on page 152.

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 display in the list, you need to define it using the Services screen (see *Outbound Rules (Service Blocking)* on page 137 and *Add Customized Services* on page 177).

- **LAN users (or DMZ users)**. You can specify which computers on your network are affected by an outbound rule. There are several options:
  - **Any**. The rule applies to all computers and devices on your LAN or DMZ.
  - **Single address**. The rule applies to the address of a particular computer.
  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule applies to a group of computers. (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 computers and network devices and is generally referred to as the network database, which is described in *Manage the Network Database* on page 97. Computers and network devices are entered into the network database by various methods, which are described in *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 96.
  - **IP Groups**. The rule applies to a group of individual LAN IP addresses. Use the IP Groups screen (under the Network Security main navigation menu) to assign IP addresses to groups. For more information, see *Create IP Groups* on page 179. (LAN IP groups do not apply to DMZ WAN outbound rules.)
- **WAN users**. You can specify which Internet locations are covered by an outbound rule, based on their IP address:
  - **Any**. The rule applies to all Internet IP address.
  - **Single address**. The rule applies to a single Internet IP address.
  - **Address range**. The rule applies to a range of Internet IP addresses.
  - **IP Groups**. The rule applies to a group of individual WAN IP addresses. Use the IP Groups screen (under the Network Security main navigation menu) to assign IP addresses to groups. For more information, see *Create IP Groups* on page 179.
- **Schedule**. You can configure three different schedules to specify when a rule is applied. Once a schedule is configured, it affects all rules that use this schedule. You specify the days of the week and time of day for each schedule. For more information, see *Set a Schedule to Block or Allow Specific Traffic* on page 189.
- **QoS profile**. You can apply QoS profiles to outbound rules to regulate the priority of traffic. For information about QoS profiles, see *Create Quality of Service Profiles for IPv4 Firewall Rules* on page 184.
- **Bandwidth profile**. You can define bandwidth profiles and then apply them outbound LAN WAN rules to limit traffic. (You cannot apply bandwidth profiles to DMZ WAN rules.) For information about how to define bandwidth profiles, see *Create Bandwidth Profiles* on page 181.

Content Filtering

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the VPN firewall's content-filtering feature. By default, this feature is disabled; all requested traffic from any website is allowed.

In order to reduce traffic, the VPN firewall provides the following methods to filter web content:

- **Keyword blocking**. You can specify words that, should they appear in the website name (URL) or newsgroup name, cause that site or newsgroup to be blocked by the VPN firewall.
- **Web object blocking**. You can block the following web component types: embedded objects (ActiveX and Java), proxies, and cookies.

To further narrow down the content filtering, you can configure groups to which the content-filtering rules apply and trusted domains for which the content-filtering rules do not apply.

Source MAC Filtering

If you want to reduce outgoing traffic by preventing Internet access by certain computers on the LAN, you can use the source MAC filtering feature to drop the traffic received from the computers with the specified MAC addresses. By default, this feature is disabled; all traffic received from computers with any MAC address is allowed. See *Enable Source MAC Filtering* on page 190 for the procedure on how to use this feature.

Features That Increase Traffic

The following features of the VPN firewall 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). Any inbound rule that you create allows additional incoming traffic and therefore increases the traffic load on the WAN side.

ON the LAN WAN screen, if you have not defined any rules, only the default rule is listed. The default LAN WAN inbound rule blocks all access from outside except responses to requests from the LAN side.

WARNING:

Incorrect configuration of inbound firewall rules can cause serious connection problems.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise allow
- ALLOW always
- ALLOW by schedule, otherwise block

The following section summarizes the various criteria that you can apply to inbound rules and that might increase traffic. For more information about inbound rules, see *Inbound Rules (Port Forwarding)* on page 140. For detailed procedures on how to configure inbound rules, see *Configure LAN WAN Rules* on page 145 and *Configure DMZ WAN Rules* on page 152.

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 display in the list, you need to define it using the Services screen (see *Inbound Rules (Port Forwarding)* on page 140 and *Add Customized Services* on page 177).
- **WAN destination IP address**. 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.
- **LAN users (or DMZ users)**. Only when the IPv4 routing mode is Classical Routing, you can specify which computers on your network are affected by an inbound rule. When Classical Routing is enabled, there are several options:
  - **Any**. The rule applies to all computers and devices on your LAN or DMZ.
  - **Single address**. The rule applies to the address of a particular computer.
  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule is applied to a group of computers. (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 computers and network devices and is generally referred to as the network database, which is described in *Manage the Network Database* on page 97. Computers and network devices are entered into the network database by various methods, which are described in *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 96.
  - **IP Groups**. The rule applies to a group of individual LAN IP addresses. Use the IP Groups screen (under the Network Security main navigation menu) to assign IP addresses to groups. For more information, see *Create IP Groups* on page 179. (LAN IP groups do not apply to DMZ WAN inbound rules.)
- **WAN users**. You can specify which Internet locations are covered by an inbound rule, based on their IP address:
  - **Any**. The rule applies to all Internet IP address.
  - **Single address**. The rule applies to a single Internet IP address.

  - **Address range**. The rule applies to a range of Internet IP addresses.
  - **IP Groups**. The rule applies to a group of individual WAN IP addresses. Use the IP Groups screen (under the Network Security main navigation menu) to assign IP addresses to groups. For more information, see *Create IP Groups* on page 179.
- **Schedule**. You can configure three different schedules to specify when a rule is applied. Once a schedule is configured, it affects all rules that use this schedule. You specify the days of the week and time of day for each schedule. For more information, see *Set a Schedule to Block or Allow Specific Traffic* on page 189.
- **Bandwidth profile**. You can define bandwidth profiles and then apply them to inbound LAN WAN rules to limit traffic. (You cannot apply bandwidth profiles to DMZ WAN rules.) For information about how to define bandwidth profiles, see *Create Bandwidth Profiles* on page 181.

Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port triggering feature requires that you know the port numbers used by the application. Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a request from the LAN network. As such, it would be handled in accordance with the inbound port forwarding rules, and most likely would be blocked.

For the procedure on how to configure port triggering, see *Configure Port Triggering* on page 197.

DMZ Port

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions when compared to the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. The fourth LAN port on the VPN firewall (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 information about how to enable the DMZ port, see *Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic* on page 114. For the procedures about how to configure DMZ traffic rules, see *Configure DMZ WAN Rules* on page 152.

Exposed Hosts

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined. For an example of how to set up an exposed host, see *IPv4 LAN WAN or IPv4 DMZ WAN Inbound Rule: Specifying an Exposed Host* on page 167.

VPN, L2TP, and PPTP Tunnels

The VPN firewall supports site-to-site IPSec VPN tunnels, dedicated SSL VPN tunnels, L2TP tunnels, and PPTP tunnels. Each tunnel requires extensive processing for encryption and authentication, thereby increasing traffic through the WAN ports.

For information about IPSec VPN, L2TP, and PPTP tunnels, see *Chapter 5, Virtual Private Networking Using IPSec and L2TP Connections*. For information about SSL VPN tunnels, see *Chapter 6, Virtual Private Networking Using SSL Connections*.

Use QoS and Bandwidth Assignment to Shift the Traffic Mix

By setting the QoS priority and assigning bandwidth profiles to firewall rules, you can shift the traffic mix to aim for optimum performance of the VPN firewall.

Set QoS Priorities

The QoS priority settings determine the Quality of Service for the traffic passing through the VPN firewall.

You can create and assign QoS profiles to WAN interfaces. For more information about QoS profiles for WAN interfaces, see *Configure WAN QoS Profiles* on page 76.

You can also create and assign a QoS profile (IPv4) or QoS priority (IPv6) to LAN WAN and DMZ WAN outbound firewall rules. The QoS is set individually for each firewall rule. 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 priority.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

For more information about QoS profiles, see *Create Quality of Service Profiles for IPv4 Firewall Rules* on page 184 and *Quality of Service Priorities for IPv6 Firewall Rules* on page 186.

Assign Bandwidth Profiles

When you set the QoS priority, the WAN bandwidth does not change. You change the WAN bandwidth that is assigned to a service or application by applying a bandwidth profile to a LAN WAN inbound or outbound rule. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic, thus allocating LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN links.

For more information about bandwidth profiles, see *Create Bandwidth Profiles* on page 181.

Monitoring Tools for Traffic Management

The VPN firewall includes several tools that can be used to monitor the traffic conditions of the firewall and content-filtering engine and to monitor the users' access to the Internet and the types of traffic that they are allowed to have. See *Chapter 9, Monitor System Access and Performance*, for a description of these tools.

System Management

- *Change Passwords and Administrator and Guest Settings*
- *Configure Remote Management Access*
- *Use the Command-Line Interface*
- *Use a Simple Network Management Protocol Manager*
- *Manage the Configuration File*
- *Upgrade the Firmware*
- *Configure Date and Time Service*

Change Passwords and Administrator and Guest Settings

The default administrator and default guest passwords for the web management interface are both password. NETGEAR recommends that you change the password for the administrator account to a more secure password, and that you configure a separate secure password for the guest account.

Note: For general information about user accounts, passwords, and login settings, see *Configure User Accounts* on page 310 and *Set User Login Policies* on page 313.

➢ **To modify the administrator and guest passwords and idle time-out settings:**

1. Select **Users > Users**. The Users screen displays. (The following figure shows the VPN firewall's default users—admin and guest—and, as an example, several other users in the List of Users table.)

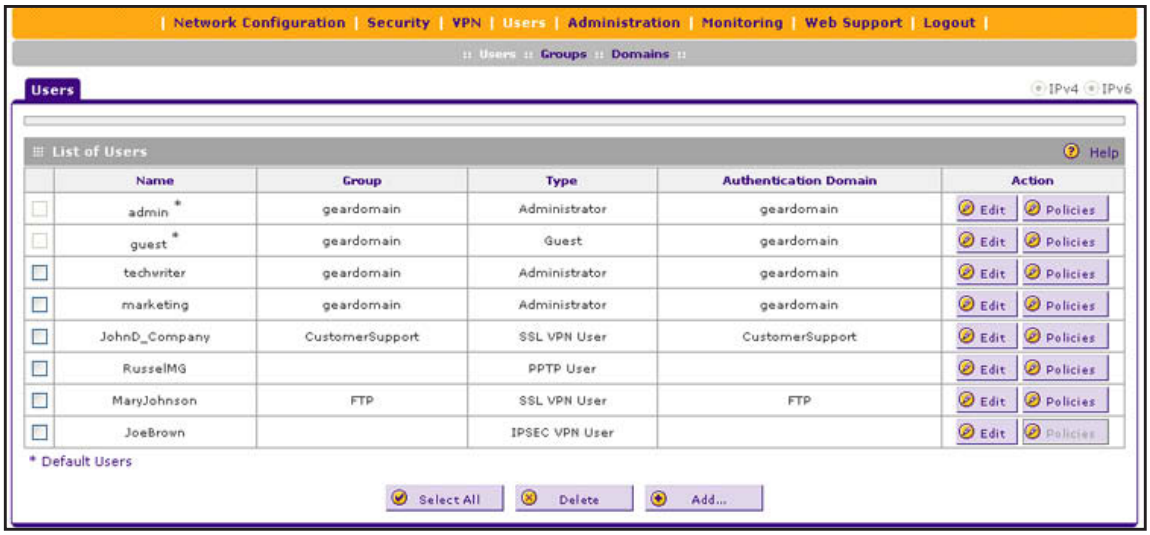

Figure 217.

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 Users screen displays:

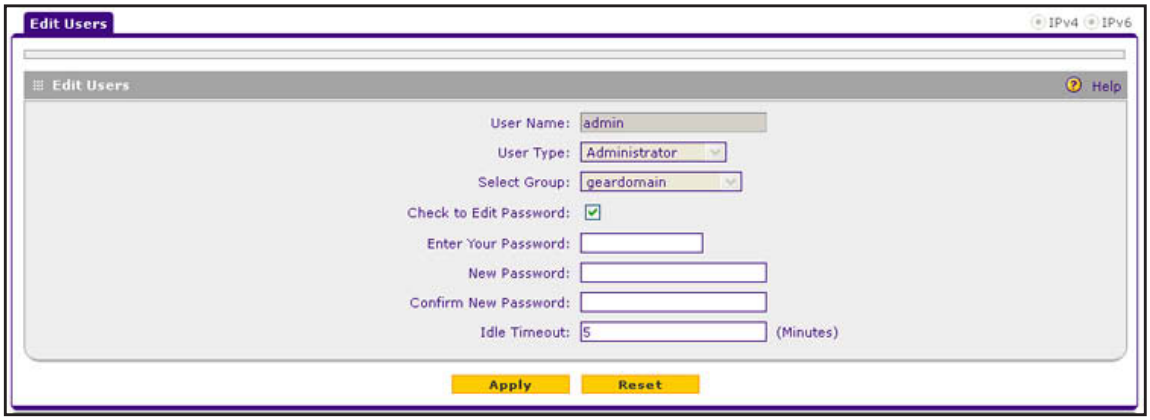

Figure 218.

You cannot modify the administrator user name, user type, or group assignment.

3. Select the **Check to Edit Password** check box. The password fields become available.
4. Enter the old password, enter the new password, and confirm the new password.

> **Note:** The most secure password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 32 characters.

5. As an option, you can change the idle time-out for an administrator login session. Enter a new number of minutes in the Idle Timeout field. (The default setting is 5 minutes.)

6. Click **Apply** to save your settings.
7. Repeat *Step 1* through *Step 6* for the user with the name guest.

Note: After a factory defaults reset, the password and time-out value are changed back to password and 5 minutes, respectively.

You can also change the administrator login policies:

- Disable login. Deny login access.

Note: You obviously do not want to deny login access to yourself if you are logged in as an administrator.

- Deny login access from a WAN interface. By default, the administrator cannot log in from a WAN interface. You can change this setting to allow login access 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, you can change the administrator login policies as described in *Set User Login Policies* on page 313.

Configure Remote Management Access

An administrator can configure, upgrade, and check the status of the VPN firewall over the Internet through a Secure Sockets Layer (SSL) VPN connection.

Note: When remote management is enabled and administrative access through a WAN interface is granted (see *Configure Login Policies* on page 313), the VPN firewall's web management interface is accessible to anyone who knows its IP address and default password. Because a malicious WAN user can reconfigure the VPN firewall and misuse it in many ways, NETGEAR highly recommends that you change the admin and guest default passwords before

continuing (see *Change Passwords and Administrator and Guest Settings* on page 336).

➢ **To configure the VPN firewall for remote management:**

1. Select **Administration > Remote Management**. The Remote Management screen displays the IPv4 settings (see the next figure).
2. Specify the IP version for which you want to configure remote management:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default. Go to *Step 3*.

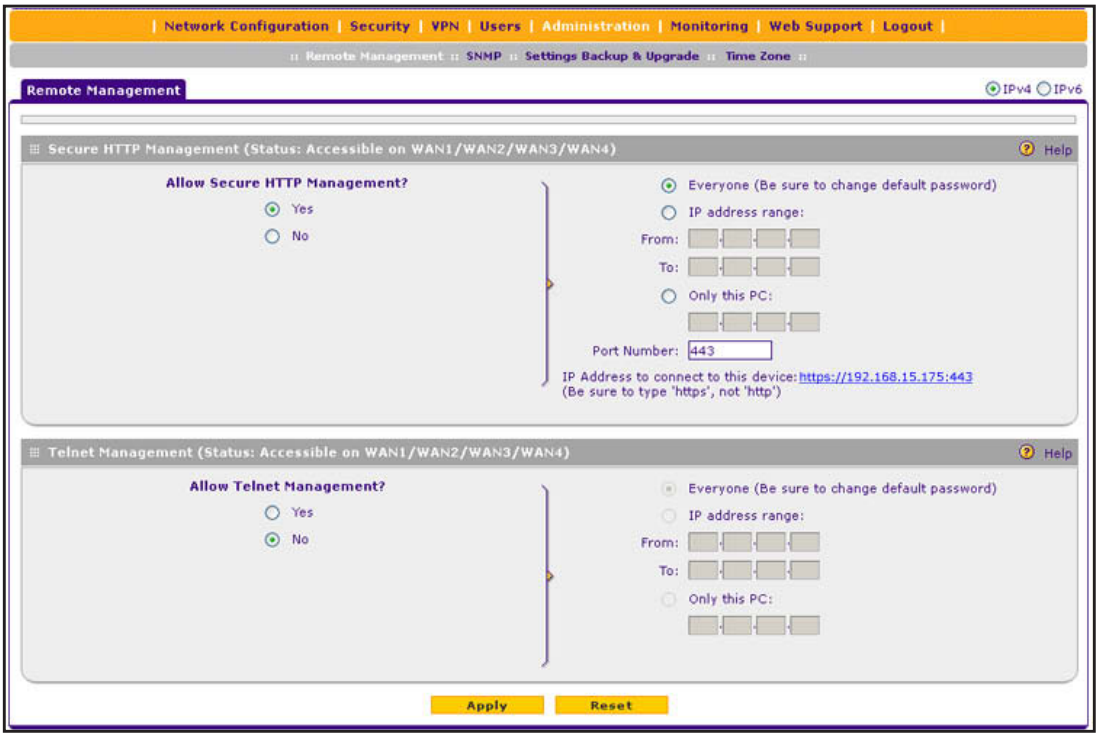

Figure 219. Remote Management screen for IPv4

   - **IPv6**. Select the **IPv6** radio button. The Remote Management screen displays the IPv6 settings:

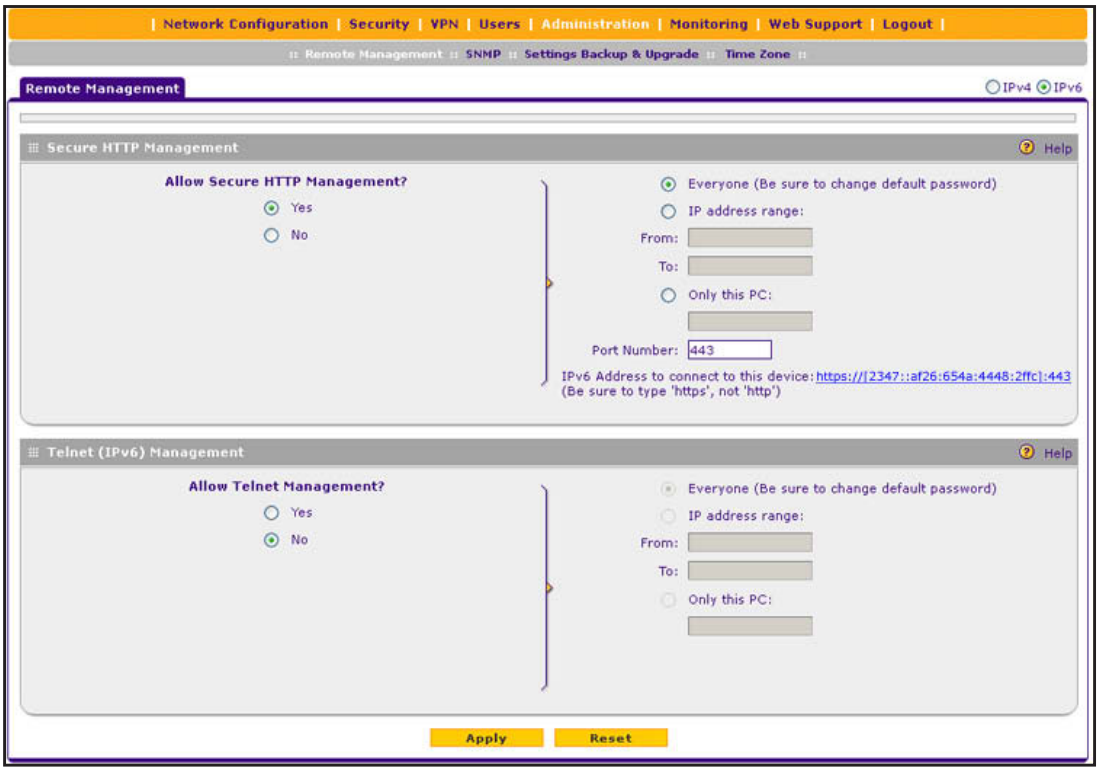

Figure 220. Remote Management screen for IPv6

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

Table 83. Remote Management screen settings for IPv4 and IPv6

Setting	Description
Secure HTTP Management	
Allow Secure HTTP Management?	To enable secure HTTP management, select the **Yes** radio button, which is the default setting. To disable secure HTTP management, select the **No** radio button. **Note:** The selected setting applies to all WAN interfaces.
	Specify the addresses through which access is allowed by selecting one of the following radio buttons: • **Everyone**. There are no IP address restrictions. • **IP address range**. Only users who use devices in the specified IP address range can securely manage over an HTTP connection. In the From fields, type the start IP address of the range; in the To fields, type the end IP address of the range. • **Only this PC**. Only a user who uses the device with the specified IP address can securely manage over an HTTP connection. Type the IP address in the fields.
	Port Number: Enter the port number through which access is allowed. The default port number is 443. **Note:** The URL through which you can securely manage over an HTTP connection displays below the Port Number field.

Table 83. Remote Management screen settings for IPv4 and IPv6 (continued)

Setting	Description
Telnet Management	
Allow Telnet Management?	To enable Telnet management, select the **Yes** radio button. To disable Telnet management, select the **No** radio button, which is the default setting.
	Specify the addresses through which access is allowed by selecting one of the following radio buttons: • **Everyone**. There are no IP address restrictions. • **IP address range**. Only users who use devices in the specified IP address range can manage over a Telnet connection. In the From fields, type the start IP address of the range; in the To fields, type the end IP address of the range. • **Only this PC**. Only a user who uses the device with the specified IP address can manage over a Telnet connection. Type the IP address in the fields.

WARNING:

If you are remotely connected to the VPN firewall and you select the No radio button to disable secure HTTP management, you and all other SSL VPN users are disconnected when you click Apply.

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

About Remote Access

When remote management is enabled, you need to use an SSL connection to access the VPN firewall from the Internet. You need to enter https:// (*not* http://) and type the VPN firewall's WAN IP address and port number in your browser. For example, if the VPN firewall's WAN IP address is 192.168.15.175 and the port number is 443, type the following in your browser: **https://192.168.15.175:443**.

The VPN firewall's remote login URL is:

https://<*IP_address*>:<*port_number*> or
https://<*FullyQualifiedDomainName*>:<*port_number*>

The IP address can be an IPv4 or IPv6 address.

Concerning security, note the following:

- For enhanced security, restrict access to as few external IP addresses as practical. See *Set User Login Policies* on page 313 for instructions on restricting administrator access by IP address.
- To maintain security, the VPN firewall rejects a login that uses http://*address* rather than the SSL https://*address*.
- The first time that you remotely connect to the VPN firewall with a browser through an SSL connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 7.0 or later, click **Yes** to accept the certificate.

Tip: If you are using a Dynamic DNS service such as TZO, you can identify the WAN IP address of your VPN firewall by running **tracert** from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter **tracert VPN firewall.mynetgear.net**, and the WAN IP address that your ISP assigned to the VPN firewall is displayed.

Use the Command-Line Interface

You can access the command-line interface (CLI) using the console port on the rear panel of the VPN firewall (see *Rear Panel* on page 19).

You can access the CLI from a communications terminal when the VPN firewall is still set to its factory defaults (or use your own settings if you have changed them).

➢ **To access the CLI:**

1. From your computer's command-line prompt, enter the following command:

   telnet *<ip address>*

   in which *ip address* is the IP address of the VPN firewall.

2. Enter **admin** and **password** when prompted for the login and password information (or enter **guest** and **password** to log in as a read-only guest).
3. Enter **exit** to end the CLI session.

Any configuration changes made through the CLI are not preserved after a reboot or power cycle unless you issue the CLI **save** command after making the changes.

Use a Simple Network Management Protocol Manager

Simple Network Management Protocol (SNMP) forms part of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems such as the NETGEAR ProSafe Network Management Software (NMS200) 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 the VPN firewall from an SNMP manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. The VPN firewall supports SNMPv1, SNMPv2c, and SNMPv3.

➢ **To configure the SNMP settings:**

1. Select **Administration > SNMP**. The SNMP screen displays. (The following figure contains an example.)

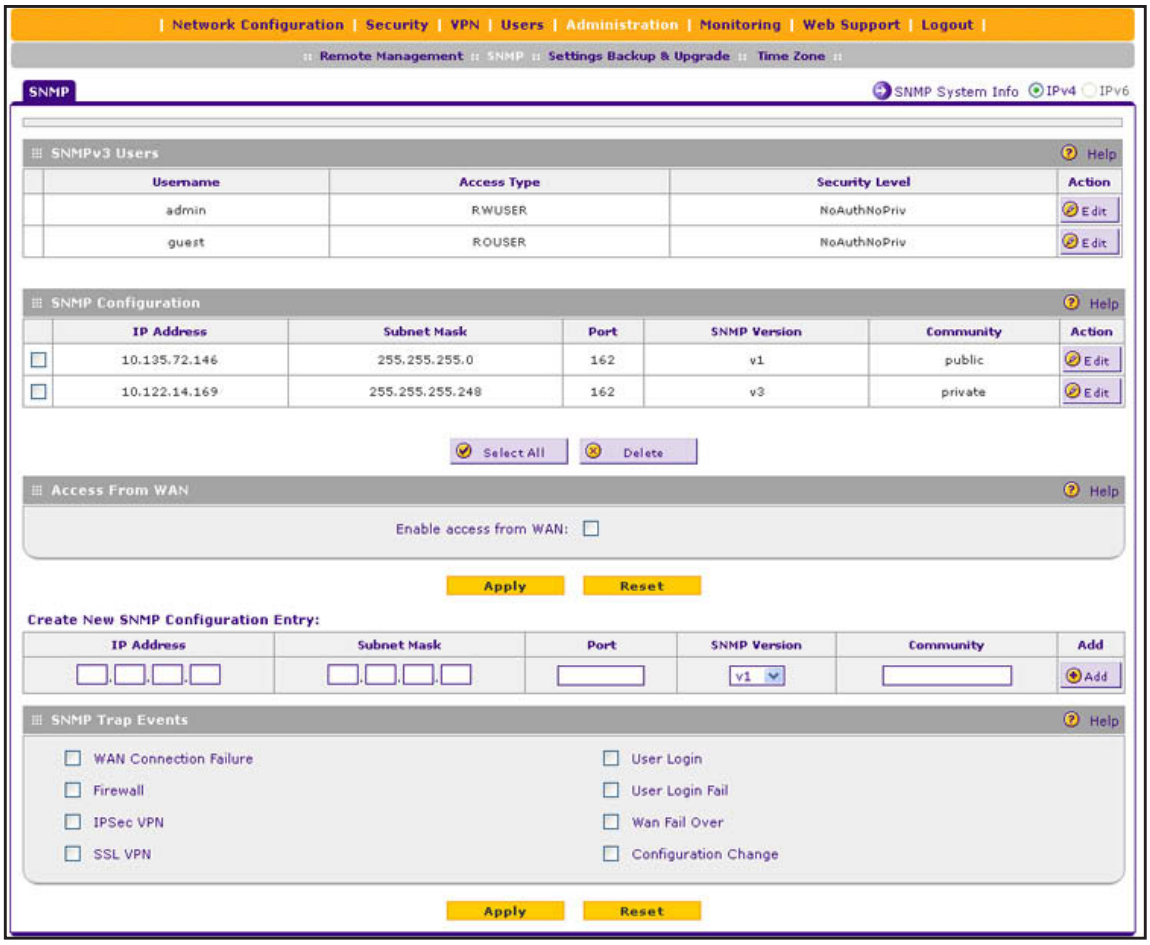

Figure 221.

The SNMPv3 Users table includes the default SNMPv3 users that are preconfigured on the VPN firewall. The SNMPv3 Users table shows the following columns:

- **Username**. The default user names (admin or guest).
- **Access Type**. Read-write user (RWUSER) or read-only user (ROUSER). By default, the user Admin is an RWUSER and the user guest is an ROUSER.
- **Security Level**. The level of security that indicates whether security is disabled:
  - **NoAuthNoPriv**. Both authentication and privacy are disabled.
  - **AuthNoPriv**. Authentication is enabled but privacy is disabled.
  - **AuthPriv**. Both authentication and privacy are enabled.

The SNMP Configuration table shows the following columns:

- **IP Address**. The IP address of the SNMP manager.
- **Subnet Mask**. The subnet mask of the SNMP manager.
- **Port**. The trap port number of the SNMP manager.
- **SNMP Version**. The SNMP version (v1, v2c, or v3).
- **Community**. The trap community string of the SNMP manager.

2. To specify a new SNMP configuration, in the Create New SNMP Configuration Entry section of the screen, configure the settings as described in the following table:

Table 84. SNMP screen settings

Setting	Description
Access From WAN	
Enable access from WAN	To enable SNMP access by an SNMP manager through the WAN interface, select the **Enable access from WAN** check box. By default, this check box is cleared and access is disabled.
Create New SNMP Configuration Entry	
IP Address	Enter the IP address of the new SNMP manager.
Subnet Mask	Enter the subnet mask of the new SNMP manager. Note the following: • If you want to narrow down the number of devices that can access the VPN firewall through the host IP address and receive traps, enter an IP address with a subnet mask of 255.255.255.252. • If you want to allow a subnet to access the VPN firewall through the host IP address and receive traps, enter an IP address with a subnet mask of 255.0.0.0. The traps are received at the IP address, but almost the entire subnet has access through the community string.
Port	Enter the port number of the new SNMP manager. The default port number is 162.
SNMP Version	From the drop-down list, select the SNMP version: • **v1**. SNMPv1. • **v2c**. SNMPv2c. • **v3**. SNMPv3.
Community	Enter the community string that allows the SNMP manager access to the MIB objects of the VPN firewall for the purpose of reading only.
SNMP Trap Events	
Select the check boxes to specify which SNMP trap events are sent to an SNMP manager: • **WAN Connection Failure**. Sent when the WAN connection fails. • **Firewall**. Sent when a new connection is initiated through addition of a custom firewall rule. • **IPSec VPN**. Sent when an IPSec VPN tunnel is established or disconnected. • **SSL VPN**. Sent when an SSL VPN tunnel is established or disconnected. • **User Login**. Sent when a user logs in to the VPN firewall. • **User Login Fail**. Sent when a user attempt to log in to the VPN firewall but fails to do so. • **Wan Fail Over**. Sent when an auto-rollover occurs from one WAN interface to another. • **Configuration Change**. Sent when the configuration of the VPN firewall changes.	

3. Click **Add** to add the new SNMP configuration to the SNMP Configuration table.

➢ **To edit an SNMP configuration:**

1. On the SNMP screen (see the previous figure), click the **Edit** button in the Action column of the SNMP Configuration table for the SNMP configuration that you want to modify. The Edit SNMP screen displays:

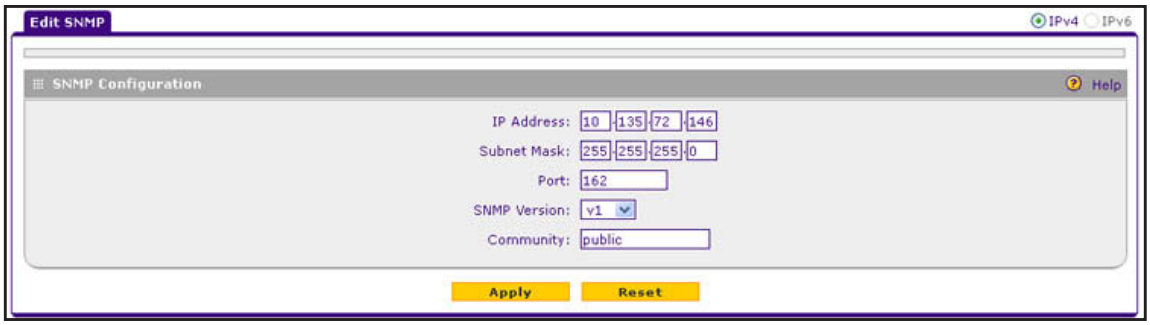

Figure 222.

2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more SNMP configurations:**

1. On the SNMP screen (see *Figure 221* on page 343), select the check box to the left of each SNMP configuration that you want to delete, or click the **Select All** table button to select all SNMP configurations.
2. Click the **Delete** table button.

➢ **To edit the SNMPv3 default users:**

1. On the SNMP screen (see *Figure 221* on page 343), click the **Edit** button in the Action column of the SNMPv3 User table for the SNMPv3 default user that you want to modify. The Edit User screen displays:

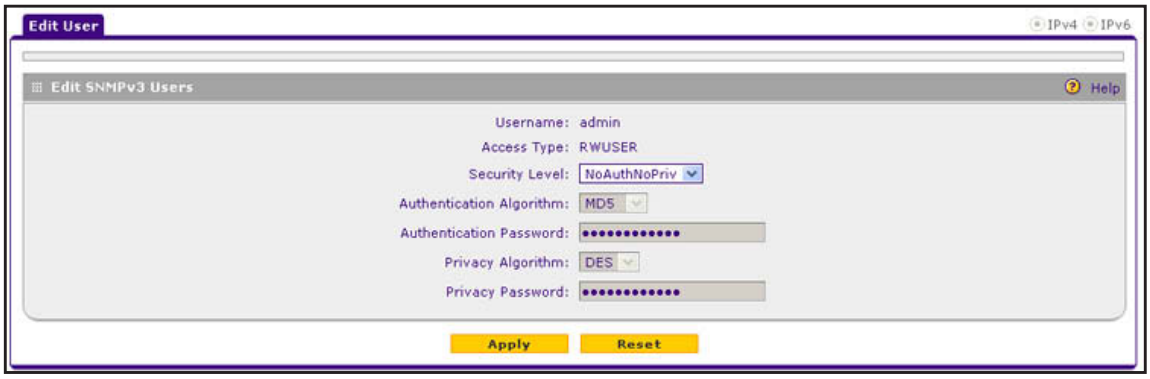

Figure 223.

2. Configure the settings as described in the following table:

Table 85. Edit User screen settings for SNMPv3 users

Setting	Description
Username	The default user name (admin or guest) for information only.
Access Type	The default access type (RWUSER or ROUSER) for information only.

Table 85. Edit User screen settings for SNMPv3 users (continued)

Setting	Description
Security Level	From the drop-down list, select the security level for communication between the SNMPv3 user and the SNMP agent that collects the MIB objects from the VPN firewall: • **NoAuthNoPriv**. Both authentication and privacy are disabled. This is the default setting. • **AuthNoPriv**. Authentication is enabled but privacy is disabled. Make a selection from the Authentication Algorithm drop-down list and enter an authentication password. • **AuthPriv**. Authentication and privacy are enabled. Make a selection from the Authentication Algorithm drop-down list and enter an authentication password. In addition, make a selection from the Privacy Algorithm drop-down list and enter a privacy password.
Authentication Algorithm	From the drop-down list, select the protocol for authenticating an SNMPv3 user: • **MD5**. Message Digest 5. This is a hash algorithm that produces a 128-bit digest. • **SHA1**. Secure Hash Algorithm 1. This is a hash algorithm that produces a 160-bit digest.
Authentication Password	The authentication password that an SNMPv3 user needs to enter to be granted access to the SNMP agent that collects the MIB objects from the VPN firewall.
Privacy Algorithm	From the drop-down list, select the encryption method for the communication between an SNMPv3 user and the SNMP agent that collects the MIB objects from the VPN firewall: • **DES**. Data Encryption Standard. • **AES**. Advanced Encryption Standard.
Privacy Password	The privacy password that an SNMPv3 user needs to enter to allow decryption of the MIB objects that the SNMP agent collects from the VPN firewall.

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

➢ **To configure the SNMP system information:**

1. On the SNMP screen (see *Figure 221* on page 343), click the **SNMP System Info** option arrow in the upper right of the screen. The SNMP SysConfiguration screen displays:

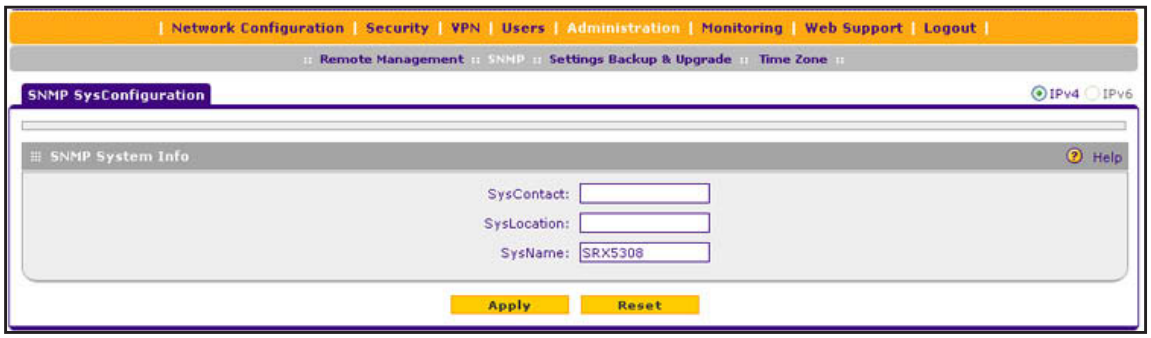

Figure 224.

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

Table 86. SNMP SysConfiguration screen settings

Setting	Description
SysContact	Enter the SNMP system contact information that is available to the SNMP manager. This setting is optional.
SysLocation	Enter the physical location of the VPN firewall. This setting is optional.
SysName	Enter the name of the VPN firewall for SNMP identification purposes. The default name is SRX5308.

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

Manage the Configuration File

The configuration settings of the VPN firewall are stored in a configuration file on the VPN firewall. This file can be saved (backed up) to a computer, retrieved (restored) from the computer, cleared to factory default settings, or upgraded to a new version.

Once the VPN firewall is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the VPN firewall settings from this file.

The Backup & Restore Settings screen lets you:

- Back up and save a copy of the current settings (see *Back Up Settings* on page 348)
- Restore saved settings from the backed-up file (see *Restore Settings* on page 349)
- Revert to the factory default settings (see *Revert to Factory Default Settings* on page 349)
- Upgrade the firmware (see *Upgrade the Firmware* on page 350)
- Reboot the VPN firewall with a different firmware version (see *Select the Firmware and Reboot the VPN Firewall* on page 351).

To display the Settings Backup and Firmware Upgrade screen, select **Administration > Settings Backup & Upgrade**.

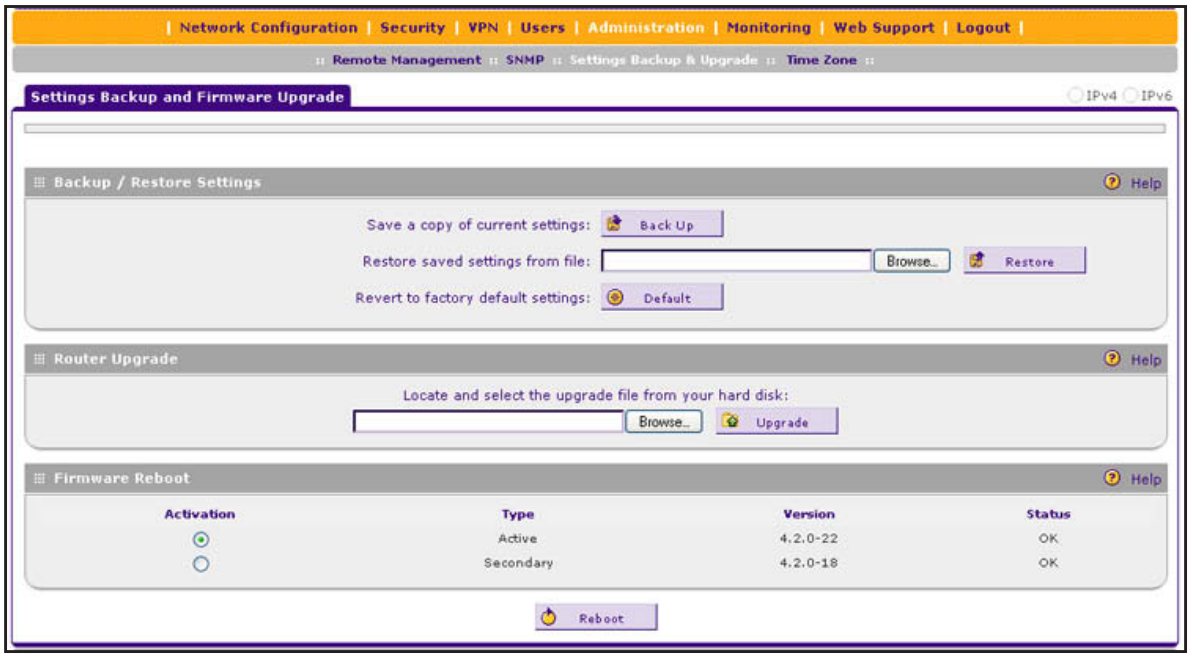

Figure 225.

Back Up Settings

The backup feature saves all VPN firewall settings to a file. Back up your settings periodically, and store the backup file in a safe place.

Tip: You can use a backup file to export all settings to another VPN firewall that has the same language and management software versions. Remember to change the IP address of the second VPN firewall before deploying it to eliminate IP address conflicts on the network.

➢ **To back up settings:**

1. On the Settings Backup and Firmware Upgrade screen (see *Figure 225* on page 348), next to Save a copy of current settings, click the **Backup** button to save a copy of your current settings. A screen displays, showing the file name of the backup file (SRX5308.cfg).
2. Select **Save file**, and click **OK**.
3. Open the folder in which you have saved the backup file, and verify that it has been saved successfully.

Note the following:

- If your browser is not configured to save downloaded files automatically, locate the folder in which you want to save the file, specify the file name, and save the file.
- If your browser is configured to save downloaded files automatically, the file is saved to your browser's download location on the hard disk.

Restore Settings

WARNING:

Restore only settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the VPN firewall system software.

➢ **To restore settings from a backup file:**

1. On the Settings Backup and Firmware Upgrade screen (see *Figure 225* on page 348), next to Restore saved settings from file, click **Browse**.
2. Locate and select the previously saved backup file (by default, SRX5308.cfg).
3. After you have selected the file, click the **Restore** button. A warning message might display, and you might have to confirm that you want to restore the configuration.

The VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete 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 VPN firewall, shut down the computer, or do anything else to the VPN firewall until the settings have been fully restored.

Revert to Factory Default Settings

➢ **To reset the VPN firewall to the original factory defaults settings:**

Use one of the following two methods:

- Using a sharp object, press and hold the factory default **Reset** button on the rear panel of the VPN firewall (see *Rear Panel* on page 19) for about 8 seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default settings when you do not know the administration password or IP address, you need to use the factory default Reset button method.
- On the Settings Backup and Firmware Upgrade screen (see the *Figure 225* on page 348), next to Revert to factory defaults settings, click the **Default** button, and confirm your selection.

The VPN firewall reboots. If you use the software Default button, the Settings Backup and Firmware Upgrade screen might remain visible during the reboot process, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

WARNING:

When you press the hardware factory default Reset button or click the software Default button, the VPN firewall settings are erased. All firewall rules, VPN policies, LAN and WAN settings, and other settings are lost. Back up your settings if you intend on using them.

Note: After you reboot with factory default settings, the VPN firewall's password is **password**, and the LAN IP address is **192.168.1.1**.

Upgrade the Firmware

You can install a different version of the VPN firewall firmware from the Settings Backup and Firmware Upgrade screen. To view the current version of the firmware that the VPN firewall is running, from the main menu, select **Monitoring**. The Router Status screen displays, showing the firmware version in the System Info section of the screen. After you have upgraded the firmware, the new firmware version is displayed.

➢ **To download a firmware version and upgrade the firmware:**

1. Go to the NETGEAR website at *http://support.netgear.com*.
2. Navigate to the SRX5308 support page, and click the **Downloads** tab.
3. Click the desired firmware version to reach the download page. Be sure to read the release notes on the download page before upgrading the VPN firewall's software.
4. On the Settings Backup and Firmware Upgrade screen of the VPN firewall (see *Figure 225* on page 348), in the Router Upgrade section, click **Browse**.
5. Locate and select the downloaded firmware file.
6. Click **Upload**. The upgrade process starts.

   During the upgrade process, the Settings Backup and Firmware Upgrade screen remains visible and a status bar shows the progress of the upgrade process. The upgrade process can take up to 10 minutes. When the status bar shows that the upgrade process is complete, it can take another 10 minutes before the VPN firewall reboots.

WARNING:

After you have started the firmware installation process, do *not* interrupt the process. Do not try to go online, turn off the VPN firewall, or do anything else to the VPN firewall until the VPN firewall has fully rebooted.

7. When the reboot process is complete, log in to the VPN firewall again. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

The newly installed firmware is the active firmware. The previously installed firmware has become the secondary firmware.

8. Select **Monitoring**. The Router Status screen displays, showing the new firmware version in the System Info section of the screen.

Note: In some cases, such as a major upgrade, it might be necessary to erase the configuration and manually reconfigure your VPN firewall after upgrading it. See the firmware release notes that NETGEAR makes available.

Select the Firmware and Reboot the VPN Firewall

After you have upgraded the firmware, the newly installed firmware is the active firmware, and the previously installed firmware has become the secondary firmware. However, you can still revert to the secondary firmware.

On the Settings Backup and Firmware Upgrade screen (see *Figure 225* on page 348), the Firmware Reboot section shows the following information fields for both the active and secondary (that is, nonactive) firmware:

- **Type**. Active or secondary firmware.
- **Version**. The firmware version.
- **Status**. The status of the firmware (*OK* or *Corrupted*).

➢ **To reboot the VPN firewall with a different firmware version:**

1. On the Settings Backup and Firmware Upgrade screen (see *Figure 225* on page 348), in the Firmware Reboot section, select the Activation radio button to the left of the firmware type (Active or Secondary) that you want to load onto the VPN firewall.
2. Click **Reboot**.

The VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

WARNING:

After you have started the firmware installation process, do *not* interrupt the process. Do not try to go online, turn off the VPN firewall, or do anything else to the VPN firewall until the settings have been fully restored.

3. When the reboot process is complete, log in to the VPN firewall again. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

4. Select **Monitoring**. The Router Status screen displays, showing the selected firmware version in the System Info section of the screen.

Configure Date and Time Service

Configure date, time, and NTP server designations on the System Date & Time screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Setting the correct system time and time zone ensures that the date and time recorded in the VPN firewall logs and reports are accurate.

➢ **To set time, date, and NTP servers:**

1. Select **Administration > Time Zone**. The Time Zone screen displays:

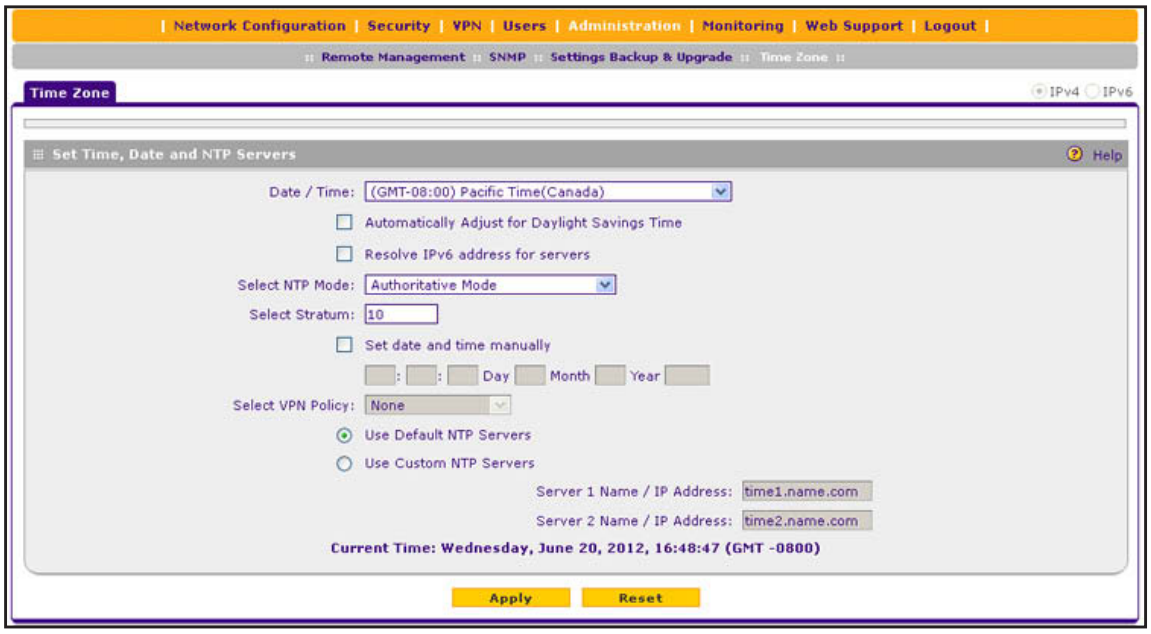

Figure 226.

The bottom of the screen display the current weekday, date, time, time zone, and year (in the example in the previous figure: Current Time: Wednesday, June 20, 2012, 16:48:47 (GMT -0800).

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

Table 87. Time Zone screen settings

Setting	Description
Date/Time	From the drop-down list, select the local time zone in which the VPN firewall operates. The correct time zone is required in order for scheduling to work correctly.
Automatically Adjust for Daylight Savings Time	If daylight saving time is supported in your region, select the **Automatically Adjust for Daylight Savings Time** check box. By default, the check box is disabled.

Table 87. Time Zone screen settings (continued)

Setting	Description	
Resolve IPv6 address for servers	Select this check box to force the use of IPv6 addresses and FQDN (domain name) resolution in the Server 1 Name / IP Address and Server 2 Name / IP Address fields when you have selected the Use Custom NTP Servers radio button.	
Select NTP Mode	In all three NTP modes, the VPN firewall functions both as a client and a server. The VPN firewall synchronizes its clock with the specified NTP server or servers and provides time service to clients. From the drop-down list, select the NTP mode: • **Authoritative Mode**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall's RTC provides time service to clients. In authoritative mode, you can enter a stratum value and set the date and time manually. • **Sync to NTP Servers on Internet**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall does *not* use its RTC. • **Sync to NTP Servers on VPN**. The VPN firewall synchronizes its clock with the specified NTP server on the VPN. If the server is unreachable, the VPN firewall does *not* use its RTC. You need to select a VPN policy that enables the VPN firewall to contact the NTP server on the VPN.	
	Select Stratum	In authoritative mode, enter a stratum value, which indicates the distance from a reference clock. The default value is 10, which specifies an unsynchronized local clock and causes NTP to use the VPN firewall's RTC when the specified NTP server is not available.
	Set date and time manually	This is an optional setting that is available in authoritative mode. Select the check box to unmask the time (hour, minute, second), Day, Month, and Year fields. Enter the date and time.
	Select VPN Policy	When the VPN firewall is configured to synchronize to an NTP server on the VPN, select the VPN policy from the drop-down list. For information about configuring VPN policies, see *Manage VPN Policies* on page 238.

Table 87. Time Zone screen settings (continued)

Setting	Description	
NTP Servers (default or custom)	Select one of the following radio buttons to specify the NTP servers: • **Use Default NTP Servers**. The VPN firewall regularly updates its RTC by contacting a default NETGEAR NTP server on the Internet. • **Use Custom NTP Servers**. The VPN firewall regularly updates its RTC by contacting one of two custom NTP servers (primary and backup), both of which you need to specify in the fields that become available with this selection. **Note:** If you select the Use Custom NTP Servers option but leave either the Server 1 or Server 2 field blank, both fields are set to the default NETGEAR NTP servers. **Note:** A list of public NTP servers is available at *http://support.ntp.org/bin/view/Servers/WebHome*.	
NTP Servers (custom)	Server 1 Name / IP Address	Enter the IP address or host name of the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name of the backup NTP server.

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

Note: If you select the default NTP servers or if you enter a custom server FQDN, the VPN firewall determines the IP address of the NTP server by performing a DNS lookup. Before the VPN firewall can perform this lookup, you need to configure a DNS server address on the WAN IPv4 ISP Settings screen (see *Manually Configure an IPv4 Internet Connection* on page 34.)

Monitor System Access and Performance

9

This chapter describes the system-monitoring features of the VPN firewall. You can be alerted to important events such 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. The chapter contains the following sections:

- *Configure and Enable the WAN Traffic Meter*
- *Configure and Enable the LAN Traffic Meter*
- *Configure Logging, Alerts, and Event Notifications*
- *View Status Screens*
- *Diagnostics Utilities*

Note: All log and report functions that are part of the Firewall Logs & E-mail screen and some of the functions that are part of the Diagnostics screen require that you configure the email notification server—see *Configure Logging, Alerts, and Event Notifications* on page 362.

Configure and Enable the WAN Traffic Meter

If your ISP charges by traffic volume over a given period, or if you want to study traffic types over a period, you can activate the traffic meter for IPV4 traffic on a WAN port.

➢ **To configure and monitor traffic limits on a WAN port:**

1. Select **Monitoring > Traffic Meter**. The WAN Traffic Meter tabs display, with the WAN1 Traffic Meter screen in view.

   The Internet Traffic Statistics section in the lower part of the screen displays statistics on Internet traffic through the WAN port. If you have not enabled the traffic meter, these statistics are not available.

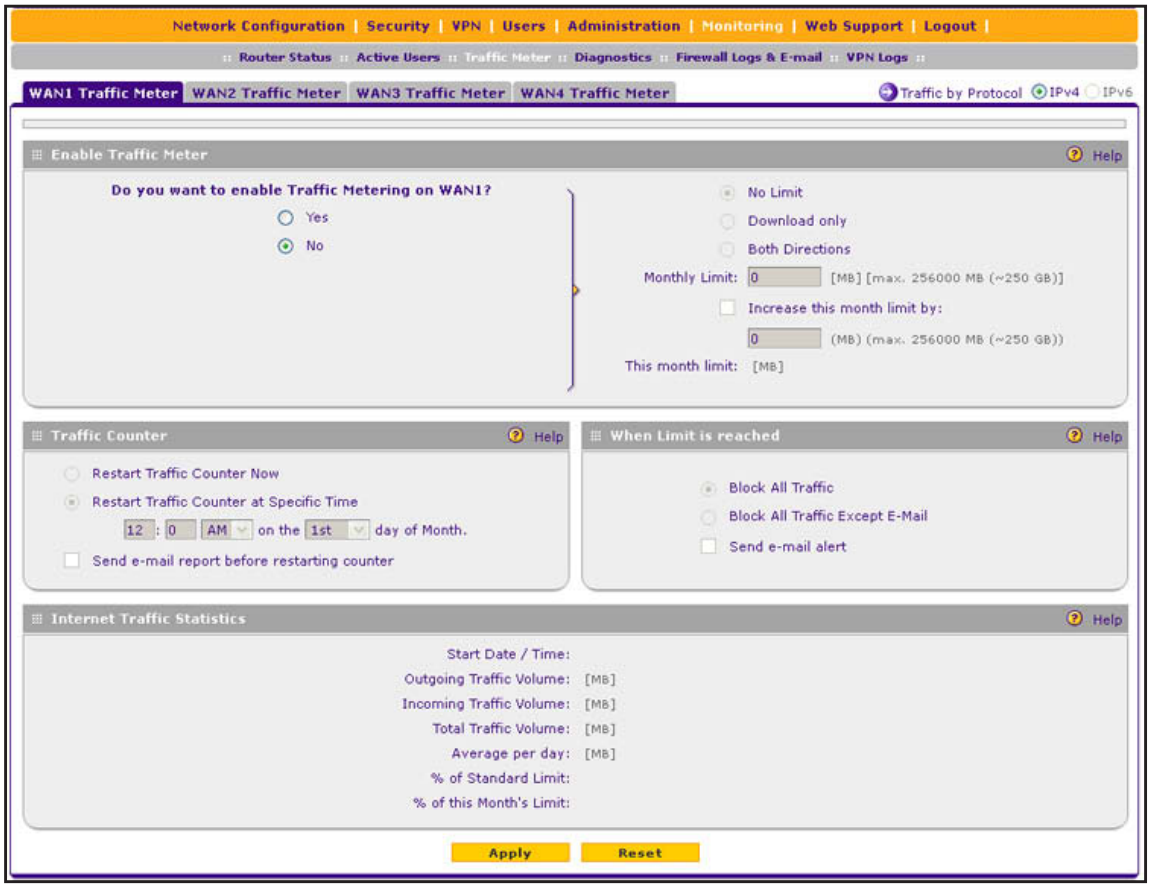

Figure 227.

2. Enter the settings for the WAN1 interface as described in the following table. If you want to configure the settings for another WAN interface, first select the associated tab for that interface.

Table 88. WAN1 Traffic Meter screen settings

Setting	Description	
Enable Traffic Meter		
Do you want to enable Traffic Metering on WAN1?	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 WAN interface. Complete the fields that are shown on the right side of the screen (see explanations later in this table). • **No**. Traffic metering is disabled. This is the default setting.	
	Select one of the following radio buttons to specify if or how the VPN firewall applies restrictions when the traffic limit is reached: • **No Limit**. No restrictions are applied when the traffic limit is reached. • **Download only**. Restrictions are applied to incoming traffic when the traffic limit is reached. Fill in the Monthly Limit field. • **Both Directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached. Fill in the Monthly Limit field.	
	Monthly Limit	Enter the monthly traffic volume limit in MB. The default setting is 0 MB.
	Increase this month limit by	Select this check box to temporarily increase a previously specified monthly traffic volume limit, and enter the additional allowed volume in MB. The default setting is 0 MB. **Note:** When you click Apply to save these settings, this field is reset to 0 MB so that the increase is applied only once.
	This month limit	This is a nonconfigurable field that displays the total monthly traffic volume limit that applies 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 select **AM** or **PM** and the day of the month from the drop-down lists.	
Send e-mail report before restarting counter	An email report is sent immediately before the counter restarts. Ensure that emailing of logs is enabled on the Firewall Logs & E-mail screen (see *Configure Logging, Alerts, and Event Notifications* on page 362).	

Table 88. WAN1 Traffic Meter screen settings (continued)

Setting	Description
When Limit is reached	
Block Traffic	Select one of the following radio buttons to specify which action the VPN firewall performs when the traffic limit has been reached: • **Block All Traffic**. All incoming and outgoing Internet and email traffic is blocked. • **Block All Traffic Except E-Mail**. All incoming and outgoing Internet traffic is blocked, but incoming and outgoing email traffic is still allowed.
Send e-mail alert	An email alert is sent when traffic is blocked. Ensure that emailing of logs is enabled on the Firewall Logs & E-mail screen (see *Configure Logging, Alerts, and Event Notifications* on page 362).

3. Click **Apply** to save your settings.
4. If you want to enable the traffic meter for another WAN interface, click the associated WAN Traffic Meter tab for that interface, and repeat *Step 2* and *Step 3* for that WAN interface.

The contents of the WAN2 Traffic Meter, WAN3 Traffic Meter, and WAN4 Traffic Meter screens are identical to the WAN1 Traffic Meter screen except for the WAN interface number.

To display a report of the Internet traffic by type for a WAN interface, click the **Traffic by Protocol** option arrow in the upper right of the associated WAN Traffic Meter screen. The Traffic by Protocol pop-up screen displays. The incoming and outgoing volume of traffic for each protocol and the total volume of traffic are displayed. Traffic counters are updated in MBs; the counter starts only when traffic passed is at least 1 MB. In addition, the pop-up screen displays the traffic meter's start and end dates. If you did not configure the traffic meter, the start date is blank.

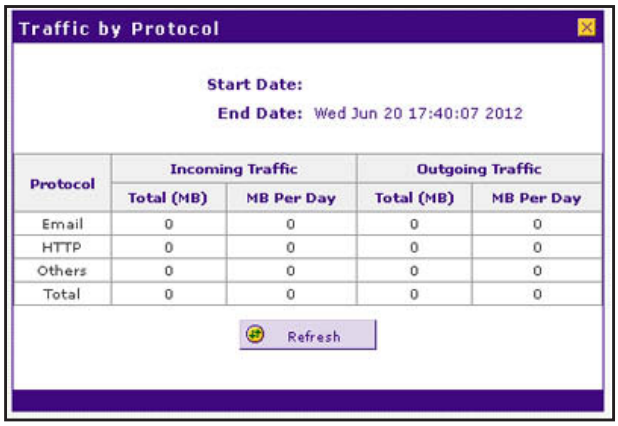

Figure 228.

Configure and Enable the LAN Traffic Meter

If your ISP charges by traffic volume over a period and you need to charge the costs to individual accounts, or if you want to study the traffic volume that is requested or sent over a LAN IP address over a period, activate the traffic meter for individual LAN IP addresses.

➢ **To configure and monitor traffic limits for LAN IP addresses:**

1. Select **Network Configuration > LAN Settings**. The LAN submenu tabs display, with the LAN Setup screen in view:

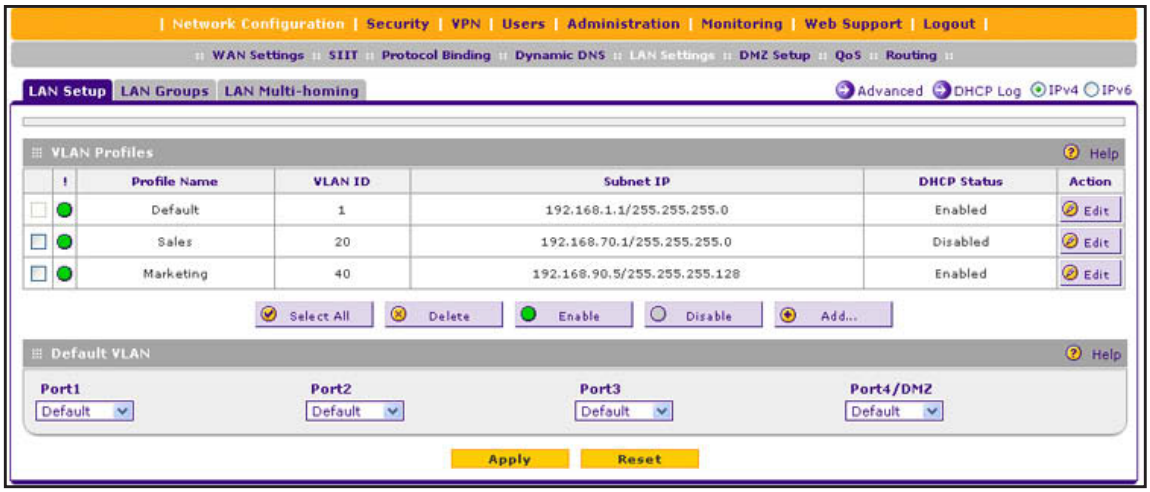

Figure 229.

2. Click the **Advanced** option arrow in the upper right of the LAN Setup screen. The IPv4 LAN Advanced screen displays.
3. Click the **LAN Traffic Meter** tab. The LAN Traffic Meter screen displays. (The following figure shows some examples in the LAN Traffic Meter Table.)

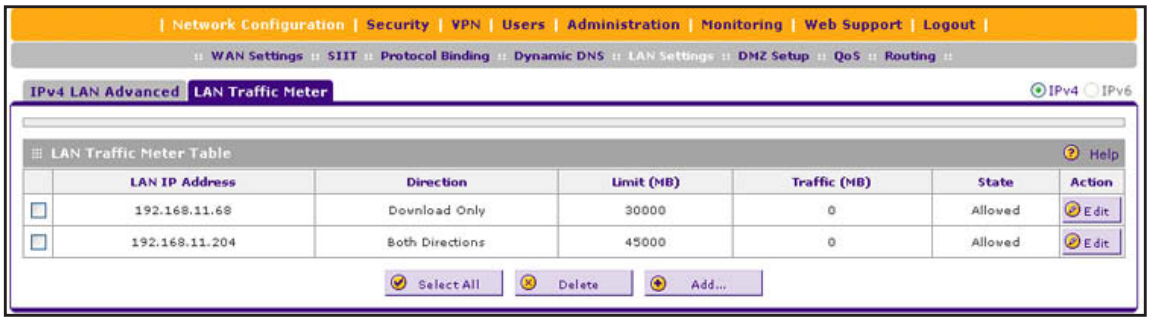

Figure 230.

The LAN Traffic Meter Table shows the following columns, all of which are described in detail in the table that follows the next figure:

- **LAN IP Address**. The LAN IP address that is subject to the traffic meter.
- **Direction**. The direction for which traffic is measured.
- **Limit (MB)**. The traffic limit in MB.

- **Traffic (MB)**. The traffic usage in MB.
- **State**. The state that indicates whether traffic to and from the IP address is allowed or blocked.
- **Action**. The Edit table button provides access to the Edit LAN Traffic Meter screen for the corresponding IP address.

4. On the LAN Traffic Meter screen, click the **Add** table button. The Add LAN Traffic Meter screen displays:

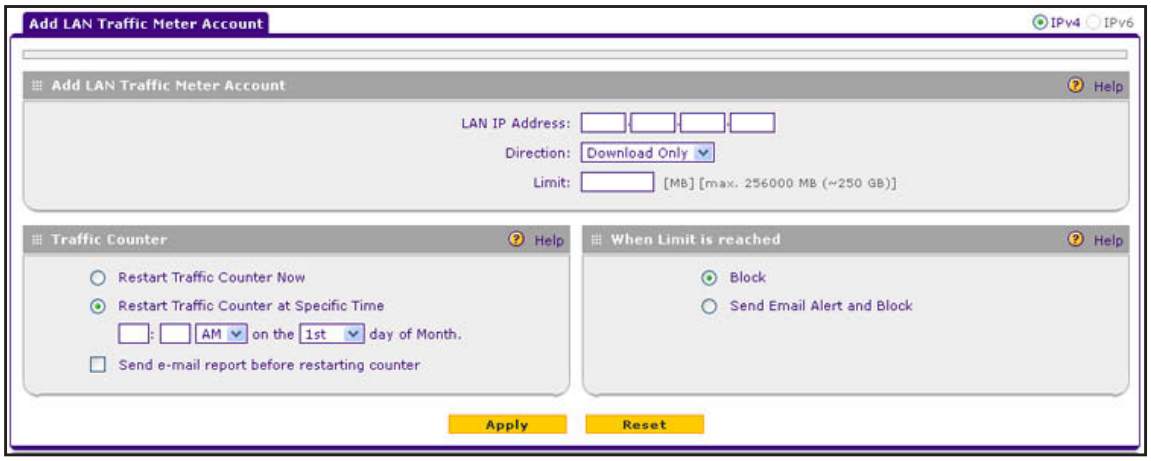

Figure 231.

5. Enter the settings as described in the following table:

Table 89. Add LAN Traffic Meter Account screen settings

Setting	Description
Add LAN Traffic Meter Account	
LAN IP Address	The LAN IP address for the account.
Direction	From the Direction drop-down list, select the direction in which traffic is measured: • **Inbound traffic**. Restrictions are applied to incoming traffic when the traffic limit is reached. • **Both directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached.
Limit	Enter the monthly traffic volume limit in MB. The default setting is 0 MB. The maximum limit that you can enter is 256,000 MB.
Traffic Counter	
Restart Traffic Counter	Select one of the following radio buttons to specify when the traffic counter restarts: • **Restart Traffic Counter Now**. The traffic counter restarts immediately after you click Apply. • **Restart Traffic Counter at a Specific Time**. Restart the traffic counter at a specific time and day of the month. Fill in the time fields and select the day of the month from the drop-down list.

Table 89. Add LAN Traffic Meter Account screen settings (continued)

Setting	Description
Send e-mail report before restarting counter	An email report is sent immediately before the counter restarts. Ensure that emailing of logs is enabled on the Firewall Logs & E-mail screen (see *Configure Logging, Alerts, and Event Notifications* on page 362).
When Limit is reached	
Block Traffic	Select one of the following radio buttons to specify what action the VPN firewall performs when the traffic limit has been reached: • **Block**. All incoming and outgoing Internet and email traffic is blocked. • **Send Email Alert and Block**. An email alert is sent when all incoming and outgoing Internet and email traffic is blocked. Ensure that emailing of logs is enabled on the Firewall Logs & E-mail screen (see *Configure Logging, Alerts, and Event Notifications* on page 362).

6. Click **Apply** to save your settings. The new account is added to the LAN Traffic Meter Table on the LAN Traffic Meter screen.

➢ **To view the LAN IP traffic meter statistics:**

In the LAN Traffic Meter Table, click the **Edit** table button to the right of the account for which you want to view the statistics. The Edit LAN Traffic Meter Account screen displays. This screen shows the same fields as the Add LAN Traffic Meter Account screen (see *Figure 231* on page 360), together with the statistics at the bottom of the screen:

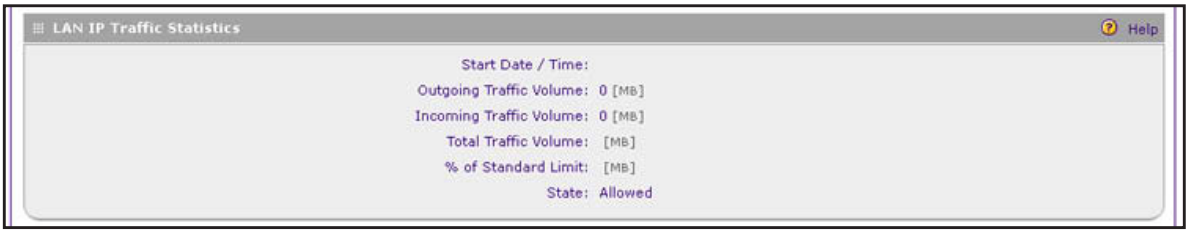

Figure 232.

➢ **To edit a LAN traffic meter account:**

1. In the LAN Traffic Meter Table, click the **Edit** table button to the right of the account that you want to edit. The Edit LAN Traffic Meter Account screen displays. This screen shows the same fields as the Add LAN Traffic Meter Account screen (see *Figure 231* on page 360).
2. Modify the settings as described in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more LAN traffic meter accounts:**

1. In the LAN Traffic Meter Table, select the check box to the left of the account that you want to delete, or click the **Select All** table button to select all accounts.
2. Click the **Delete** table button.

Configure Logging, Alerts, and Event Notifications

You can configure the VPN firewall to log routing events such as dropped and accepted packets, to log system events such as a change of time by an NTP server, secure login attempts, and reboots, and to log other events. You can also schedule logs to be sent to the administrator and enable logs to be sent to a syslog server on the network.

➢ **To configure and activate logs:**

1. Select **Monitoring > Firewall Logs & E-mail**. The Firewall Logs & E-mail screen displays:

Figure 233.

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

Table 90. Firewall Logs & E-mail screen settings

Setting	Description
Log Options	
Log Identifier	Enter the name of the log identifier. The identifier is appended to log messages to identify the device that sent the log messages. The default identifier is SRX5308.
Routing Logs	
In the Accepted Packets and Dropped Packets columns, select check boxes to specify which traffic is logged: • **LAN to WAN** • **LAN to DMZ** • **DMZ to WAN** • **WAN to LAN** • **DMZ to LAN** • **WAN to DMZ**	
System Logs Option	
Select the check boxes to specify which system events are logged: • **Change of Time by NTP**. Logs a message when the system time changes after a request from an NTP server. • **Login Attempts**. Logs a message when a login is attempted. Both successful and failed login attempts are logged. • **Secure Login Attempts**. Logs a message when a secure login is attempted. Both successful and failed secure login attempts are logged. • **Reboots**. Logs a message when the VPN firewall has been rebooted through the web management interface. (No message is logged when the factory default Reset button has been pressed.) • **All Unicast Traffic**. All incoming unicast packets are logged. • **All Broadcast/Multicast Traffic**. All incoming broadcast and multicast packets are logged. • **WAN Status**. WAN link status–related events are logged. • **Resolved DNS Names**. All resolved DNS names are logged. • **VPN**. All VPN negotiation messages are logged.	
Other Event Logs	
Source MAC Filter	Select this check box to log packets from MAC addresses that match the source MAC address filter settings.
Session Limit	Select this check box to log packets that are dropped because the session limit has been exceeded.
Bandwidth Limit	Select this check box to log packets that are dropped because the bandwidth limit has been exceeded.

Table 90. Firewall Logs & E-mail screen settings (continued)

Setting	Description	
Enable E-mail Logs		
Do you want logs to be emailed to you?	Select the **Yes** radio button to enable the VPN firewall to email logs to a specified email address. Complete the fields that are shown on the right side of the screen. Select the **No** radio button to prevent the logs from being emailed, which is the default setting.	
	E-Mail Server Address	The IP address or Internet name of your ISP's outgoing email SMTP server. **Note:** If you leave this field blank, the VPN firewall cannot send email logs and alerts.
	Return E-Mail Address	The email address of the sender for email identification purposes. For example, enter srx_alerts@company.com.
	Send to E-Mail Address	The email address to which the logs are sent. Typically, this is the email address of the administrator.
	Custom SMTP Port	Enter the port number of the SMTP server for the outgoing email.
	Select one of the following radio buttons to specify SMTP server authentication for the outgoing email: • **No Authentication**. The SMTP server does not require authentication. • **Login Plain**. The SMTP server requires authentication with regular login. Specify the user name and password to be used for authentication. • **CRAM-MD5**. The SMTP server requires authentication with CRAM-MD5 login. Specify the user name and password to be used for authentication.	
	Username	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.
	Respond to Identd from SMTP Server	To respond to Ident protocol messages, select the **Respond to Identd from SMTP Server** check box. The Ident protocol is a relatively weak scheme to verify the sender of an email. (A common daemon program for providing the Ident service is Identd.)
Send e-mail logs by Schedule		
Unit	Enter a schedule for sending the logs. From the Unit drop-down list, select one of the following: • **Never**. No logs are sent. • **Hourly**. The logs are sent every hour. • **Daily**. The logs are sent daily. Specify the time. • **Weekly**. The logs are sent weekly. Specify the day and time.	
Day	From the Day drop-down list, select the day on which the logs are sent.	
Time	From the Time drop-down list, select the hour on which the logs are sent, and select either the **a.m.** or **p.m.** radio button.	

Table 90. Firewall Logs & E-mail screen settings (continued)

Setting	Description	
Enable SysLogs		
Do you want to enable syslog?	To enable the VPN firewall to send logs to a specified syslog server, select the **Yes** radio button. Complete the fields that are shown on the right side of the screen. To prevent the logs from being sent, select the **No** radio button, which is the default setting.	
	SysLog Server	The IP address or FQDN of the syslog server.
	SysLog Severity	All the logs with a severity that is equal to and above the severity that you specify are logged on the specified syslog server. For example, if you select LOG_CRITICAL as the severity, the logs with the severities LOG_CRITICAL, LOG_ALERT, and LOG_EMERG are logged. Select one of the following syslog severities from the drop-down list: • **LOG DEBUG**. Debug-level messages. • **LOG INFO**. Informational messages. • **LOG NOTICE**. There are normal but significant conditions. • **LOG WARNING**. There are warning conditions. • **LOG ERROR**. There are error conditions. • **LOG CRITICAL**. There are critical conditions. • **LOG ALERT**. An action has to be taken immediately. • **LOG EMERG**. The VPN firewall is unusable.

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

Note: Enabling routing and other event logs might generate a significant volume of log messages. NETGEAR recommends that you enable firewall logs for debugging purposes only.

➢ **To view the routing logs, system logs, and other event logs onscreen:**

1. Select **Monitoring > Firewall Logs & E-mail**. The Firewall Logs & E-mail screen displays.
2. Click the **View Log** option arrow in the upper right of the Firewall Logs & E-mail screen. The View Log screen displays:

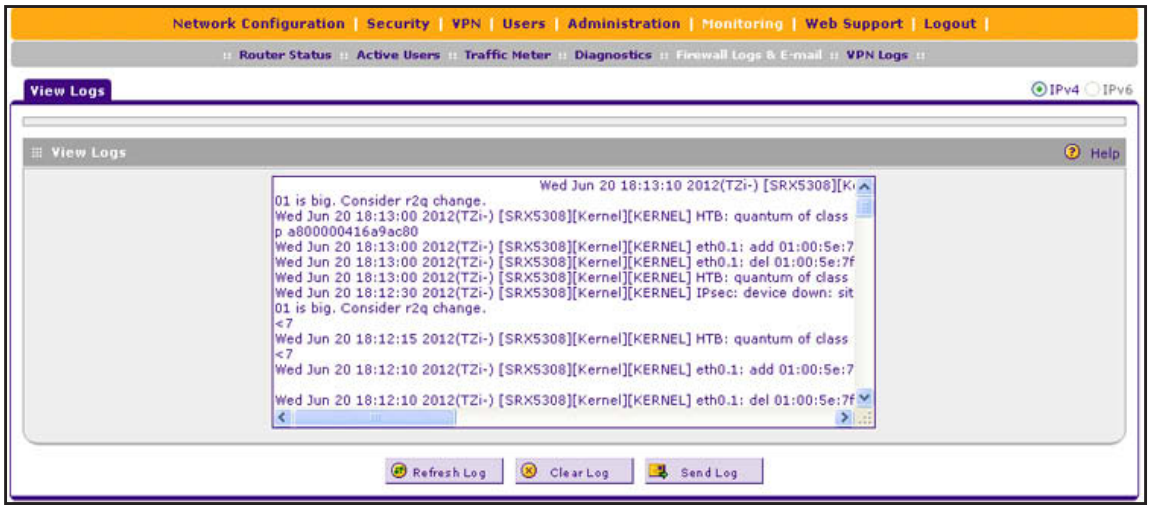

Figure 234.

You can refresh the logs, clear the logs, or send the logs to an email address.

➢ **To view the DNS logs onscreen:**

1. Select **Monitoring > Firewall Logs & E-mail**. The Firewall Logs & E-mail screen displays.
2. Click the **DNS Logs** option arrow in the upper right of the Firewall Logs & E-mail screen. The DNS Logs screen displays:

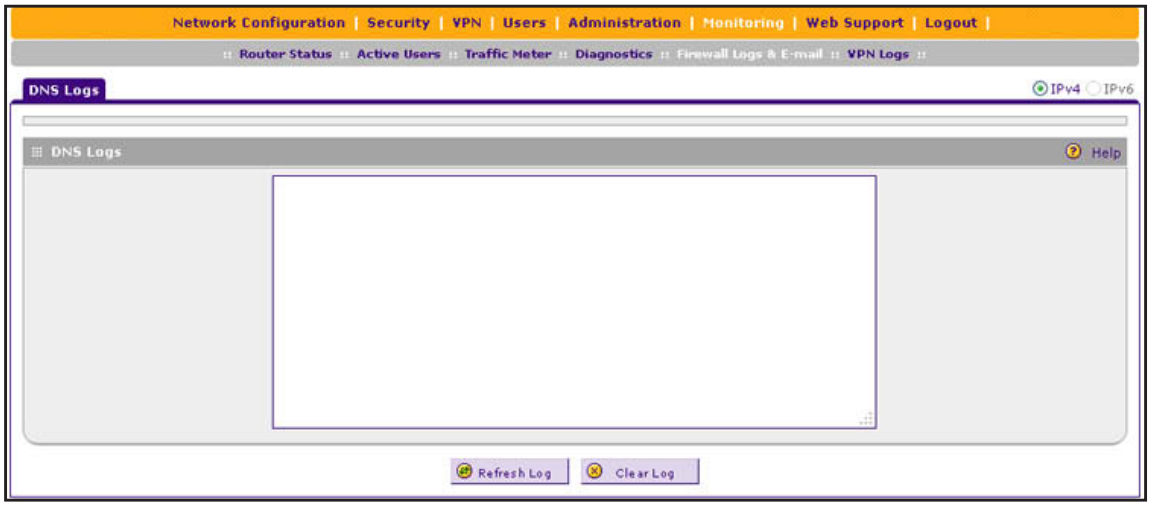

Figure 235.

You can refresh the logs or clear the logs.

How to Send Syslogs over a VPN Tunnel between Sites

➢ **To send syslogs from one site to another over a gateway-to-gateway VPN tunnel:**

1. At Site 1, set up a syslog server that is connected to Gateway 1.
2. Set up a VPN tunnel between Gateway 1 at Site 1 and Gateway 2 at Site 2.
3. Change the remote IP address in the VPN policy on Gateway 1 to the WAN IP address of Gateway 2.
4. Change the local IP address in the VPN policy on Gateway 2 to the WAN IP address of Gateway 2.
5. At Site 2, specify that Gateway 2 should send the syslogs to the syslog server at Site 1.

The following sections describe steps 2 through 4, using the topology that is described in the following table:

Type of Address	Gateway 1 at Site 1	Gateway 2 at Site 2
WAN IP address	10.0.0.1	10.0.0.2
LAN IP address	192.168.10.0	192.168.20.0
LAN subnet mask	255.255.255.0	255.255.255.0
LAN IP address syslog server	192.168.10.2	Not applicable

Configure Gateway 1 at Site 1

➢ **To create a gateway-to-gateway VPN tunnel to Gateway 2, using the IPSec VPN wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays.
2. Configure a gateway-to-gateway VPN tunnel using the following information:
   - Connection name. Any name of your choice
   - Pre-shared key. Any key of your choice
   - Remote WAN IP address. 10.0.0.2
   - Local WAN IP address. 10.0.0.1
   - Remote LAN IP Address. 192.168.20.0
   - Remote LAN subnet mask. 255.255.255.0
3. Click **Apply** to save the settings.

➢ **To change the remote IP address in the VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policy screen displays.
2. Next to the policy name for the Gateway 1–to–Gateway 2 autopolicy, click **Edit**. The Edit VPN Policy screen displays.
3. In the General section of the screen, clear the **Enable NetBIOS** check box.

4. In the Traffic Selector section of the screen, make the following changes:
   - From the Remote IP drop-down list, select **Single**.
   - In the Start IP fields, type **10.0.0.2**, which is the WAN IP address of Gateway 2.
5. Click **Apply** to save the settings.

Configure Gateway 2 at Site 2

➢ **To create a gateway-to-gateway VPN tunnel to Gateway 1, using the IPSec VPN wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays.
2. Configure a gateway-to-gateway VPN tunnel using the following information:
   - Connection name. Any name of your choice
   - Pre-shared key. The same key as you configured on Gateway 1
   - Remote WAN IP address. 10.0.0.1
   - Local WAN IP address. 10.0.0.2
   - Remote LAN IP Address. 192.168.10.0
   - Remote LAN subnet mask. 255.255.255.0
3. Click **Apply** to save the settings.

➢ **To change the local IP address in the VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policy screen displays.
2. Next to the policy name for the Gateway 2–to–Gateway 1 autopolicy, click **Edit**. The Edit VPN Policy screen displays.
3. In the General section of the screen, clear the **Enable NetBIOS** check box.
4. In the Traffic Selector section of the screen, make the following changes:
   - From the Local IP drop-down list, select **Single**.
   - In the Start IP fields, type **10.0.0.2**, which is the WAN IP address of Gateway 2.
5. Click **Apply** to save the settings.

➢ **To specify the syslog server that is connected to Gateway 1:**

1. Select **Monitoring > Firewall Logs & E-mail**. The Firewall Logs & E-mail screen displays.
2. Enable the syslog server and specify its IP address at Site 1. Enter **192.168.10.2** as the IP address.
3. Click **Apply** to save the settings.

Note: The VPN tunnel should be established automatically, and the syslogs should be sent to the syslog server at Site 1. You can use the IPSec VPN Connection Status screen to verify the connection.

View Status Screens

View the System Status

When you start up the VPN firewall, the default screen that displays is the Router Status screen.

The Router Status screen and Detailed Status screen provide real-time information about the following important components of the VPN firewall:

- Firmware version
- Both IPv4 and IPv6 WAN and LAN port information
- Interface statistics
- VLAN status, including port memberships

The Tunnel Status screen provides real-time information about the IPv6 tunnels.

These status screens are described in the following sections:

Router Status Screen

➢ **To view the Router Status screen:**

Select **Monitoring > Router Status**. The Router Status screen displays:

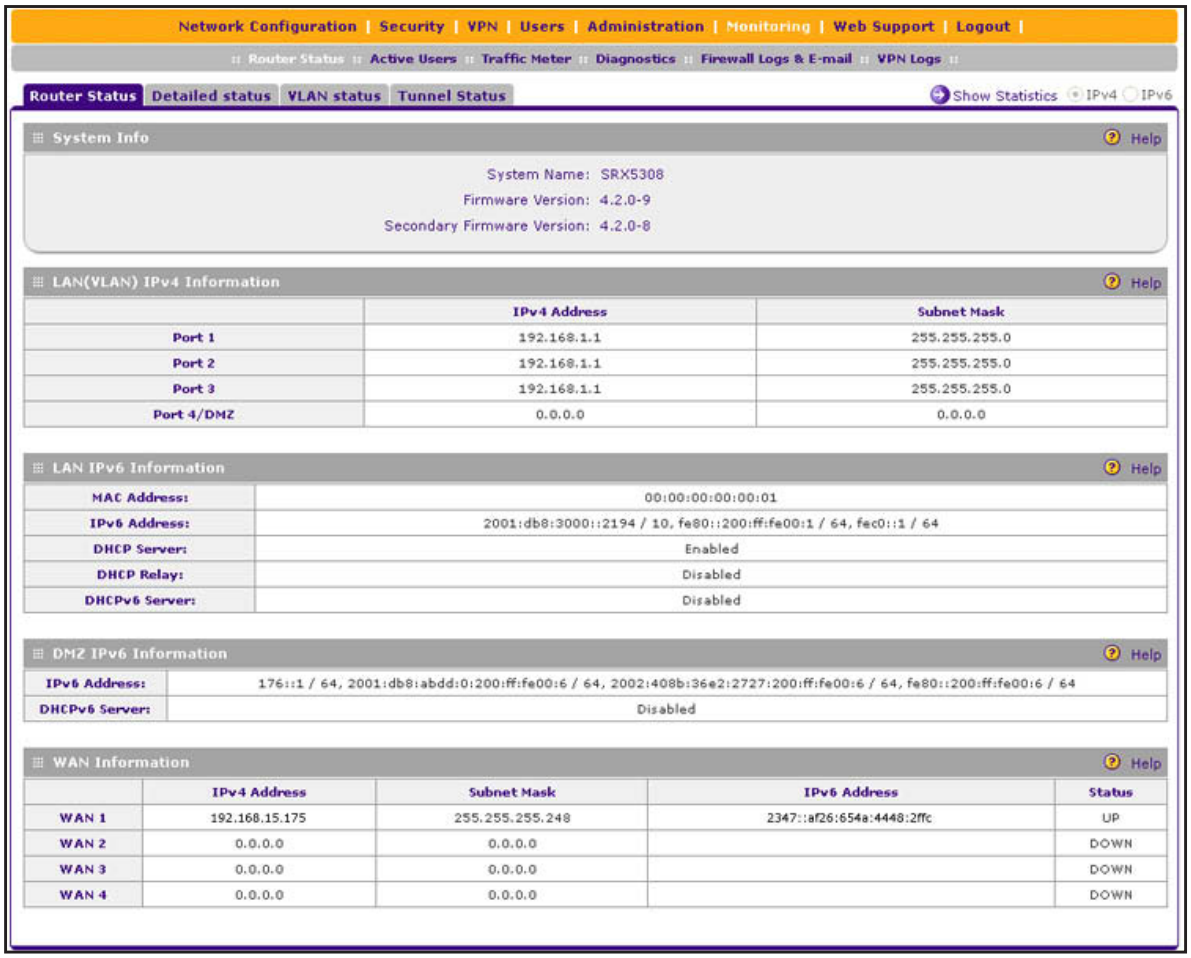

Figure 236.

The following table explains the fields of the Router Status screen:

Table 91. Router Status screen information

Item	Description
System Info	
System Name	The NETGEAR system name.
Firmware Version	The installed firmware version.
Secondary Firmware Version	The secondary software version. This version is for display only. (You cannot configure or select this version.)
LAN (VLAN) IPv4 Information	
For each of the four LAN ports, the screen shows the IPv4 LAN address and subnet mask. For more detailed information, see *Table 93* on page 374.	

Table 91. Router Status screen information (continued)

Item	Description
LAN IPv6 Information	
MAC Address	The MAC address of the VPN firewall.
IPv6 Address	The IPv6 LAN address that is assigned to the VPN firewall. For information about configuring the IPv6 address, see *Configure the IPv6 Internet Connection and WAN Settings* on page 52.
DHCP Server	The status of the IPv4 DHCP server (Enabled or Disabled). For information about configuring the IPv4 DHCP server, see *Configure a VLAN Profile* on page 88.
DHCP Relay	The status of the IPv4 DHCP relay (Enabled or Disabled). For information about configuring the IPv4 DHCP relay, see *Configure a VLAN Profile* on page 88.
DHCPv6 Server	The status of the DHCPv6 server for the LAN (Enabled or Disabled). For information about configuring the DHCPv6 server, see *Manage the IPv6 LAN* on page 102.
DMZ IPv6 Information	
IPv6 Address	The IPv6 DMZ address that is assigned to the VPN firewall. For information about configuring the IPv6 address, see *Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic* on page 114.
DHCPv6 Server	The status of the DHCPv6 server for the DMZ (Enabled or Disabled). For information about configuring the DHCPv6 server, see *Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic* on page 114.
WAN Information	
WAN 1	For each WAN interface, the screen shows the IPv4 address, subnet mask, IPv6 address, and status of the port (UP or Down). For more detailed information, see *Table 93* on page 374.
WAN 2	
WAN 3	
WAN 4	

Router Statistics Screen

➢ **To view the Router Statistics screen:**

1. Select **Monitoring > Router Status**. The Router Status screen displays (see the previous figure).
2. Click the **Show Statistics** option arrow in the upper right of the Router Status screen. The Router Statistics screen displays:

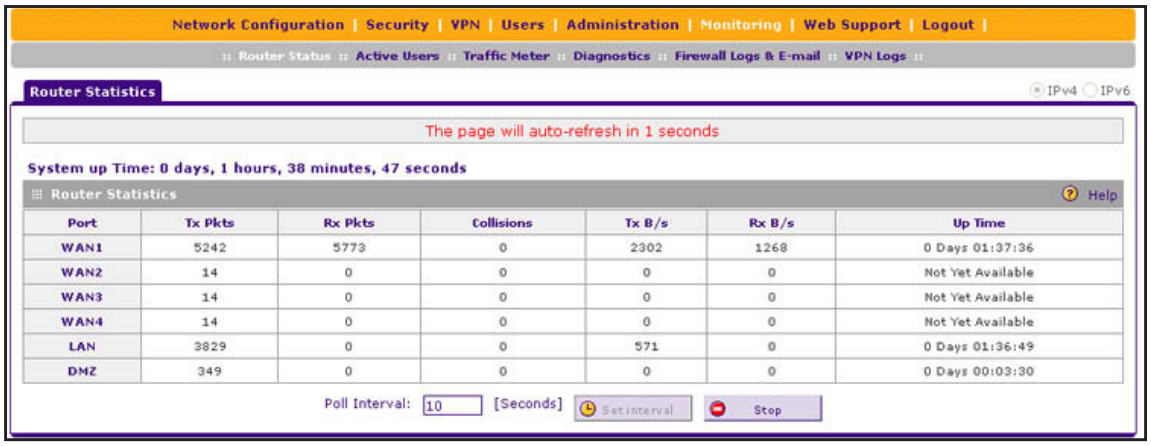

Figure 237.

The following table explains the fields of the Router Statistics screen.

To change the poll interval period, enter a new value (in seconds) in the Poll Interval field, and click **Set interval**. To stop polling, click **Stop**.

Table 92. Router Statistics screen information

Item	Description
System up Time. The period since the last time that the VPN firewall was started up.	
Router Statistics	
The following statistics are displayed for each of the four WAN interfaces, for all LAN interfaces combined, and for the DMZ interface:	
Tx Pkts	The number of packets transmitted on the port in bytes.
Rx Pxts	The number of packets received on the port in bytes.
Collisions	The number of signal collisions that have occurred on the port. A collision occurs when the port attempts to send data at the same time as a port on the other router or computer that is connected to this port.
Tx B/s	The number of bytes transmitted per second on the port.
Rx B/s	The number of bytes received per second on the port.
Up Time	The period that the port has been active since it was restarted.

Detailed Status Screen

To view the Detailed Status screen, select **Monitoring > Router Status > Detailed Status**. The Detailed Status screen displays:


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
Router Status | Active Users | Traffic Meter | Diagnostics | Firewall Logs & E-mail | VPN Logs
Router Status | Detailed status | VLAN status | Tunnel Status
IPv4 IPv6
LAN Port 1 Configuration Help
VLAN Profile: Default
VLAN ID: 1
MAC Address: 00:00:00:00:00:01
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled
LAN Port 2 Configuration Help
VLAN Profile: Default
VLAN ID: 1
MAC Address: 00:00:00:00:00:01
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled
LAN Port 3 Configuration Help
Not shown in this example
LAN Port 4 Configuration Help
Not shown in this example
LAN IPV6 Configuration Help
IPv6 Address: 2001:db8:3000::2194 / 10, fe80::200:ff:fe00:1 / 64, fec0::1 / 64
DHCP Status: Disabled
Primary DNS Server:
Secondary DNS Server:
DMZ IPV6 Configuration Help
IPv6 Address: 176::1 / 64, 2001:db8:abdd:0:200:ff:fe00:6 / 64, 2002:408b:36e2:2727:200:ff:fe00:6 / 64, fe80::200:ff:fe00:6 / 64
DHCP Status: Disabled
Primary DNS Server:
Secondary DNS Server:
WAN1 Info Help
WAN Mode: Single Port
Wan State: UP
NAT: Enabled
IPv4 Connection Type: Static IP
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Connected
IPv6 Connection State: Connected
WAN Connection Type: Other
Upload Connection Speed: 1000000 Kbps
Download Connection Speed: 1000000 Kbps
IP Address: 192.168.15.175
IPv6 Address: 2347::af26:654a:4448:2ffc /64
Subnet Mask: 255.255.255.248
Gateway: 192.168.15.180
Primary DNS: 10.221.23.5
Secondary DNS: 10.221.23.8
MAC Address: 00:00:00:00:11:22
Gateway (IPv6):
Primary DNS (IPv6):
Secondary DNS (IPv6):
WAN2 Info Help
WAN Mode: Single Port
Wan State: Down
NAT: Enabled
IPv4 Connection Type: Dynamic IP (DHCP)
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Not Yet Connected
IPv6 Connection State: Not Yet Connected
WAN Connection Type: Other
Upload Connection Speed: 1000000 Kbps
Download Connection Speed: 1000000 Kbps
IP Address: 0.0.0.0
IPv6 Address:
Subnet Mask: 0.0.0.0
Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
MAC Address:
Gateway (IPv6):
Primary DNS (IPv6):
Secondary DNS (IPv6):
WAN3 Info Help
Not shown in this example
WAN4 Info Help
Not shown in this example

Figure 238.

The following table explains the fields of the Detailed Status screen:

Table 93. Detailed Status screen information

Item	Description
LAN Port Configuration The following fields are shown for each of the LAN ports.	
VLAN Profile	The name of the VLAN profile that you assigned to the LAN port on the LAN Setup screen (see *Assign and Manage VLAN Profiles* on page 86). If the VLAN is not enabled on this port, the default profile (with VLAN ID 1) is assigned automatically.
VLAN ID	The VLAN ID that you assigned to the LAN port on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 88). If the default VLAN profile is used, the VLAN ID is 1, which means that all tagged and untagged traffic can pass on the LAN port.
MAC Address	The MAC address for this port. Note the following about the LAN MAC address: • All LAN ports that are part of the default VLAN share the same default MAC address (00:00:00:00:00:01), unless you have specified that each VLAN needs to be assigned a unique MAC address (see *Configure VLAN MAC Addresses and LAN Advanced Settings* on page 93). • LAN ports that have an IPv4 address that differs from the default VLAN can still share the same MAC address as the default VLAN. • LAN port 4 can be assigned as the DMZ port, in which case its default MAC address is 00:00:00:00:00:06. For information about configuring the DMZ port, see *Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic* on page 114.
IP Address	The IPv4 address for the LAN port. If the port is part of the default VLAN, the IP address is the default LAN IP address (192.168.1.1). For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 88.
Subnet Mask	The subnet mask for the LAN port. If the port is part of the default VLAN, the subnet mask is the default LAN IP subnet mask (255.255.255.0). For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 88.
DHCP Status	The status of the IPv4 DHCP server for the VLAN (Enabled or Disabled). For information about enabling DHCP for VLANs, see *Configure a VLAN Profile* on page 88.
LAN IPv6 Configuration	
IPv6 Address	The IPv6 address and prefix length for the LAN.
DHCP Status	The status of the DHCPv6 server for the LAN (Enabled or Disabled).
Primary DNS Server	The IPv6 address of the primary DNS server for the LAN.
Secondary DNS Server	The IP address of the secondary DNS server for the LAN.

For information about configuring the IPv6 LAN, see *DHCPv6 Server Options* on page 103 and *Configure the IPv6 LAN* on page 104.

Table 93. Detailed Status screen information (continued)

Item	Description	
DMZ IPv6 Configuration		
IPv6 Address	The IPv6 address and prefix length for the DMZ.	For information about configuring the IPv6 DMZ, see *DMZ Port for IPv6 Traffic* on page 118.
DHCP Status	The status of the DHCPv6 server for the DMZ (Enabled or Disabled).	
Primary DNS Server	The IPv6 address of the primary DNS server for the DMZ.	
Secondary DNS Server	The IP address of the secondary DNS server for the DMZ.	
WAN Configuration		
WAN Mode	The WAN mode can be Single Port, Load Balancing, or Auto Rollover. For information about configuring the WAN mode, see *Configure the IPv4 WAN Mode* on page 29.	
WAN State	The WAN state can be either UP or DOWN, depending on whether the port is connected to the Internet.	
NAT	The NAT state for IPv4 can be either Enabled or Disabled, depending on whether NAT is enabled (see *Network Address Translation* on page 29) or classical routing is enabled (see *Classical Routing* on page 30).	
IPv4 Connection Type	The connection type can be Static IP, DHCP, PPPoE, or PPTP, depending on whether the WAN address is obtained dynamically through a DHCP server or assigned statically by you. For information about connection types, see *Configure the IPv4 Internet Connection and WAN Settings* on page 29.	
IPv6 Connection Type	The connection type can be Static IPv6, PPPoE, or Dynamic IP (DHCPv6), depending on whether the WAN address is obtained dynamically through a DHCP server or ISP, or assigned statically by you. For information about connection types, see *Configure the IPv6 Internet Connection and WAN Settings* on page 52.	
IPv4 Connection State	The IPv4 connection state can be either Connected or Not Yet Connected, depending on whether the WAN interface is connected to the Internet over an IPv4 address. For information about configuring the IPv4 address of the WAN port, see *Configure the IPv4 Internet Connection and WAN Settings* on page 29.	
IPv6 Connection State	The IPv6 connection state can be either Connected or Not Yet Connected, depending on whether the WAN interface is connected to the Internet over an IPv6 address. For information about configuring the IPv6 address of the WAN port, see *Configure the IPv6 Internet Connection and WAN Settings* on page 52.	
WAN Connection Type	The detected type of Internet connection that is used on this port. The WAN connection type can be DSL, ADSL, T1, T3, or Other.	For information about configuring the WAN connection type, upload speed, and download speed, see *Configure Advanced WAN Options and Other Tasks* on page 71.
Upload Connection Speed	The maximum upload speed that is provided by your ISP.	
Download Connection Speed	The maximum download speed that is provided by your ISP.	

Table 93. Detailed Status screen information (continued)

Item	Description	
IP Address	The IPv4 address of the WAN port. For information about configuring the IPv4 address of the WAN port, see *Configure the IPv4 Internet Connection and WAN Settings* on page 29.	
IPv6 Address	The IPv6 address and prefix length of the WAN port. For information about configuring the IPv6 address and prefix length of the WAN port, see *Configure the IPv6 Internet Connection and WAN Settings* on page 52.	
Subnet Mask	The IPv4 subnet mask of the WAN port. For information about configuring the subnet mask of the WAN port, see *Configure the IPv4 Internet Connection and WAN Settings* on page 29.	
Gateway	The IPv4 address of the gateway.	These IPv4 settings are either obtained dynamically from your ISP or specified by you on the WAN IPv4 ISP Settings screen (see *Manually Configure an IPv4 Internet Connection* on page 34).
Primary DNS	The IPv4 address of the primary DNS server.	
Secondary DNS	The IPv4 address of the secondary DNS server.	
MAC Address	The default MAC address for the port or the MAC address that you have specified on the WAN Advanced Options screen for the port. For information about configuring the MAC address, see *Configure Advanced WAN Options and Other Tasks* on page 71.	
Gateway (IPv6)	The IPv6 address of the gateway.	These IPv6 settings are either obtained dynamically from your ISP or specified by you on the WAN IPv6 ISP Settings screen (see *Configure a Static IPv6 Internet Connection* on page 58 or *Configure a PPPoE IPv6 Internet Connection* on page 61).
Primary DNS (IPv6)	The IPv6 address of the primary DNS server.	
Secondary DNS (IPv6)	The IPv6 address of the secondary DNS server.	

VLAN Status Screen

The VLAN Status screen displays information about the VLANs that are enabled. Disabled VLANs are not displayed. For information about enabling and disabling VLANs, see *Assign and Manage VLAN Profiles* on page 86.

➢ **To view the status of the IPv4 VLANs:**

Select **Monitoring > Router Status > VLAN Status**. The VLAN Status screen displays:

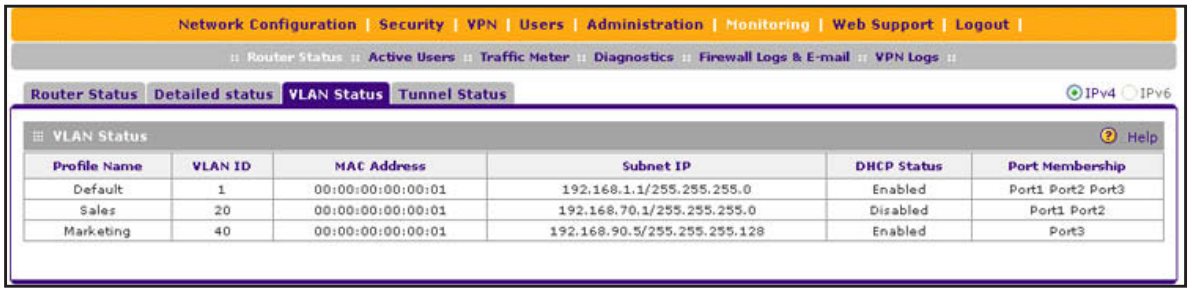

Figure 239.

The following table explains the fields of the VLAN Status screen:

Table 94. VLAN Status screen information

Item	Description	
Profile Name	The unique name for the VLAN that you have assigned on the Add VLAN Profile screen.	For information about configuring VLANs, see *Configure a VLAN Profile* on page 88.
VLAN ID	The identifier for the VLAN that you have assigned on the Add VLAN Profile screen.	
MAC Address	VLANs can have the same MAC address as the associated LAN port or can be assigned a unique MAC address, depending on the VLAN MAC settings that you have specified on the IPv4 LAN Advanced screen (see *Configure VLAN MAC Addresses and LAN Advanced Settings* on page 93).	
Subnet IP	The IP address and subnet mask that you have assigned on the Add VLAN Profile screen.	
DHCP Status	The DHCP status for the VLAN, which can be either DHCP Enabled or DHCP Disabled, depending on the DHCP configuration that you have specified on the Add VLAN Profile screen.	
Port Membership	The ports that you have associated with the VLAN on the Add VLAN Profile screen.	

Tunnel Status Screen

The IPv6 Tunnel Status screen displays the status of all active 6to4 and ISATAP tunnels and their IPv6 addresses.

➢ **To view the status of the tunnels and IPv6 addresses:**

Select **Monitoring > Router Status > Tunnel Status**. The Tunnel Status screen displays:

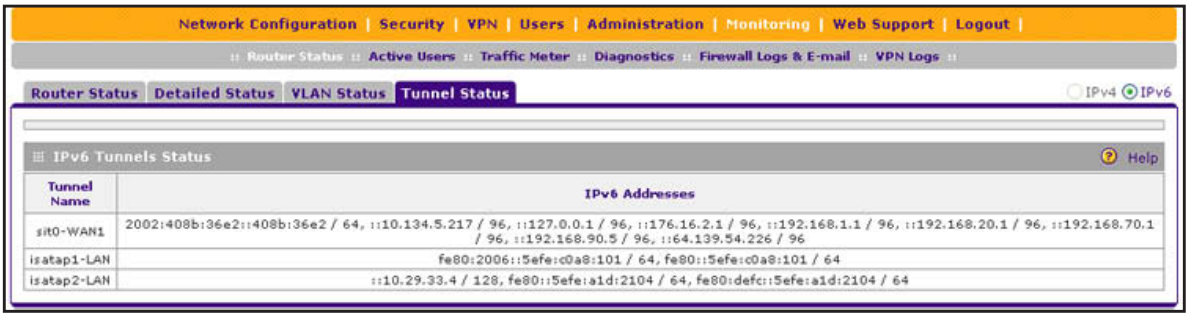

Figure 240.

The IPv6 Tunnel Status table shows the following fields:

- **Tunnel Name**. The tunnel name for the 6to4 tunnel is always sit0-WAN1 (SIT stands for simple Internet transition); the tunnel name for an ISATAP tunnel is isatapx-LAN, in which x is an integer.
- **IPv6 Address**. The IPv6 address of the local tunnel endpoint.

View the VPN Connection Status, L2TP Users, and PPTP Users

The Connection Status screens display a list of IPSec VPN connections, SSL VPN connections, and L2TP users who are logged in to the VPN firewall.

- **To view the active IPSec VPN connections:**

Select **VPN > Connection Status**. The Connection Status submenu tabs display with the IPSec VPN Connection Status screen in view:

Figure 241.

The policy name, the endpoint's IP address, the amount of data and number of packets transmitted, and the state of the connection are listed in the table.

To activate a tunnel, click the **Connect** table button to the right of the policy's table entry; to disconnect an active connection, click the **Disconnect** table button to the right of the policy's table entry.

The default poll interval is 10 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and click the **Set Interval** button. To stop polling, click the **Stop** button.

- **To view the active SSL VPN connections:**

Select **VPN > Connection Status > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:

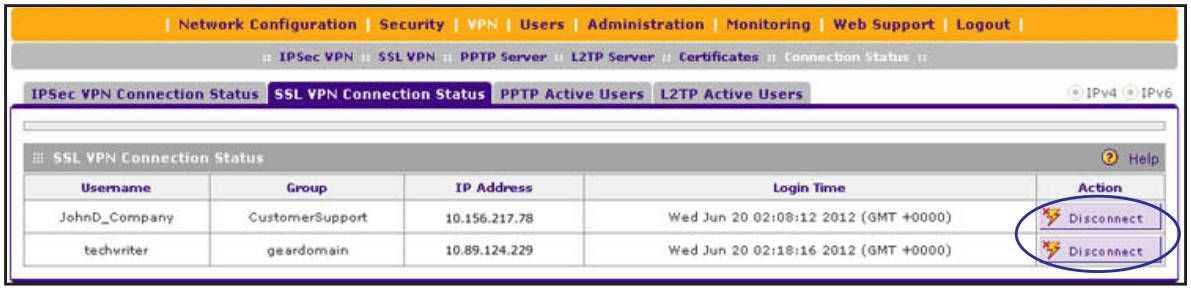

Figure 242.

The active user's user name, group, and IP address are listed in the table with a time stamp indicating the time and date that the user connected.

To disconnect an active connection, click the **Disconnect** table button to the right of the policy's table entry.

- **To view the active L2TP tunnel users:**

Select **VPN > Connection Status > L2TP Active Users**. The L2TP Active Users screen displays. (The following figure does not show any active users.)

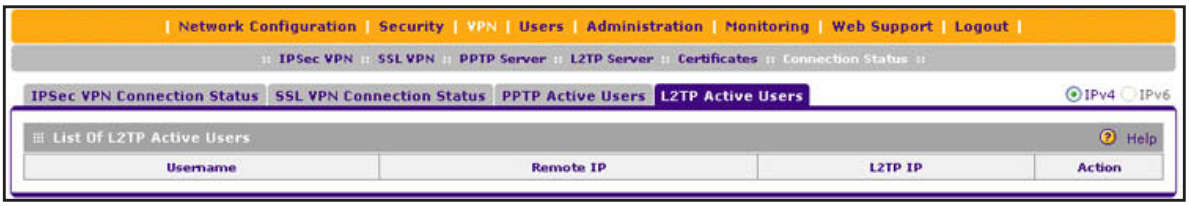

Figure 243.

The List of L2TP Active Users table lists each active connection with the information that is described in the following table.

Table 95. L2TP Active Users screen information

Item	Description
Username	The name of the L2TP user that you have defined (see *Configure User Accounts* on page 310).
Remote IP	The client's IP address on the remote LAC.
L2TP IP	The IP address that is assigned by the L2TP server on the VPN firewall.
Action	Click the **Disconnect** table button to terminate the L2TP connection.

- **To view the active PPTP tunnel users:**

Select **Monitoring > Active Users & VPNs > PPTP Active Users**. The PPTP Active Users screen displays. (The following figure does not show any active users.)

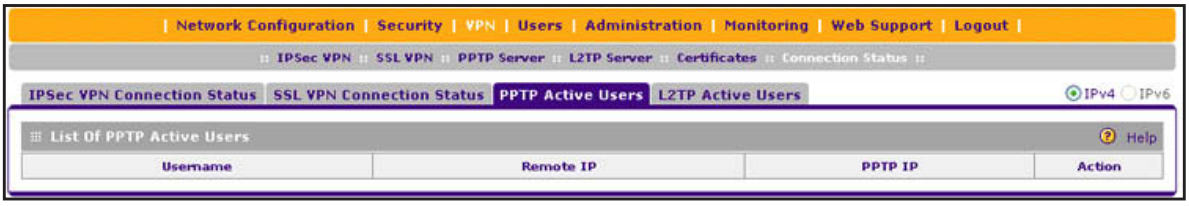

Figure 244.

The List of PPTP Active Users table lists each active connection with the information that is described in the following table.

Table 96. PPTP Active Users screen information

Item	Description
Username	The name of the PPTP user that you have defined (see *Configure User Accounts* on page 310).
Remote IP	The remote client's IP address.
PPTP IP	The IP address that is assigned by the PPTP server on the VPN firewall.
Action	Click the **Disconnect** table button to terminate the connection. (This button is displayed only when there an active connection.)

View the VPN Logs

➢ **To display the IPSec VPN log:**

Select **Monitoring > VPN Logs**. The Logs tabs display with the IPSec VPN Logs screen in view.

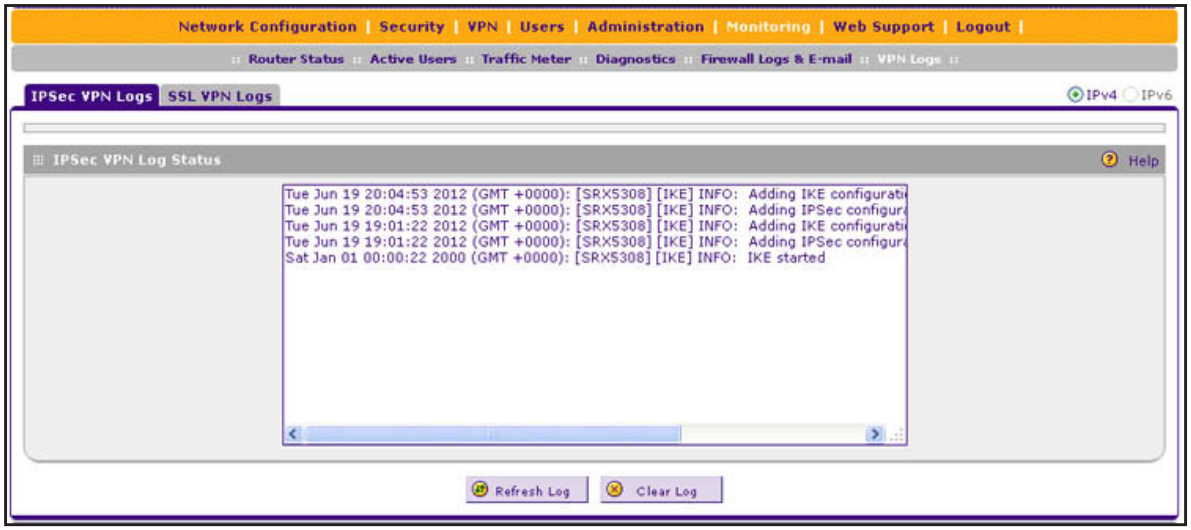

Figure 245.

➢ **To display the SSL VPN log:**

Select **Monitoring > VPN Logs > SSL VPN Logs**. The SSL VPN Logs screen displays:

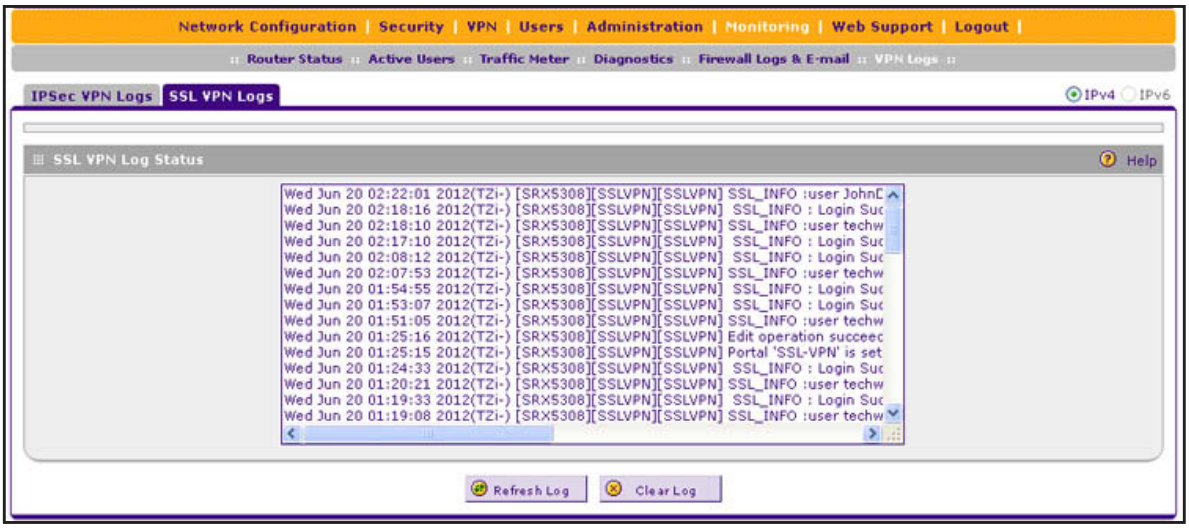

Figure 246.

View the Port Triggering Status

➢ **To view the status of the port triggering feature:**

1. Select **Security > Port Triggering**. The Port Triggering screen displays. (The following figure shows one rule in the Port Triggering Rules table as an example.)

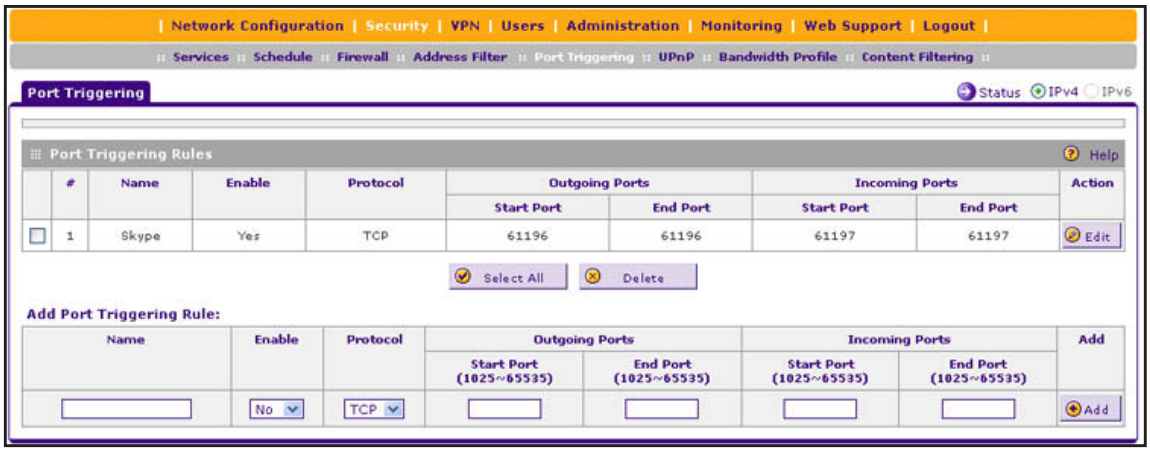

Figure 247.

2. Click the **Status** option arrow in the upper right of the Port Triggering screen. The Port Triggering Status pop-up screen displays.

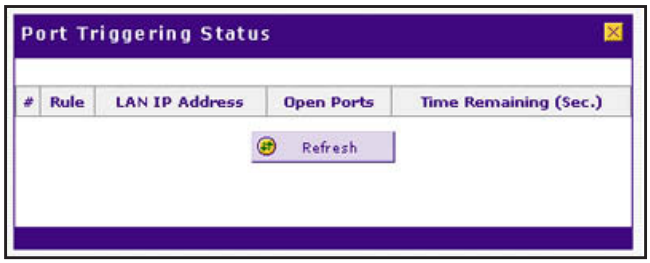

Figure 248.

The Port Triggering Status screen displays the information that is described in the following table:

Table 97. Port Triggering Status screen information

Item	Description
#	The sequence number of the rule onscreen.
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 using this rule.
Open Ports	The incoming ports that are associated with this rule. Incoming traffic using one of these ports is sent to the IP address that is listed in the LAN IP Address field.
Time Remaining	The time remaining before this rule is released and made available for other computers or devices. This timer is restarted when incoming or outgoing traffic is received.

View the WAN Port Status

You can view the status of the IPv4 and IPv6 WAN connections, the DNS servers, and the DHCP servers.

IPv4 WAN Port Status

➢ **To view the IPv4 status of a WAN port:**

1. Select **Network Configuration > WAN Settings > WAN Setup**. The WAN Setup screen displays the IPv4 settings:

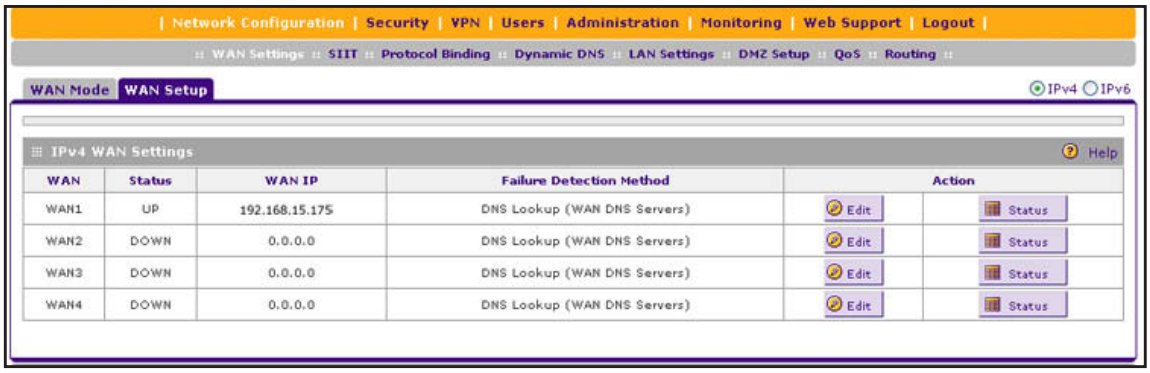

Figure 249.

2. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen. (The following figure shows a static IP address configuration.)

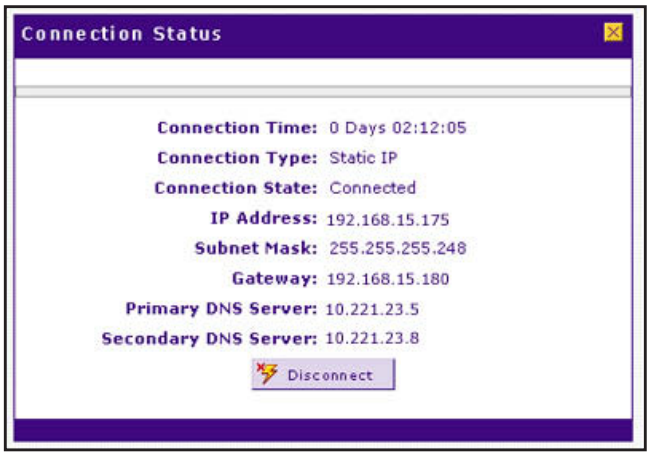

Figure 250.

The type of connection determines the information that is displayed on the Connection Status screen. The screen can display the information that is described in the following table:

Table 98. Connection Status screen information for an IPv4 connection

Item	Description
Connection Time	The period that the VPN firewall has been connected through the WAN port.
Connection Type	The connection type can be either DHCP or Static IP.
Connection Status	The connection status can be either Connected or Disconnected.
IP Address	The addresses that were automatically detected or that you configured on the WAN IPv4 ISP Settings screen. **Note:** For more information, see *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 31 and *Manually Configure an IPv4 Internet Connection* on page 34.
Subnet Mask	
Gateway	
DNS Server	

Table 98. Connection Status screen information for an IPv4 connection (continued)

Item	Description
DHCP Server	DHCP only. The DHCP server that was automatically detected. This field displays only if your ISP does not require a login and the IP address is acquired dynamically from your ISP. You have configured these ISP settings on the WAN IPv4 ISP Settings screen. **Note:** For more information, see *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 31 and *Manually Configure an IPv4 Internet Connection* on page 34.
Lease Obtained	DHCP only. The time when the DHCP lease was obtained.
Lease Duration	DHCP only. The period that the DHCP lease remains in effect.

Click **Disconnect** to disconnect the connection; click **Connect** to establish the connection.

IPv6 WAN Port Status

➢ **To view the IPv6 status of the WAN port:**

1. Select **Network Configuration > WAN Settings > WAN Setup**.
2. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings:

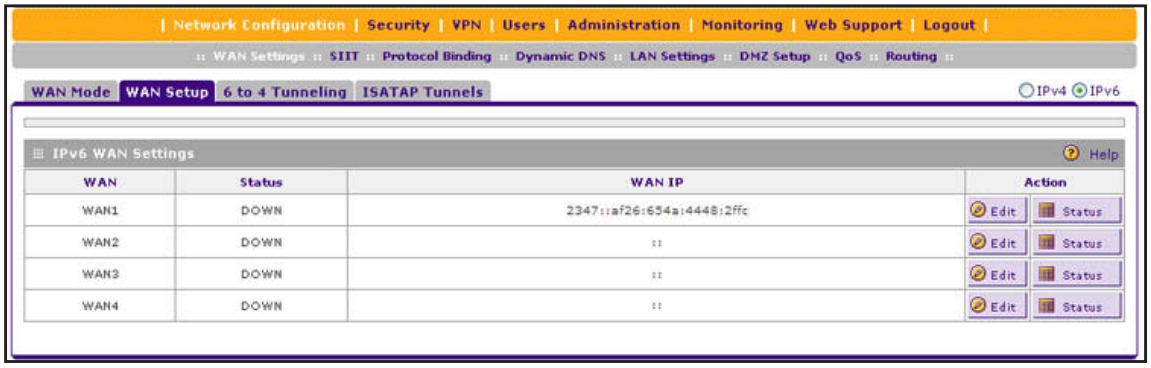

Figure 251.

3. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen. (The following figure shows a dynamic IP address configuration.)

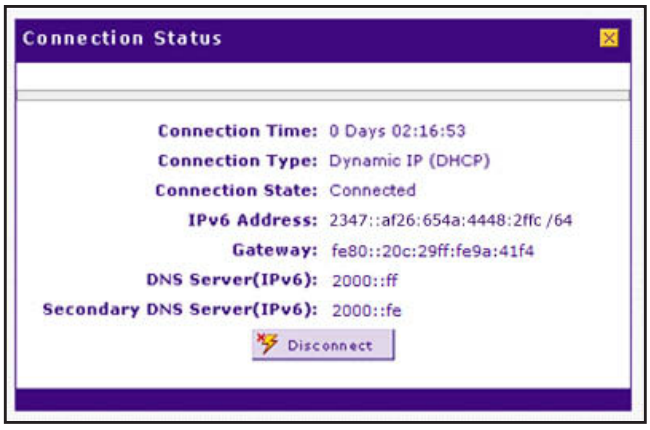

Figure 252.

The type of connection determines the information that is displayed on the Connection Status screen. The screen can display the information that is described in the following table:

Table 99. Connection Status screen information for an IPv6 connection

Item	Description
Connection Time	The period that the VPN firewall has been connected through the WAN port.
IPv6 Connection Type	The connection type can be either Dynamic IP (DHCP), Static, or PPPoE.
IPv6 Connection Status	The connection status can be either Connected or Disconnected.
IPv6 Address	The IPv6 addresses that were automatically detected or that you configured on the WAN IPv6 ISP Settings screen. **Note:** The Gateway and DNS Server (IPv6) fields apply only to static IPv6 and PPPoE IPv6 connections. **Note:** For more information, see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 55 and *Configure a Static IPv6 Internet Connection* on page 58.
Gateway	
Primary DNS Server (IPv6)	
Secondary DNS Server (IPv6)	

Click **Disconnect** to disconnect the connection; click **Connect** to establish the connection.

View the Attached Devices and the DHCP Log

The LAN Groups screen shows the network database, which is the Known PCs and Devices table, which contains all IP devices that VPN firewall has discovered on the local network. The LAN Setup screen lets you access the DHCP log.

View the Attached Devices

➢ **To view the attached devices on the LAN Groups screen:**

Select **Network Configuration > LAN Settings > LAN Groups**. The LAN Groups screen displays. (The following figure shows some examples in the Known PCs and Devices table.)

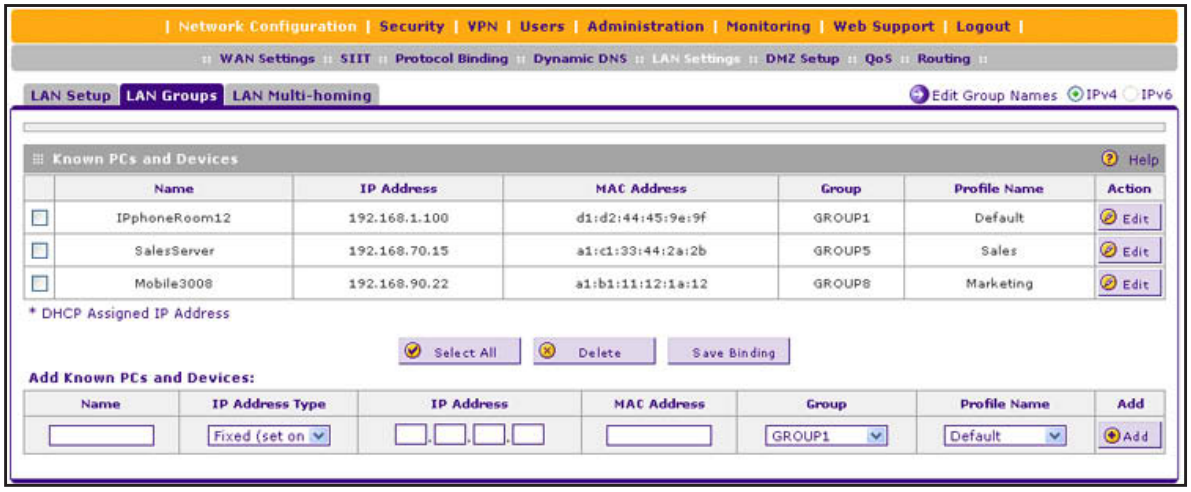

Figure 253.

The Known PCs and Devices table contains a list of all known computers and network devices that are assigned dynamic IP addresses by the VPN firewall, have been discovered by other means, or were manually added. Collectively, these entries make up the network database. For information about how to edit the Known PCs and Devices table or manually add entries to the table, see *Manage the Network Database* on page 97.

For each attached computer or device, the Known PCs and Devices table displays the following fields:

- **Check box**. Allows you to select the computer or device in the table.
- **Name**. The name of the computer 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 computer or device was assigned an IP address by the DHCP server, the name is appended by an asterisk.
- **IP Address**. The current IP address of the computer or device. For DHCP clients of the VPN firewall, this IP address does not change. If a computer or device is assigned a static IP address, you need to update this entry manually after the IP address on the computer or device has changed.
- **MAC Address**. The MAC address of the computer's or device's network interface.
- **Group**. Each computer or device can be assigned to a single LAN group. By default, a computer or device is assigned to Group 1. You can select a different LAN group from the Group drop-down list in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen.
- **Action**. The Edit table button, which provides access to the Edit Groups and Hosts screen.

Note: If the VPN firewall is rebooted, the data in the Known PCs and Devices table is lost until the VPN firewall rediscovers the devices.

View the DHCP Log

➢ **To review the most recent entries in the DHCP log:**

1. Select **Network Configuration > LAN Settings**. The LAN Setup screen displays the IPv4 settings. (see *Figure 51* on page 88).
2. Click the **DHCP Log** option arrow to the right of the LAN Setup tab. The DHCP Log screen displays:

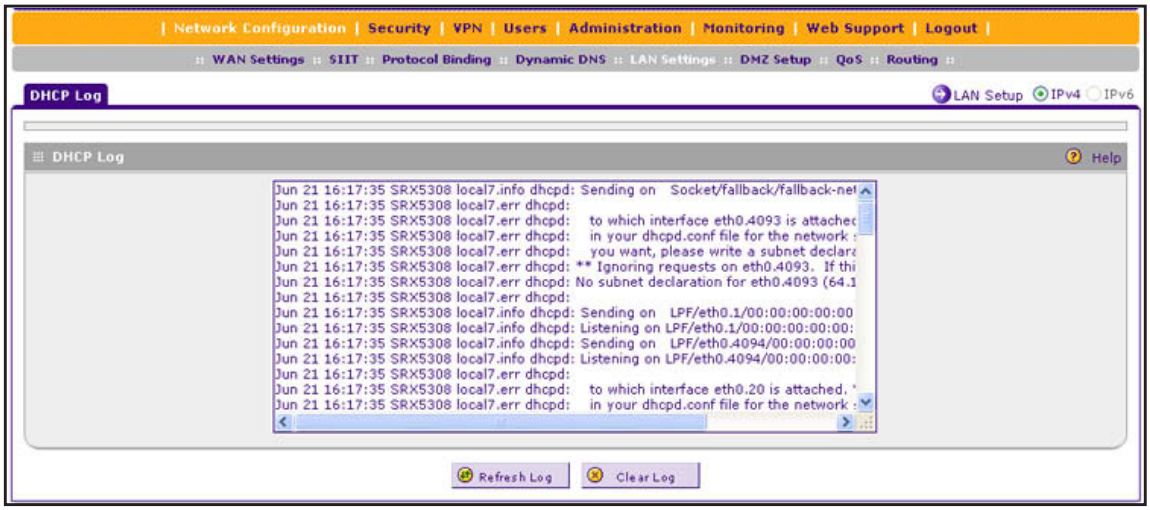

Figure 254.

To view the most recent entries, click **Refresh Log**. To delete all the existing log entries, click **Clear Log**. Click the **LAN Setup** option arrow in the upper right to display the LAN Setup screen for IPv4, from which you can modify the DHCP settings (see *Configure a VLAN Profile* on page 88).

Diagnostics Utilities

The VPN firewall provides diagnostic tools that help you analyze the status of the network and traffic conditions. Two types 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 tables.
- **Packet capture tool**. This tool lets you capture packets per interface in real time for a short period, and download the packet information.

Note: For normal operation, diagnostic tools are not required.

➢ **To display the Diagnostics screen:**

1. Select **Monitoring > Diagnostics**. The Diagnostics screen displays the IPv4 settings (see the next figure).
2. Specify the IP version for which you want to display the Diagnostics screen:
   - **IPv4**. In the upper right of the screen, the IPv4 radio button is already selected by default.

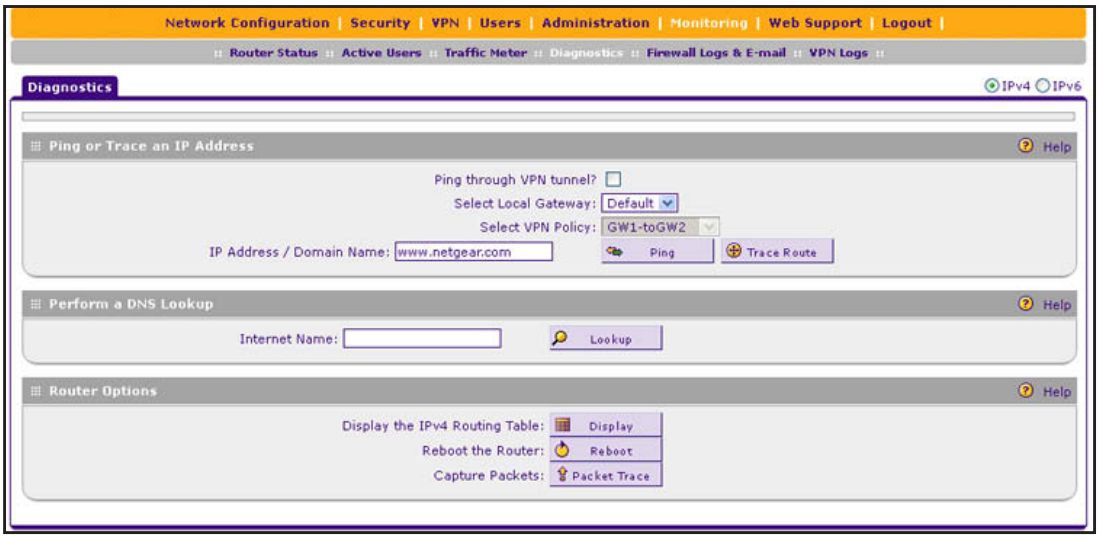

Figure 255.

- **IPv6**. Select the **IPv6** radio button. The Diagnostics screen displays the IPv6 settings:

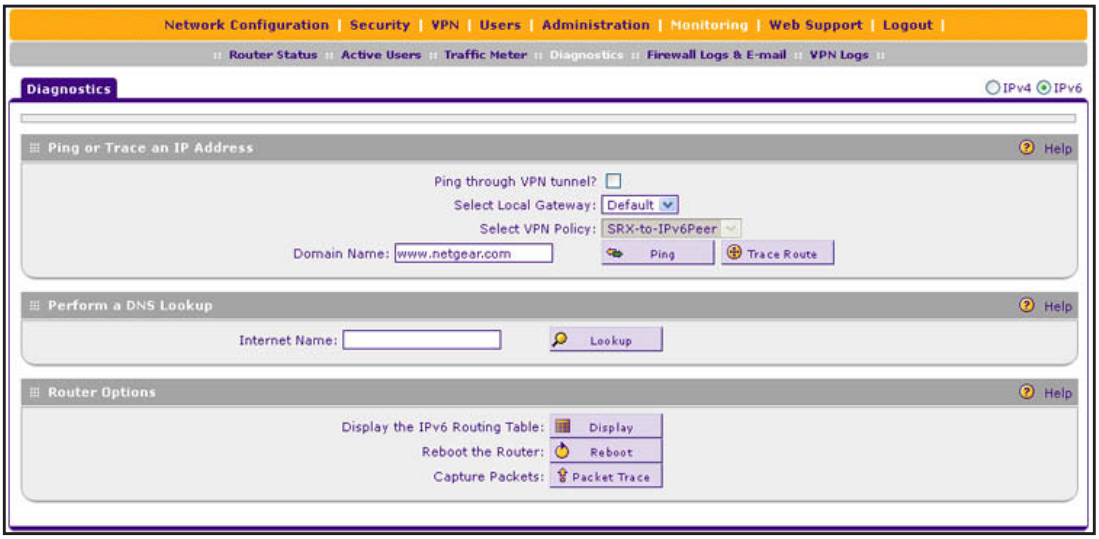

Figure 256.

The various tasks that you can perform on the Diagnostics screen are described in the following sections.

Send a Ping Packet

Use the ping utility to send a ping packet request in order to check the connection between the VPN firewall and a specific IP address or FQDN. 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.

➢ **To send a ping:**

1. On the Diagnostics screen for IPv4, in the IP Address / Domain Name field of the Ping or Trace an IP Address section, enter the IP address or domain name that you want to ping; on the Diagnostics screen for IPv6, in the Domain Name field, enter the domain name that you want to ping (you cannot enter an IP address).
2. Do one of the following:
   - Make sure that the **Ping through VPN tunnel?** check box is cleared, and select a gateway from the Select Local Gateway drop-down list. (The Select VPN Policy drop-down list is masked out.)
   - Select the **Ping through VPN tunnel?** check box, and select a VPN policy from the Select VPN Policy drop-down list. (The Select Local Gateway drop-down list is masked out.)
3. Click the **Ping** button. The results of the ping are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Trace a Route

A traceroute lists all routers between the source (the VPN firewall) and the destination IP address.

➢ **To send a traceroute:**

1. On the Diagnostics screen for IPv4, in the IP Address / Domain Name field of the Ping or Trace an IP Address section, enter the IP address or domain name that you want to trace; on the Diagnostics screen for IPv6, in the Domain Name field, enter the domain name that you want to trace (you cannot enter an IP address).
2. Do one of the following:
   - Make sure that the **Ping through VPN tunnel?** check box is cleared, and select a gateway from the Select Local Gateway drop-down list. (The Select VPN Policy drop-down list is masked out.)
   - Select the **Ping through VPN tunnel?** check box, and select a VPN policy from the Select VPN Policy drop-down list. (The Select Local Gateway drop-down list is masked out.)
3. Click the **Traceroute** button. The results of the traceroute are displayed in a new screen.
4. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Look Up a DNS Address

A Domain Name Server (DNS) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a web, FTP, mail, or other server on the Internet, request a DNS lookup to find the IP address.

➢ **To look up a DNS address:**

1. In the Perform a DNS Lookup section of the screen, in the Internet Name field, enter a domain name.
2. Click the **Lookup** button. The results of the lookup action are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Display the Routing Tables

Displaying the internal routing table can assist NETGEAR technical support in diagnosing routing problems.

➢ **To display the routing table:**

On the Diagnostics screen for IPv4, in the Router Options section of the screen, click the **Display** button next to Display the IPv4 Routing Table. The routing table is shown in the Route Display pop-up screen.

On the Diagnostics screen for IPv6, in the Router Options section of the screen, click the **Display** button next to Display the IPv6 Routing Table. The routing table is shown in the Route Display pop-up screen.

Capture Packets in Real Time

Capturing packets can assist NETGEAR technical support in diagnosing packet transfer problems. You can also use a traffic analyzer to do your own problem diagnoses.

➢ **To capture packets in real time:**

1. In Router Options section of the screen, next to Capture Packets, click the **Packet Trace** button. The Capture Packets pop-up screen displays:

Figure 257.

2. From the Select Network drop-down list, select the physical or virtual interface for which you want to capture packets.
3. Click **Start**. After a few seconds, the packet-tracing process starts, which is indicated by a message onscreen.
4. When you want to stop the packet-tracing process, click **Stop**. After a few seconds, the packet-tracing process stops, which is indicated by a message onscreen.
5. Click **Download**. Select a location to save the captured packets. (The default file name is pkt.cap.) The file is downloaded to the location that you specify.
6. When the download is complete, browse to the download location you specified, and verify that the file was downloaded successfully.
7. Optional step: Send the file to NETGEAR technical support for analysis.

Reboot the VPN Firewall Remotely

You can perform a remote reboot, for example, when the VPN firewall seems to have become unstable or is not operating normally.

Rebooting breaks any existing connections either to the VPN firewall (such as your management session) or through the VPN firewall (for example, LAN users accessing the Internet). However, connections to the Internet are automatically reestablished when possible.

➢ **To reboot the VPN firewall:**

In Router Options section of the screen, next to Reboot the Router, click the **Reboot** button. The VPN firewall reboots. The Diagnostics screen might remain visible during the reboot process, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds.

10 Troubleshooting

This chapter provides troubleshooting tips and information for the VPN firewall. 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 VPN firewall on?

  Go to *Basic Functioning* on page 393.
- Have I connected the VPN firewall correctly?

  Go to *Basic Functioning* on page 393.
- I cannot access the VPN firewall's web management interface.

  Go to *Troubleshoot the Web Management Interface* on page 394.
- A time-out occurs.

  Go to *When You Enter a URL or IP Address, a Time-Out Error Occurs* on page 395.
- I cannot access the Internet or the LAN.

  Go to *Troubleshoot the ISP Connection* on page 396.
- I have problems with the IPv6 connection.

  Go to *Troubleshooting the IPv6 Connection* on page 397
- I have problems with the LAN connection.

  Go to *Troubleshoot a TCP/IP Network Using a Ping Utility* on page 400.
- I want to clear the configuration and start over again.

  Go to *Restore the Default Configuration and Password* on page 401.
- The date or time is not correct.

  Go to *Address Problems with Date and Time* on page 403.
- I need more information.

  Go to *Access the Knowledge Base and Documentation* on page 403.

Note: The VPN firewall's diagnostic tools are described in *Diagnostics Utilities* on page 388.

Basic Functioning

- *Power LED Not On*
- *Test LED Never Turns Off*
- *LAN or WAN Port LEDs Not On*

➢ **After you turn on power to the VPN firewall, verify that the following sequence of events occurs:**

1. When power is first applied, verify that the Power LED is on.
2. After approximately 2 minutes, verify that:
   a. The Test LED is no longer lit.
   b. The left LAN port LEDs are lit for any local ports that are connected.
   c. The left WAN port LEDs are lit for any WAN ports that are connected.

   If a port's left LED is lit, a link has been established to the connected device. If a port is connected to a 1000 Mbps device, verify that the port's right LED is green. If the port functions at 100 Mbps, the right LED is amber. If the port functions at 10 Mbps, the right LED is off.

If any of these conditions do not occur, see the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your VPN firewall is turned on, make sure that the power cord is correctly connected to your VPN firewall and that the power supply adapter is correctly connected to a functioning power outlet.

If the error persists, you have a hardware problem and should contact NETGEAR technical support.

Test LED Never Turns Off

When the VPN firewall is powered on, the Test LED turns on for approximately 2 minutes and then turns off when the VPN firewall has completed its initialization. If the Test LED remains on, there is a fault within the VPN firewall.

- **If all LEDs are still on more than several minutes minute after power-up, do the following:**
  - Turn off the power, and turn it on again to see if the VPN firewall recovers.
  - Reset the VPN firewall's configuration to factory default settings. Doing so sets the VPN firewall's IP address to **192.168.1.1**. This procedure is described in *Restore the Default Configuration and Password* on page 401.

  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 VPN firewall and at the hub, router, or workstation.
  - Make sure that power is turned on to the connected hub, router, or workstation.
  - Be sure that you are using the correct cables:

    When connecting the VPN firewall's WAN ports to one or two devices that provide the Internet connections, use the cables that are supplied with the devices. These cables could be standard straight-through Ethernet cables or Ethernet crossover cables.

Troubleshoot the Web Management Interface

- **If you cannot access the VPN firewall's web management interface from a computer on your local network, check the following:**
  - Check the Ethernet connection between the computer and the VPN firewall as described in the previous section (*LAN or WAN Port LEDs Not On*).
  - If your computer's IP address is shown as 169.254.x.x:
    Windows and Mac operating systems generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the VPN firewall and reboot your computer.
  - If your VPN firewall's IP address has been changed and you do not know the current IP address, reset the VPN firewall's configuration to factory default settings. This sets the VPN firewall's IP address to **192.168.1.1**. This procedure is described in *Restore the Default Configuration and Password* on page 401.

    Tip: If you do not want to revert to the factory default settings and lose your configuration settings, you can reboot the VPN firewall and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the VPN firewall'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.
- Clear the browser's cache.
- 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.

Note: To be able to configure the VPN firewall, your computer's IP address does not need to be on the same subnet as the VPN firewall.

If the VPN firewall does not save changes you made in the web management interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

When You Enter a URL or IP Address, a Time-Out Error Occurs

➢ **A number of things could be causing this situation. Try the following troubleshooting steps:**

- Check whether other computers on the LAN work correctly. If they do, ensure that your computer's TCP/IP settings are correct. If you use a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses on a WAN IPv4 ISP Settings screen. For more information, see *Manually Configure an IPv4 Internet Connection* on page 34.
- If the computer is configured correctly, but still not working, ensure that the VPN firewall is connected and turned on. Connect to the web management interface, and check the VPN firewall's settings. If you cannot connect to the VPN firewall, see the information in the previous section (*Troubleshoot the Web Management Interface* on page 394).
- If the VPN firewall is configured correctly, check your Internet connection (for example, your modem, dish, or router) to make sure that it is working correctly.

Troubleshoot the ISP Connection

If your VPN firewall is unable to access the Internet, you should first determine whether the VPN firewall is able to obtain a WAN IP address from the ISP. Unless you were assigned a static IP address, your VPN firewall 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 VPN firewall's configuration at https://192.168.1.1.
3. Select **Network Configuration > WAN Settings > WAN Setup**. The WAN Setup screen for IPv4 displays.
4. Take one of the following actions:
   - **For IPv4**. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen (see *Figure 13* on page 34).
   - **For IPv6**. In the upper right of the screen, select the **IPv6** radio button. The WAN Setup screen displays the IPv6 settings. In the Action column, click the **Status** button of the WAN interface for which you want to display the Connection Status pop-up screen (see *Figure 31* on page 57).
5. Check that an IP address is shown for the WAN port. If an IP address with zeros only is shown, or if no IP address is shown, the VPN firewall has not obtained an IP address from your ISP, or for IPv6, has not obtained or generated an IP address.

➢ **If your VPN firewall is unable to obtain an IP address from the ISP, you might need to force your modem, dish, or router to recognize your new VPN firewall by performing the following procedure:**

1. Turn off the power to the modem, dish, or router.
2. Turn off the power to your VPN firewall.
3. Wait 5 minutes, and turn on the power to the modem, dish, or router.
4. When the LEDs of the modem, dish, or router indicate that synchronization with the ISP has occurred, turn on the power to your VPN firewall.

If your VPN firewall 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.
  For IPv4 connections, ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- For IPv4 connections, if your ISP requires a login, you might have incorrectly set the login name and password.
- For IPv4 connections, your ISP might check for your computer's host name. On a WAN IPv4 ISP Settings screen, in the Account Name field, enter the host name, system name, or account name that was assigned to you by your ISP. You might also need to enter the assigned domain name or workgroup name in the Domain Name field, and you might

have to enter additional information. For more information, see *Manually Configure an IPv4 Internet Connection* on page 34.

- Your ISP allows only one Ethernet MAC address to connect to the Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have a new network device, and ask them to use the VPN firewall's MAC address.
  - Configure your VPN firewall to spoof your computer's MAC address. You can do this in the Router's MAC Address section on a WAN Advanced Options screen. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 71.

If your VPN firewall can obtain an IP address, but an attached computer is unable to load any web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. You can configure your computer manually with DNS addresses, as described in your operating system documentation.

- Your computer might not have the VPN firewall configured as its TCP/IP gateway.

Troubleshooting the IPv6 Connection

If you have difficulty connecting over an IPv6 connection, there might be an incorrect configuration on the VPN firewall or the computer from which you are trying to connect to the VPN firewall:

Check the VPN firewall:

- By default, the VPN firewall is set to IPv4-only mode. Make sure that the VPN firewall is set to IPv4/IPv6 mode (see *Configure the IPv6 Routing Mode* on page 53).
- Make sure that the ISP settings are correct (see *Configure a Static IPv6 Internet Connection* on page 58). The VPN firewall cannot receive a valid IPv6 address if the Internet connection is not correctly configured.
- Make sure that the VPN firewall can provide IPv6 addresses to the computers on the LAN (see *Manage the IPv6 LAN* on page 102). Check the settings on the LAN Setup screen for IPv6, and if applicable for your type of configuration, on the RADVD screen.

Check the computer:

- Make sure that the operating system supports IPv6. Normally, the following operating systems support IPv6:
  - Windows 7, all 32- and 64-bit versions
  - Windows Vista, all 32- and 64-bit versions
  - Windows XP Professional SP3 (32- and 64-bit)
  - Windows Server 2008, all versions
  - Windows Server 2008 R2, all versions

- Windows Server 2003, all versions
- Windows Server 2003 R2, all versions
- Linux and other UNIX-based systems with a correctly configured kernel
- MAC OS X

- Make sure that IPv6 is enabled on the computer. On a computer that runs a Windows-based operating system, do the following (note that the steps might differ on the various Windows operating systems):

  a. Open the Network Connections screen or the Network and Sharing Center screen. For example, on the Windows taskbar, click **Start**, select **Control Panel**, and select **Network Connections**.

  b. Click or double-click **Local Area Connection** for the connection to the VPN firewall. The Local Area Connection Properties screen displays:

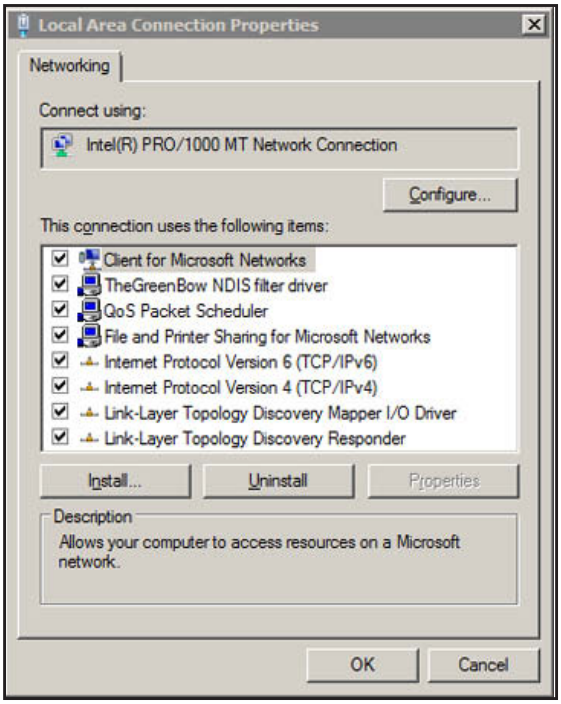

Figure 258.

  c. Make sure that Internet Protocol Version 6 (TCP/IPv6) displays, as is shown in the previous figure.

- Make sure that the computer has an IPv6 address. If the computer has a link-local address only, it cannot reach the VPN firewall or the Internet. On a computer that runs a Windows-based operating system, do the following (note that the steps might differ on the various Windows operating systems):

  a. Open the Network Connections screen or the Network and Sharing Center screen. For example, on the Windows taskbar, click **Start**, select **Control Panel**, and select **Network Connections**.

  b. Click or double-click **Local Area Connection** for the connection to the VPN firewall.

c. Click or double-click **View status of this connection**. The Local Area Connection Status screen displays:

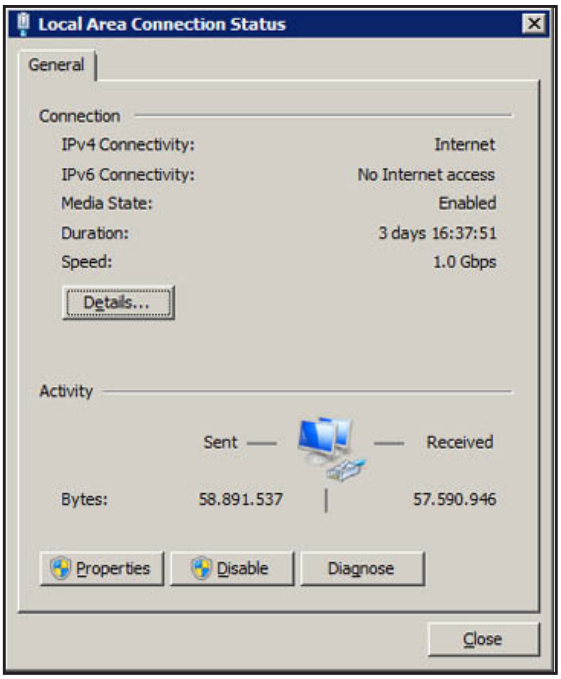

Figure 259.

d. Make sure that Internet access shows for the IPv6 connection. (The previous figure shows that there is no Internet access.)

e. Click **Details**. The Network Connection Details screen displays:

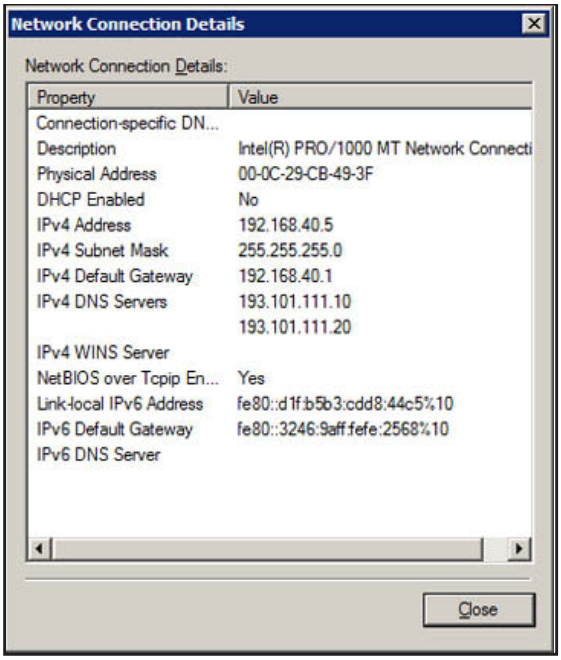

Figure 260.

f. Make sure that an IPv6 address shows. The previous figure does not show an IPv6 address for the computer but only a link-local IPv6 address and an IPv6 default gateway address, both of which start, in this case, with FE80.

Troubleshoot a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer or workstation.

Test the LAN Path to Your VPN Firewall

You can ping the VPN firewall from your computer to verify that the LAN path to the VPN firewall is set up correctly.

➢ **To ping the VPN firewall from a computer running Windows 95 or later:**

1. From the Windows taskbar, click **Start** and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the VPN firewall, 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 see this message:

   ```
   Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you might 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 394.
     - 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 VPN firewall.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
     - Verify that the IP address for your VPN firewall and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows Run dialog box, type:

ping -n 10 <IP address>

in which `<IP address>` is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your computer has the IP address of your VPN firewall listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel.
- Check to see that the network address of your computer (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, dish, or router is connected and functioning.
- For IPv4 connections, if your ISP assigned a host name, system name, or account name to your computer, enter that name in the Account Name field on a WAN IPv4 ISP Settings screen. You might also need to enter the assigned domain name or workgroup name in the Domain Name field, and you might have to enter additional information. For more information, see *Manually Configure an IPv4 Internet Connection* on page 34.
- Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If so, you need to configure your VPN firewall to *clone* or *spoof* the MAC address from the authorized computer. You can do this in the Router's MAC Address section on the WAN Advanced Options screen. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 71.

Restore the Default Configuration and Password

➢ **To reset the VPN firewall to the original factory default settings, you can use one of the following two methods:**

- Press the factory default **Reset** button on the rear panel of the VPN firewall (see *Rear Panel* on page 19) and hold the button for about 8 seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default settings when you do not know the administration password or IP address, you need to use the factory default Reset button method.
- Use the Default button on the Settings Backup and Firmware Upgrade screen:

  a. Select **Administration > Settings Backup & Upgrade**:

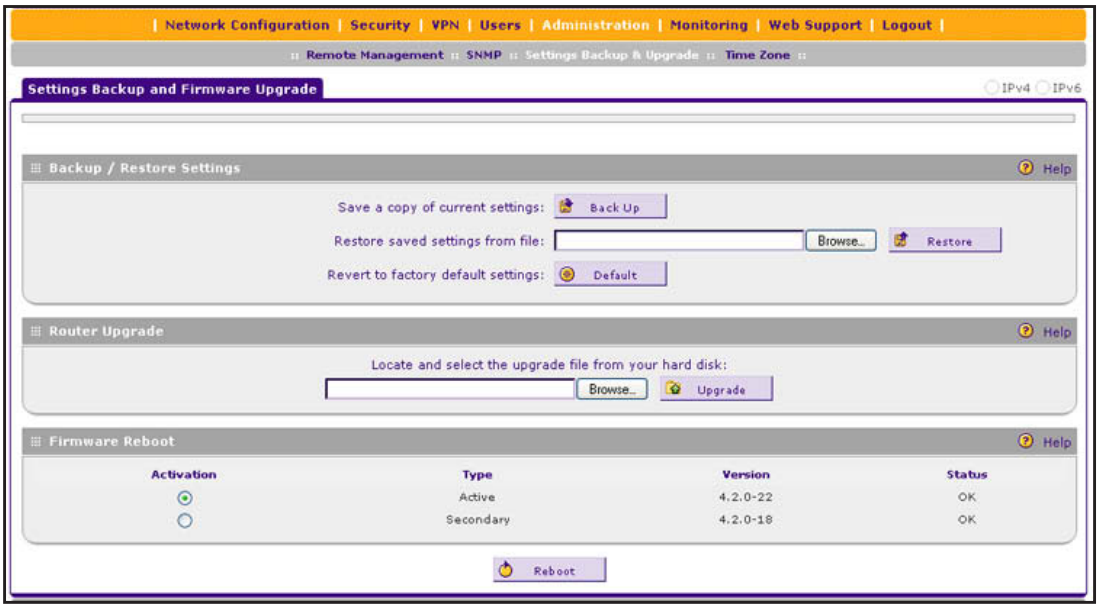

Figure 261.

b. In the Backup / Restore Settings section of the screen, click the **Default** button.

The VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

WARNING:

When you press the hardware factory default Reset button or click the software Default button, the VPN firewall settings are erased. All firewall rules, VPN policies, LAN and WAN settings, and other settings are lost. Back up your settings if you intend on using them.

Note: After you reboot with factory default settings, the VPN firewall's password is **password**, and the LAN IPv4 address is **192.168.1.1**.

Address Problems with Date and Time

The System Date & Time screen displays the current date and time of day (see *Configure Date and Time Service* on page 352). The VPN firewall 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 VPN firewall 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 VPN firewall, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour. Cause: The VPN firewall does not automatically sense daylight saving time. Go to the Time Zone screen (**Administration > Time Zone**), and select or clear the **Automatically Adjust for Daylight Savings Time** check box.

Access the Knowledge Base and Documentation

➢ **To access NETGEAR's knowledge base for the VPN firewall:**

Select **Web Support > Knowledgebase**.

➢ **To access NETGEAR's documentation library for your VPN firewall model:**

Select **Web Support > Documentation**.

Default Settings and Technical Specifications

A

This appendix provides the default settings and the physical and technical specifications of the VPN firewall in the following sections:

- *Factory Default Settings*
- *Physical and Technical Specifications*

Factory Default Settings

You can use the factory default **Reset** button on the rear panel to reset all settings to their factory defaults. This is called a hard reset (for more information, see *Revert to Factory Default Settings* on page 349):

- To perform a hard reset, press and hold the factory default Reset button for approximately 8 seconds (until the Test LED blinks rapidly). The VPN firewall returns to the factory configuration settings that are shown in the following table.
- Pressing the factory default Reset button for a shorter period causes the VPN firewall to reboot.

The following table shows the default configuration settings for the VPN firewall:

Table 100. VPN firewall factory default configuration settings

Feature		Default Behavior
Login settings		
	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
WAN settings		
	WAN IPv4 mode (all WAN interfaces)	NAT
	WAN IPv4 load balancing settings (all WAN interfaces)	Primary WAN mode
	WAN IPv6 mode (all WAN interfaces)	IPv4 only mode
	Stateless IP/ICMP Translation (SIIT)	Disabled
	WAN MAC address (all WAN interfaces)	Use default MAC addresses of the VPN firewall.
	WAN MTU size (all WAN interfaces)	1500 bytes 1492 bytes for PPPoE connections
	Port speed (all WAN interfaces)	AutoSense
	Secondary IPv4 WAN addresses	None
	Dynamic DNS for IPv4	Disabled
	WAN QoS profiles for IPv4	None

Table 100. VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
IPv4 LAN, DMZ, and routing settings		
	LAN IPv4 address for the default VLAN	192.168.1.1
	LAN IPv4 subnet mask for the default VLAN	255.255.255.0
	VLAN 1 membership	All ports
	LAN DHCP server for the default VLAN	Enabled
	LAN DHCP IPv4 starting address for the default VLAN	192.168.1.100
	LAN DHCP IPv4 ending address for the default VLAN	192.168.1.254
	VLAN MAC addresses	All LAN ports share the same MAC address
	Broadcast of ARP packets	Enabled for the default VLAN
	DMZ port for IPv4	Disabled
	DMZ IPv4 address (Port 4)	172.16.2.1
	DMZ IPv4 subnet mask (Port 4)	255.255.255.0
	DMZ DHCP server	Disabled
	DMZ DHCP IPv4 starting address	176.16.2.100
	DMZ DHCP IPv4 ending address	176.16.2.254
	RIP direction	None
	RIP version	Disabled
	RIP authentication	Disabled
IPv6 LAN and DMZ settings		
	LAN IPv6 address	fec0::1
	LAN IPv6 prefix length	64
	LAN DHCPv6 server	Disabled
	DMZ port for IPv6	Disabled
	DMZ IPv6 address (Port 4)	176::1
	DMZ IPv6 prefix length (Port 4)	64
	DMZ DHCPv6 server	Disabled

Table 100. VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
Firewall and security settings		
	Inbound LAN WAN rules (communications coming in from the Internet)	All traffic is blocked, except for traffic in response to requests from the LAN.
	Outbound LAN WAN rules (communications from the LAN to the Internet)	All traffic is allowed.
	Inbound and outbound DMZ WAN rules	None
	Inbound and outbound LAN DMZ rules	None
	Respond to ping on WAN (Internet) ports	Disabled
	Stealth mode	Enabled
	TCP flood	Enabled
	UDP flood	Enabled
	Respond to ping on LAN ports	Disabled
	IPv4 VPN pass-through for IPSec in NAT mode	Enabled
	IPv4 VPN pass-through for PPTP in NAT mode	Enabled
	IPv4 VPN pass-through for L2TP in NAT mode	Enabled
	IPv6 VPN pass-through for IPSec	Enabled
	Multicast pass-through for IGMP	Disabled
	Session limits	Disabled
	TCP time-out	1200 seconds
	UDP time-out	180 seconds
	ICMP time-out	8 seconds
	SIP ALG	Disabled
	Source MAC filtering	Disabled
	IP/MAC bindings	Disabled
	Port triggering rules	None
	UPnP	Disabled
	Bandwidth profiles	None
	QoS profiles (for IPv4 firewall rules)	None

Table 100. VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
	QoS priorities (for IPv6 firewall rules)	Normal-Service Minimize-Cost Maximize-Reliability Maximize-Throughput Minimize-Delay
	Content filtering	Disabled
	Proxy server blocking	Disabled
	Java applets blocking	Disabled
	ActiveX controls blocking	Disabled
	Cookies blocking	Disabled
	Blocked keywords	None
	Trusted domains	All
VPN IPsec Wizard: IKE policy settings for IPv4 and IPv6 gateway-to-gateway tunnels		
	Exchange mode	Main
	ID type	Local WAN IP address
	Local WAN ID	Local WAN IP address
	Remote WAN ID	Not applicable
	Encryption algorithm	3DES
	Authentication algorithm	SHA-1
	Authentication method	Pre-shared Key
	Key group	DH-Group 2 (1024 bit)
	Life time	8 hours
VPN IPsec Wizard: VPN policy settings for IPv4 and IPv6 gateway-to-gateway tunnels		
	Encryption algorithm	3DES
	Authentication algorithm	SHA-1
	Life time	1 hour
	Key group	DH-Group 2 (1024 bit)
	NetBIOS	Enabled

Table 100. VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
VPN IPsec Wizard: IKE policy settings for IPv4 gateway-to-client tunnels		
	Exchange mode	Aggressive
	ID type	FQDN
	Local WAN ID	remote.com
	Remote WAN ID	local.com
	Encryption algorithm	3DES
	Authentication algorithm	SHA-1
	Authentication method	Pre-shared Key
	Key group	DH-Group 2 (1024 bit)
	Life time	8 hours
VPN IPsec Wizard: VPN policy settings for IPv4 gateway-to-client tunnels		
	Encryption algorithm	3DES
	Authentication algorithm	SHA-1
	Life time	1 hour
	Key group	DH-Group 2 (1024 bit)
	NetBIOS	Disabled
RADIUS settings		
	Primary RADIUS server	Disabled and none configured
	Secondary RADIUS server	Disabled and none configured
	RADIUS time-out period	30 seconds
	RADIUS maximum retry count	4
SSL VPN settings		
	SSL VPN IPv4 client address range	192.168.251.1–192.168.251.254
	SSL VPN IPv6 client address range	4000::1–4000::200
User, group, and domain settings		
	default domain	geardomain
	default group	geardomain
	default users, default passwords	admin, password
		guest, password

Table 100. VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
Administrative and monitoring settings		
	Secure HTTP management	Enabled
	Telnet management	Disabled
	Traffic meter	Disabled
	SNMP	Disabled
	Time zone	GMT
	Time zone adjusted for daylight saving time	Disabled
	Routing logs	Disabled
	System Logs	Disabled
	Other event logs	Disabled
	Email logs	Disabled
	Syslogs	Disabled
	IPSec VPN logs	Enabled
	SSL VPN logs	Enabled

Physical and Technical Specifications

The following table shows the physical and technical specifications for the VPN firewall:

Table 101. VPN firewall physical and technical specifications

Feature		Specification
Network protocol and standards compatibility		
	Data and Routing Protocols	TCP/IP, RIP-1, RIP-2, PPP over Ethernet (PPPoE), DHCP, DHCPv6
Power adaptor		
	Universal input	100–240V, AC/50–60 Hz, 1.2 Amp maximum
Dimensions and weight		
	Dimensions (W x H x D)	33 x 4.3 x 20.9 cm (13 x 1.7 x 8.2 in)
	Weight	2.1 kg (4.8 lb)

Table 101. VPN firewall physical and technical specifications (continued)

Feature		Specification
Environmental specifications		
	Operating temperatures	0º to 45º C
		32º to 113º F
	Storage temperatures	–20º to 70º C
		–4º to 158º F
	Operating humidity	90% maximum relative humidity, noncondensing
	Storage humidity	95% maximum relative humidity, noncondensing
Electromagnetic emissions		
	Meets requirements of	FCC Class A
		CE
		WEEE
		RoHS
Wired compliance		
	See *Appendix E, Notification of Compliance*.	
Interface specifications		
	4 LAN, one of which is a configurable DMZ interface	AutoSense 10/100/1000BASE-T, RJ-45
	4 WAN	AutoSense 10/100/1000BASE-T, RJ-45
	1 administrative console port	RS-232

The following table shows the IPSec VPN specifications for the VPN firewall:

Table 102. VPN firewall IPSec VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	125
IPSec authentication algorithm	SHA-1, MD5
IPSec encryption algorithm	DES, 3DES, AES-128, AES-192, AES-256
IPSec key exchange	IKE, manual key, pre-shared key, X.509 certificate
IPSec authentication types	Local user database, RADIUS PAP, RADIUS CHAP
IPSec certificates supported	CA certificates, self-signed certificate

The following table shows the SSL VPN specifications for the VPN firewall:

Table 103. VPN firewall SSL VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	50
SSL versions	SSLv3, TLS1.0
SSL encryption algorithm	DES, 3DES, ARC4, AES-128, AES-192, AES-256
SSL message integrity	MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1
SSL authentication types	Local user database, RADIUS-PAP, RADIUS-CHAP, RADIUS-MSCHAP, RADIUS-MSCHAPv2, WiKID-PAP, WiKID-CHAP, MIAS-PAP, MIAS-CHAP, NT domain, Active Directory, LDAP
SSL certificates supported	CA certificates, self-signed certificate

Network Planning for Multiple WAN Ports

B

This appendix describes the factors to consider when planning a network using a firewall that has more than one WAN port.

This appendix contains the following sections:

What to Consider Before You Begin

The VPN firewall 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 several 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 several 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 need an FQDN to implement features such as exposed hosts and virtual private networks.
        - For load balancing mode, you might still need an FQDN either for convenience or to remotely access a dynamic WAN IP address.
      - Protocol binding.
        - For auto-rollover mode, protocol binding does not apply.
        - For load balancing mode, decide which protocols should be bound to a specific WAN port.
        - You can also add your own service protocols to the list.
2. Set up your accounts.
   a. Obtain active Internet services such as DSL broadband accounts, and locate the Internet service provider (ISP) configuration information.
      - In this manual, the WAN side of the network is presumed to be provisioned as shown in the following figure, with two ISPs connected to the VPN firewall through separate physical facilities.
      - Each WAN port needs to be configured separately, whether you are using a separate ISP for each WAN port or you are using the same ISP to route the traffic of both WAN ports.
      - If your ISP charges by the volume of data traffic each month, consider enabling the VPN firewall's traffic meter to monitor or limit your traffic.

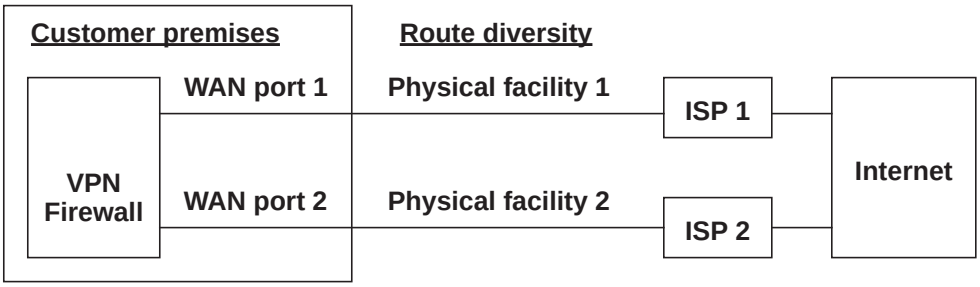

Figure 262.

b. Contact a Dynamic DNS service, and register FQDNs for one or both WAN ports.

3. Plan your network management approach.
   - The VPN firewall can be managed remotely, but you need to enable remote management locally after each factory default reset.

     NETGEAR strongly advises you to change the default management password to a strong password before enabling remote management.
   - if the factory default settings are not suitable for your installation, you can choose various WAN options. 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 VPN firewall are in the *ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 Installation Guide*.

Cabling and Computer Hardware Requirements

For you to use the VPN firewall in your network, each computer needs to have an Ethernet network interface card (NIC) installed and needs to be equipped with an Ethernet cable. If the computer connects to your network at 100 Mbps or higher speeds, you need to use a Category 5 (Cat 5) cable.

Computer Network Configuration Requirements

The VPN firewall integrates a web management interface. To access the configuration screens on the VPN firewall, you need to use a Java-enabled web browser that supports HTTP uploads, such as Microsoft Internet Explorer 6 or later, Mozilla Firefox 3 or later, or Apple Safari 3 or later with JavaScript, cookies, and SSL enabled. Free browsers are readily available for Windows, Macintosh, and UNIX/Linux.

For the initial connection to the Internet and configuration of the VPN firewall, you need to connect a computer to the VPN firewall, and the computer needs to be configured to automatically get its TCP/IP configuration from the VPN firewall through DHCP.

The DSL broadband access device needs to provide a standard Ethernet interface.

Internet Configuration Requirements

Depending on how your ISP sets up your Internet accounts, you need the following Internet configuration information to connect VPN firewall to the Internet:

- Host and domain names
- One or more ISP login names and passwords
- ISP Domain Name Server (DNS) addresses
- One or more fixed IP addresses (also known as static IP addresses)

Where Do I Get the Internet Configuration Information?

There are several ways you can gather the required Internet connection information.

Your ISPs provide all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide you with it, or, if you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.

- For Windows 95/98/ME, open the Network Control Panel, select the TCP/IP entry for the Ethernet adapter, and click **Properties**. Record all the settings for each tab 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 this page with the Internet connection information. Fill in the configuration settings that are provided to you by ISP.

- **ISP login name**. The login name and password are case-sensitive and need to be entered exactly as given by your ISP. For AOL customers, the login name is their primary screen name. Some ISPs use your full email address as the login name. The service name is not required by all ISPs. If you connect using a login name and password, 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 such as CCA7324-A or home. If you have not been given host or domain names, you can use the following examples as a guide:
  - If your main email account with your ISP is aaa@yyy.com, 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, use **xxx.yyy.com** as the domain name.

  ISP host name: _____

  ISP domain name: _____

- **Fully qualified domain name**. Some organizations use a fully qualified domain name (FQDN) from a Dynamic DNS service provider for their IP addresses.

  Dynamic DNS service provider: _____

  FQDN: _____

Overview of the Planning Process

The areas that require planning when you use a firewall that has multiple WAN ports such as the VPN firewall include the following:

- Inbound traffic (port forwarding, port triggering)
- Outbound traffic (protocol binding)
- Virtual private networks (VPNs)

Two WAN ports can be configured on a mutually exclusive basis to do either of the following:

- Auto-rollover for increased reliability
- Load balance for outgoing traffic

These various types of traffic and auto-rollover or load balancing all interact to make the planning process more challenging:

- **Inbound traffic**. Unrequested incoming traffic can be directed to a computer on your LAN rather than being discarded. The mechanism for making the IP address public depends on whether the dual WAN ports are configured for auto-rollover or load balancing.
- **Virtual private networks**. A virtual private network (VPN) tunnel provides a secure communication channel either between two gateway VPN firewalls or between a remote computer client and gateway VPN firewall. As a result, the IP address of at least one of the tunnel endpoints needs to be known in advance in order for the other tunnel endpoint to establish (or reestablish) the VPN tunnel.

Note: When the VPN firewall's WAN port rolls over, the VPN tunnel closes and needs to be reestablished using the new WAN IP address. However, you can configure automatic IPSec VPN rollover to ensure that an IPSec VPN tunnel is reestablished.

- **Dual WAN ports in auto-rollover mode**. Rollover for a VPN firewall 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.

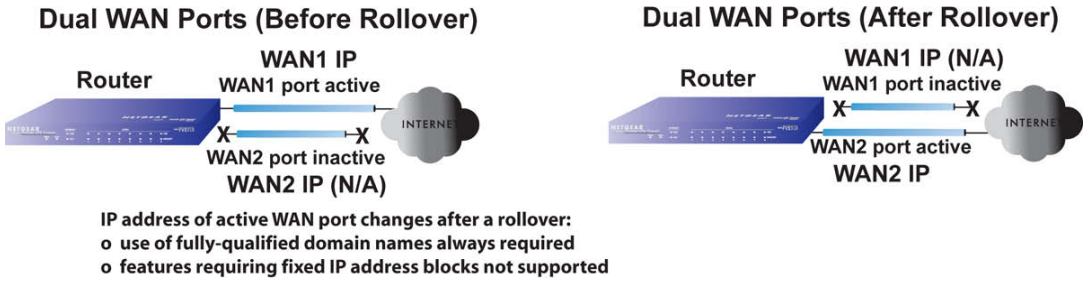

Figure 263.

Features such as multiple exposed hosts are not supported in auto-rollover mode because the IP addresses of each WAN port need to be in the identical range of fixed addresses.

- **Dual WAN ports in load balancing mode**. Load balancing for a VPN firewall with dual WAN ports is similar to a single WAN gateway configuration when you specify the IP address. Each IP address is either fixed or dynamic based on the ISP: You need to use FQDNs when the IP address is dynamic, but FQDNs are optional when the IP address is static.

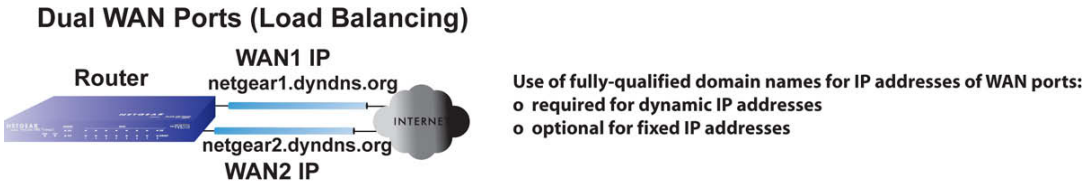

Figure 264.

Inbound Traffic

- *Inbound Traffic to a Single WAN Port System*
- *Inbound Traffic to a Dual WAN Port System*

Incoming traffic from the Internet is normally discarded by the VPN firewall 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 VPN firewall to forward it to one or more LAN hosts on your network.

The addressing of the VPN firewall's dual WAN port depends on the configuration being implemented.

Table 104. IP addressing requirements for exposed hosts in a dual WAN port configuration

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 VPN firewall's WAN port needs to be known to the public so that the public can send incoming traffic to the exposed host when this feature is supported and enabled.

In the single WAN case, the WAN's Internet address is either a fixed IP address or an FQDN if the IP address is dynamic.

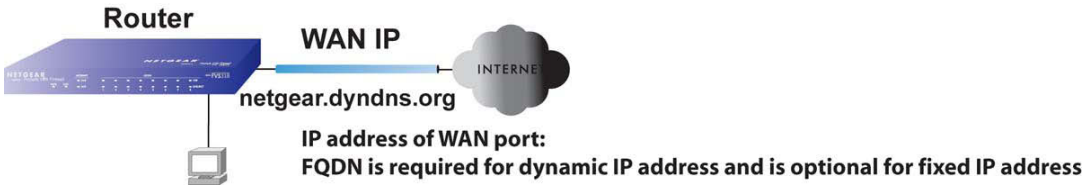

Figure 265.

Inbound Traffic to a Dual WAN Port System

The IP address range of the VPN firewall's WAN port needs to be both fixed and public so that the public can send incoming traffic to the multiple exposed hosts when this feature is supported and enabled.

Inbound Traffic: Dual WAN Ports for Improved Reliability

In a dual WAN port auto-rollover configuration, the WAN port's IP address always changes when a rollover occurs. You need to use an FQDN that toggles between the IP addresses of the WAN ports (that is, WAN1 or WAN2).

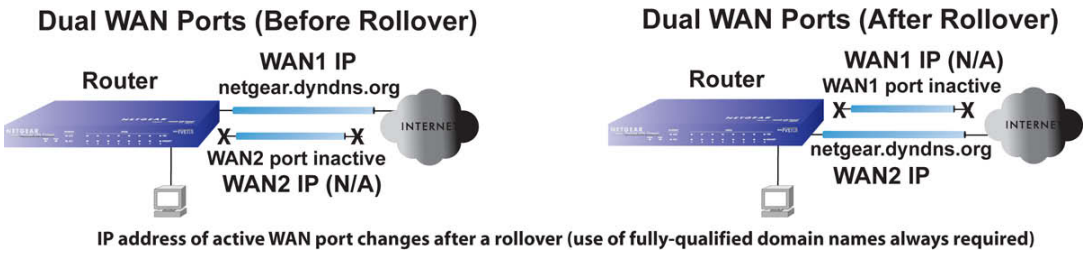

Figure 266.

Inbound Traffic: Dual WAN Ports for Load Balancing

In a dual WAN port load balancing configuration, the Internet address of each WAN port is either fixed if the IP address is fixed or an FQDN if the IP address is dynamic (see the following figure).

Note: Load balancing is implemented for outgoing traffic and not for incoming traffic. To maintain better control of WAN port traffic, consider to make one of the WAN port Internet addresses public and to keep the other one private.

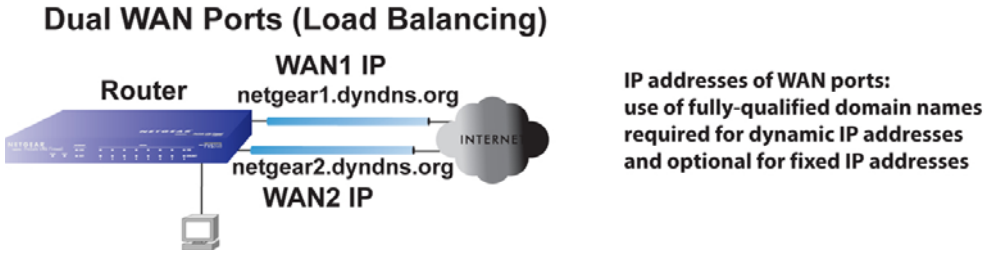

Figure 267.

Virtual Private Networks

- *VPN Road Warrior (Client-to-Gateway)*
- *VPN Gateway-to-Gateway*
- *VPN Telecommuter (Client-to-Gateway through a NAT Router)*

When implementing virtual private network (VPN) tunnels, you need to use a mechanism for determining the IP addresses of the tunnel endpoints. The addressing of the firewall's WAN ports in a dual WAN port auto-rollover or load balancing configuration depends on the configuration being implemented.

Table 105. IP addressing requirements for VPNs in a dual WAN port configuration

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. After a rollover, all tunnels need to be reestablished using the new WAN IP address.

For a single WAN gateway configuration, use an FQDN when the IP address is dynamic and either an FQDN or the IP address itself when the IP address is fixed. The situation is different in dual WAN port gateway configurations.

- **Dual WAN ports in auto-rollover mode**. A gateway configuration with dual WAN ports that function in auto-rollover mode is different from a gateway configuration with a single WAN port 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 VPN firewall's WAN port rolls over, the VPN tunnel collapses and needs to be reestablished using the new WAN IP address. However, you can configure automatic IPSec VPN rollover to ensure that an IPSec VPN tunnel is reestablished.

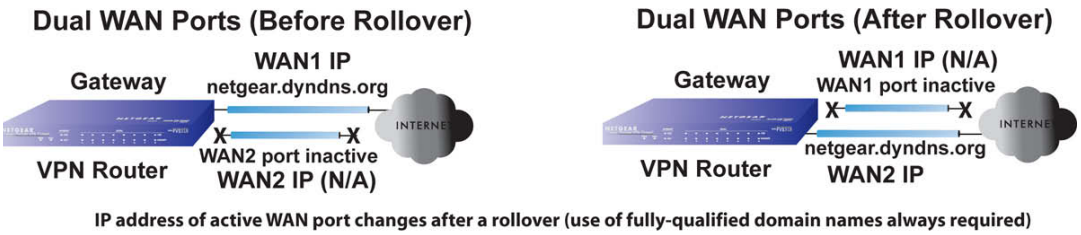

Figure 268.

- **Dual WAN ports in load balancing mode**. A gateway configuration with dual WAN ports that function in load balancing mode is the same as a single WAN port configuration when you specify the IP address of the VPN tunnel endpoint. Each IP address is either fixed or dynamic based on the ISP: You need to use FQDNs when the IP address is dynamic, and FQDNs are optional when the IP address is static.

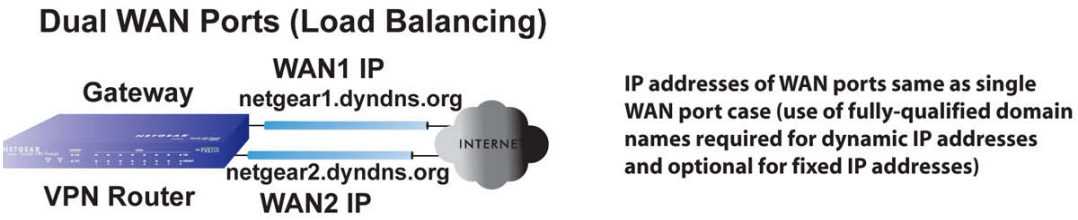

Figure 269.

VPN Road Warrior (Client-to-Gateway)

The following situations exemplify the requirements for a remote computer client with no firewall to establish a VPN tunnel with a gateway VPN firewall:

- 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 computer client initiates the VPN tunnel because the IP address of the remote computer client is not known in advance. The gateway WAN port needs to act as the responder.

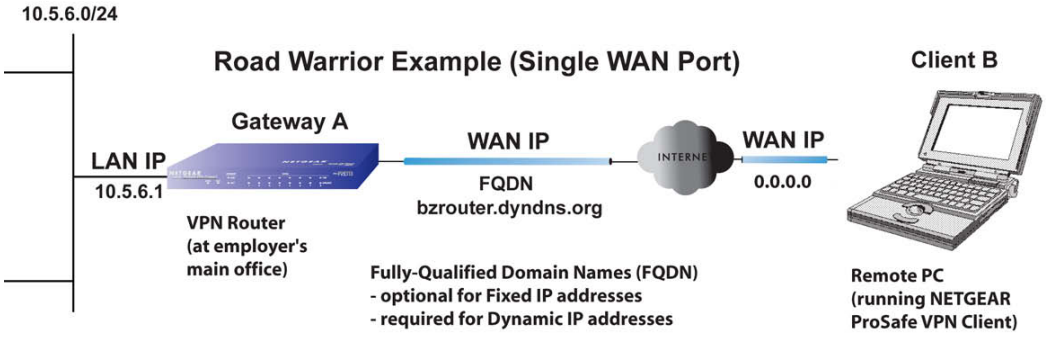

Figure 270.

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, an FQDN needs to be used. If the IP address is fixed, an FQDN is optional.

VPN Road Warrior: Dual-Gateway WAN Ports for Improved Reliability

In a gateway configuration with dual WAN ports that function in auto-rollover mode, the remote computer client initiates the VPN tunnel with the active WAN port (port WAN1 in the following figure) because the IP address of the remote computer client is not known in advance. The gateway WAN port needs to act as a responder.

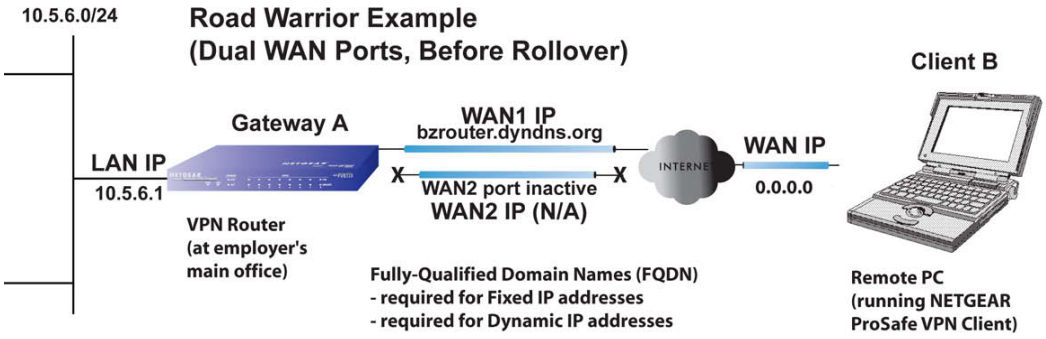

Figure 271.

The IP addresses of the WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN port could be either WAN1 or WAN2 (that is, the IP address of the active WAN port is not known in advance).

After a rollover of the WAN port has occurred, the previously inactive gateway WAN port becomes the active port (port WAN2 in the following figure) and the remote computer client needs to reestablish the VPN tunnel. The gateway WAN port needs to act as the responder.

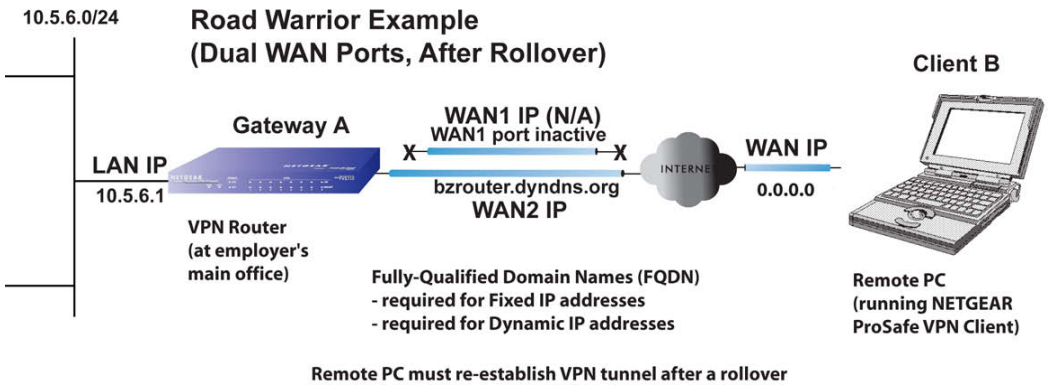

Figure 272.

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 computer client can determine the gateway IP address to establish or reestablish a VPN tunnel.

VPN Road Warrior: Dual-Gateway WAN Ports for Load Balancing

In a gateway configuration with dual WAN ports that function in load balancing mode, the remote computer initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the active WAN port is not known in advance. The selected gateway WAN port needs to act as the responder.

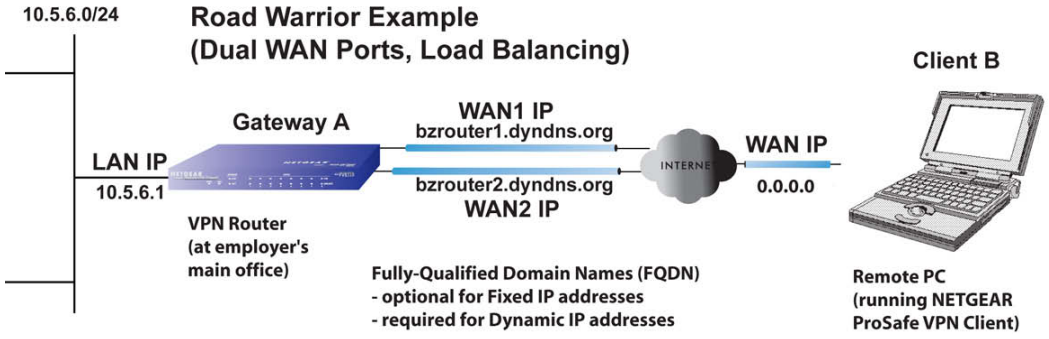

Figure 273.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Gateway-to-Gateway

The following situations exemplify the requirements for a gateway VPN firewall to establish a VPN tunnel with another gateway VPN firewall:

- Single-gateway WAN ports
- Redundant dual-gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Gateway-to-Gateway: Single-Gateway WAN Ports (Reference Case)

In a configuration with two single WAN port gateways, either gateway WAN port can initiate the VPN tunnel with the other gateway WAN port because the IP addresses are known in advance.

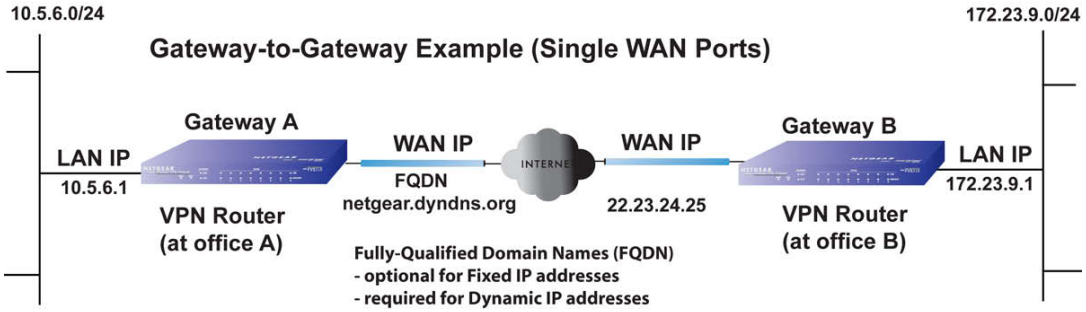

Figure 274.

The IP address of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Gateway-to-Gateway: Dual-Gateway WAN Ports for Improved Reliability

In a configuration with two dual WAN port VPN gateways that function in auto-rollover mode, either of the gateway WAN ports at one end can initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to balance the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance. In this example (see the following figure), port WAN_A1 is active and port WAN_A2 is inactive at Gateway A; port WAN_B1 is active and port WAN_B2 is inactive at Gateway B.

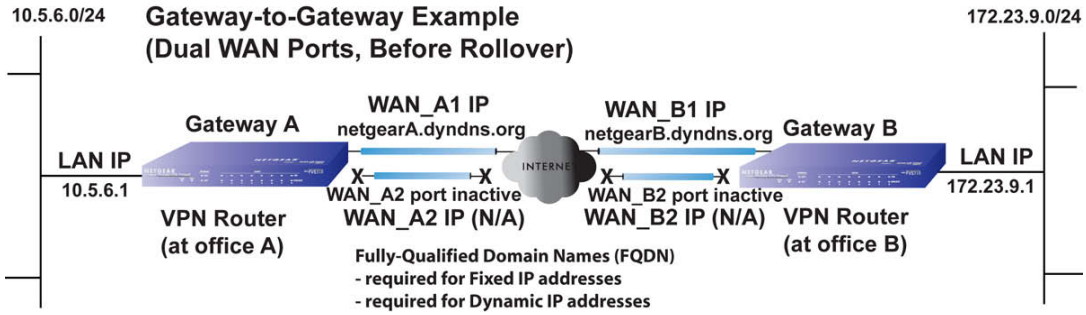

Figure 275.

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN ports could be either WAN_A1, WAN_A2, WAN_B1, or WAN_B2 (that is, the IP address of the active WAN ports is not known in advance).

After a rollover of a gateway WAN port, the previously inactive gateway WAN port becomes the active port (port WAN_A2 in the following figure), and one of the gateways needs to reestablish the VPN tunnel.

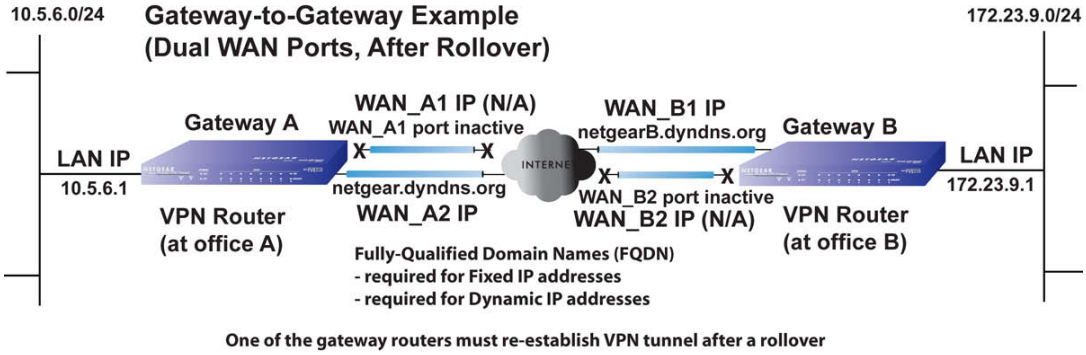

Figure 276.

The purpose of the FQDNs is to toggle the domain name of the rolled-over gateway between the IP addresses of the active WAN port (that is, WAN_A1 and WAN_A2 in the previous figure) so that the other end of the tunnel has a known gateway IP address to establish or reestablish a VPN tunnel.

VPN Gateway-to-Gateway: Dual-Gateway WAN Ports for Load Balancing

In a configuration with two dual-WAN port VPN gateways that function in load balancing mode, either of the gateway WAN ports at one end can be programmed in advance to initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to manage the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance.

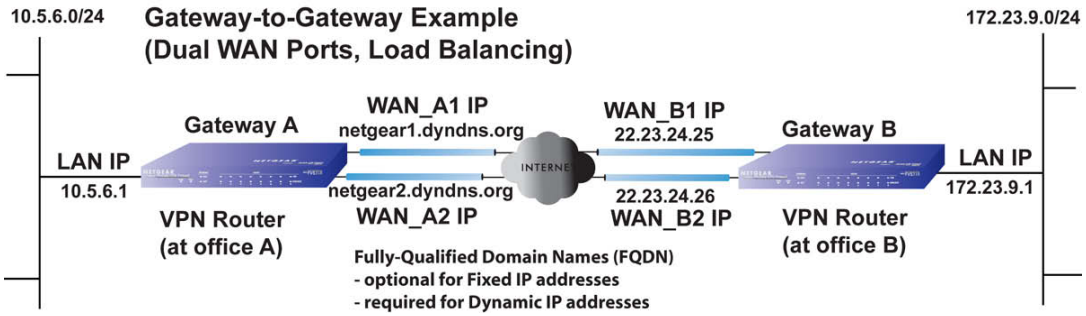

Figure 277.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Telecommuter (Client-to-Gateway through a NAT Router)

Note: The telecommuter case presumes the home office has a dynamic IP address and NAT router.

The following situations exemplify the requirements for a remote computer client connected to the Internet with a dynamic IP address through a NAT router to establish a VPN tunnel with a gateway VPN firewall 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 computer client at the NAT router initiates the VPN tunnel because the IP address of the remote NAT router is not known in advance. The gateway WAN port needs to act as the responder.

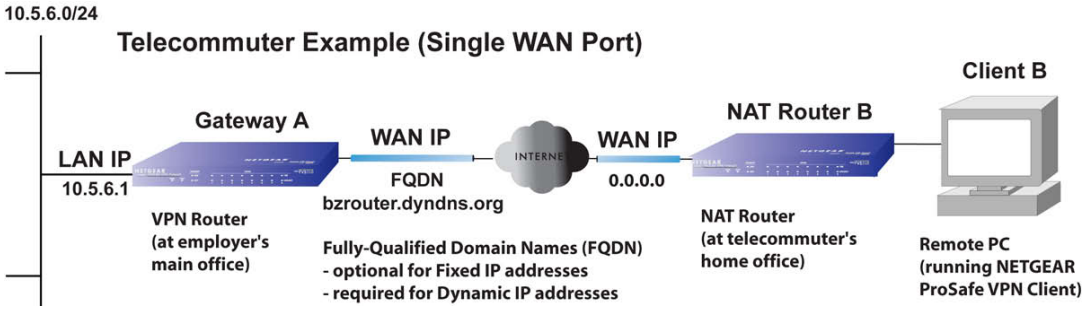

Figure 278.

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, you need to use an FQDN. If the IP address is fixed, an FQDN is optional.

VPN Telecommuter: Dual-Gateway WAN Ports for Improved Reliability

In a gateway configuration with dual WAN ports that function in auto-rollover mode, the remote computer client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in the following figure) because the IP address of the remote NAT router is not known in advance. The gateway WAN port needs to act as the responder.

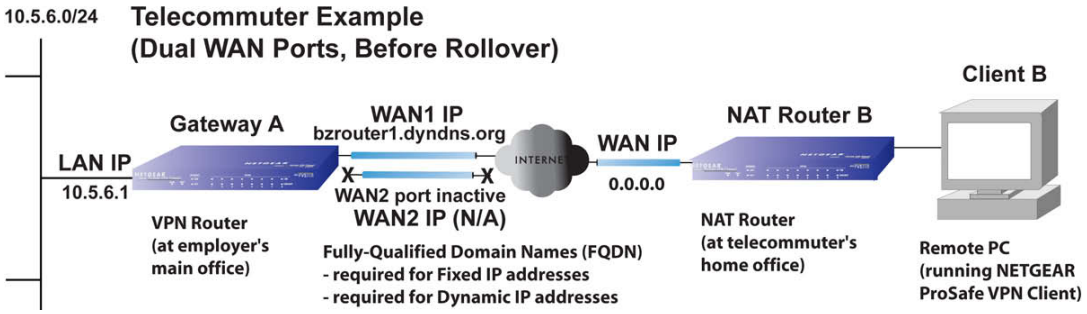

Figure 279.

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN port could be either WAN1 or WAN2 (that is, the IP address of the active WAN port is not known in advance).

After a rollover of the WAN port has occurred, the previously inactive gateway WAN port becomes the active port (port WAN2 in the following figure), and the remote computer needs to reestablish the VPN tunnel. The gateway WAN port needs to act as the responder.

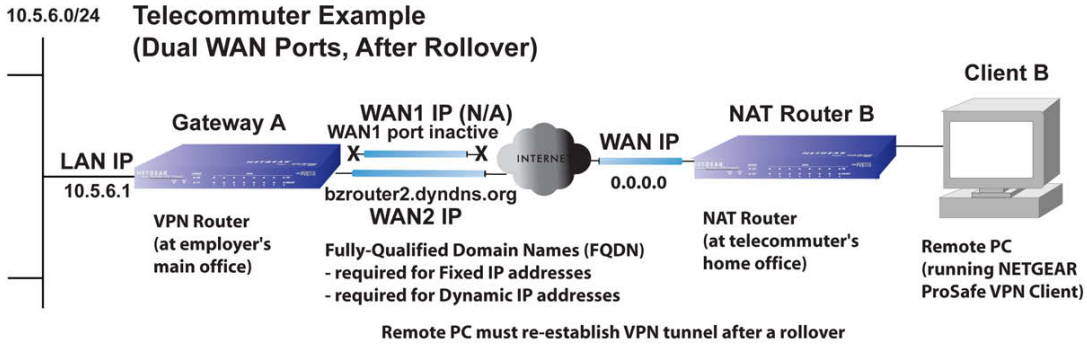

Figure 280.

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 computer client can determine the gateway IP address to establish or reestablish a VPN tunnel.

VPN Telecommuter: Dual-Gateway WAN Ports for Load Balancing

In a gateway configuration with dual WAN ports that function in load balancing mode, the remote computer client initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote NAT router is not known in advance. The selected gateway WAN port needs to act as the responder.

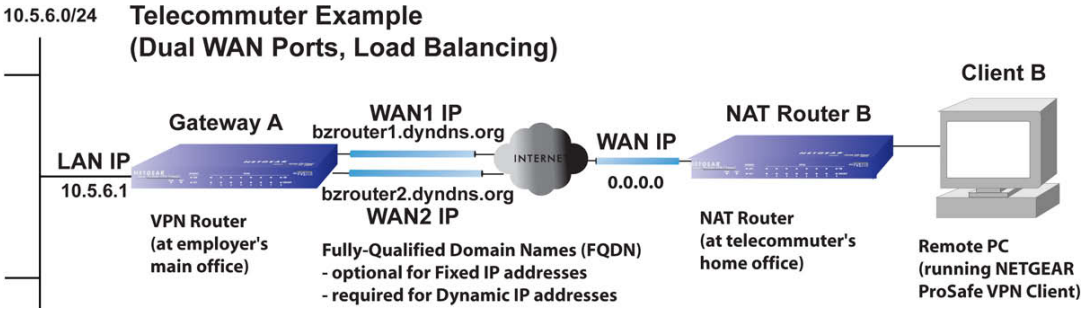

Figure 281.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

System Logs and Error Messages

C

This appendix provides examples and explanations of system logs and error message. When applicable, a recommended action is provided.

This appendix contains the following sections:

Log Message Terms

This appendix uses the following log message terms.

Table 106. Log message terms

Term	Description
[SRX5308]	System identifier.
[kernel]	Message from the kernel.
CODE	Protocol code (for example, protocol is ICMP, type 8) and CODE=0 means successful reply.
DEST	Destination IP address of the machine to which the packet is destined.
DPT	Destination port.
IN	Incoming interface for packet.
OUT	Outgoing interface for packet.
PROTO	Protocol used.
SELF	Packet coming from the system only.
SPT	Source port.
SRC	Source IP address of machine from which the packet is coming.
TYPE	Protocol type.

System Log Messages

- *NTP*
- *Login/Logout*
- *System Startup*
- *Reboot*
- *Firewall Restart*
- *IPSec Restart*
- *Unicast, Multicast, and Broadcast Logs*
- *WAN Status*
- *Resolved DNS Names*
- *VPN Log Messages*
- *Traffic Meter Logs*

This section describes log messages that belong to one of the following categories:

- Logs generated by traffic that is meant for the VPN firewall.
- Logs generated by traffic that is routed or forwarded through the VPN firewall.
- Logs generated by system daemons, the NTP daemon, the WAN daemon, and other daemons.

For information about how to select many of these logs, see *Configure Logging, Alerts, and Event Notifications* on page 362.

NTP

This section describes log messages generated by the NTP daemon during synchronization with the NTP server.

Table 107. System logs: NTP

Message	Nov 28 12:31:13 [SRX5308] [ntpdate] Looking Up time-f.netgear.com Nov 28 12:31:13 [SRX5308] [ntpdate] Requesting time from time-f.netgear.com Nov 28 12:31:14 [SRX5308] [ntpdate] adjust time server 69.25.106.19 offset 0.140254 sec Nov 28 12:31:14 [SRX5308] [ntpdate] Synchronized time with time-f.netgear.com Nov 28 12:31:16 [SRX5308] [ntpdate] Date and Time Before Synchronization: Tue Nov 28 12:31:13 GMT+0530 2006 Nov 28 12:31:16 [SRX5308] [ntpdate] Date and Time After Synchronization: Tue Nov 28 12:31:16 GMT+0530 2006 Nov 28 12:31:16 [SRX5308] [ntpdate] Next Synchronization after 2 Hours
Explanation	Message 1: DNS resolution for the NTP server (time-f.netgear.com). Message 2: Request for NTP update from the time server. Message 3: Adjust time by re-setting system time. Message 4: Display date and time before synchronization, that is, when resynchronization started. Message 5: Display the new updated date and time. Message 6: Next synchronization will be after the specified time. Example: In these logs the next synchronization will be after 2 hours. The synchronization time interval is configurable through the CLI.
Recommended action	None

Login/Logout

This section describes logs generated by the administrative interfaces of the device.

Table 108. System logs: login/logout

Message	Nov 28 14:45:42 [SRX5308] [login] Login succeeded: user admin from 192.168.10.10
Explanation	Login of user admin from host with IP address 192.168.10.10.

Table 108. System logs: login/logout (continued)

Recommended action	None
Message	Nov 28 14:55:09 [SRX5308] [seclogin] Logout succeeded for user admin Nov 28 14:55:13 [SRX5308] [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

System Startup

This section describes the log message generated during system startup.

Table 109. System logs: system startup

Message	Jan 1 15:22:28 [SRX5308] [ledTog] [SYSTEM START-UP] System Started
Explanation	Log generated when the system is started.
Recommended action	None

Reboot

This section describes the log message generated during system reboot.

Table 110. System logs: reboot

Message	Nov 25 19:42:57 [SRX5308] [reboot] Rebooting in 3 seconds
Explanation	Log generated when the system is rebooted from the web management interface.
Recommended action	None

Firewall Restart

This section describes logs that are generated when the VPN firewall restarts.

Table 111. System logs: VPN firewall restart

Message	Jan 23 16:20:44 [SRX5308] [wand] [FW] Firewall Restarted
Explanation	Log generated when the VPN firewall is restarted. This message is logged when the VPN firewall restarts after any changes in the configuration are applied.
Recommended action	None

IPSec Restart

This section describes logs that are generated when IPSec restarts.

Table 112. System logs: IPSec restart

Message	Jan 23 16:20:44 [SRX5308] [wand] [IPSEC] IPSEC Restarted
Explanation	Log generated when the IPSec is restarted. This message is logged when IPSec restarts after any changes in the configuration are applied.
Recommended action	None

Unicast, Multicast, and Broadcast Logs

Table 113. System logs: unicast

Message	Nov 24 11:52:55 [SRX5308] [kernel] UCAST IN=SELF OUT=WAN SRC= 192.168.10.1 DST=192.168.10.10 PROTO=UDP SPT=800 DPT=2049
Explanation	• This packet (unicast) is sent to the device from the WAN network. • For other settings, see *Table 106* on page 431.
Recommended action	None

ICMP Redirect Logs

Table 114. System logs: unicast, redirect

Message	Feb 2007 22 14:36:07 [SRX5308] [kernel] [LOG_PACKET] SRC=192.168.1.49 DST=192.168.1.124 PROTO=ICMP TYPE=5 CODE=1
Explanation	• This packet is an ICMP redirect message sent to the device by another device. • For other settings, see *Table 106* on page 431.
Recommended action	To enable these logs, from the CLI command prompt of the VPN firewall, enter this command: **`monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 1`** And to disable it enter: **`monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 0`**

Multicast/Broadcast Logs

Table 115. System logs: multicast/broadcast

Message	Jan 1 07:24:13 [SRX5308] [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 multicast or broadcast packet is sent to the device from the WAN network. • For other settings, see *Table 106* on page 431.
Recommended action	None

WAN Status

This section describes the logs generated by the WAN component. If there are several ISP links for Internet connectivity, the VPN firewall can be configured either in auto-rollover or load balancing mode.

Load Balancing

When the WAN mode is configured for load balancing, all 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 other WAN links that are active.

This section describes the logs generated when the WAN mode is set to load balancing.

Table 116. System logs: WAN status, load balancing

Message	Dec 1 12:11:27 [SRX5308] [wand] [LBFO] Restarting WAN1_ Dec 1 12:11:31 [SRX5308] [wand] [LBFO] Restarting WAN2_ Dec 1 12:11:35 [SRX5308] [wand] [LBFO] WAN1(UP), WAN2(UP)_ Dec 1 12:24:12 [SRX5308] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_ Dec 1 12:29:43 [SRX5308] [wand] [LBFO] Restarting WAN2_ Dec 1 12:29:47 [SRX5308] [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. Messages 4, 5, and 6: These messages show that one of the WAN links is down, and that restarting the WAN link does not resolve the situation. At this point, all the traffic is directed through the WAN that is up.
Recommended action	None

Auto-Rollover

When the WAN mode is configured for auto-rollover, the primary link is active, and the secondary link acts only as a backup. When the primary link goes down, the secondary link becomes active only until the primary link comes back up. The VPN firewall monitors the status of the primary link using the configured WAN failure detection method.

This section describes the logs generated when the WAN mode is set to auto-rollover.

Table 117. System logs: WAN status, auto-rollover

Message	Nov 17 09:59:09 [SRX5308] [wand] [LBFO] WAN1 Test Failed 1 of 3 times_ Nov 17 09:59:39 [SRX5308] [wand] [LBFO] WAN1 Test Failed 2 of 3 times_ Nov 17 10:00:09 [SRX5308] [wand] [LBFO] WAN1 Test Failed 3 of 3 times_ Nov 17 10:01:01 [SRX5308] [wand] [LBFO] WAN1 Test Failed 4 of 3 times_ Nov 17 10:01:35 [SRX5308] [wand] [LBFO] WAN1 Test Failed 5 of 3 times_ Nov 17 10:01:35 [SRX5308] [wand] [LBFO] WAN1(DOWN), WAN2(UP), ACTIVE(WAN2)_ Nov 17 10:02:25 [SRX5308] [wand] [LBFO] WAN1 Test Failed 6 of 3 times_ Nov 17 10:02:25 [SRX5308] [wand] [LBFO] Restarting WAN1_ Nov 17 10:02:57 [SRX5308] [wand] [LBFO] WAN1 Test Failed 7 of 3 times_ Nov 17 10:03:27 [SRX5308] [wand] [LBFO] WAN1 Test Failed 8 of 3 times_ Nov 17 10:03:57 [SRX5308] [wand] [LBFO] WAN1 Test Failed 9 of 3 times_ Nov 17 10:03:57 [SRX5308] [wand] [LBFO] Restarting WAN1_
Explanation	The logs suggest that the failover was detected after 5 attempts instead of 3. However, the reason that the messages appear in the log is because of the WAN state transition logic, which is part of the failover algorithm. These logs can be interpreted as follows: The primary link failure is correctly detected after the 3rd attempt. Thereafter, the algorithm attempts to restart the WAN connection and checks once again to determine if WAN1 is still down. This results in the 4th failure detection message. If it is still down, then it starts a secondary link, and once the secondary link is up, the secondary link is marked as active. Meanwhile, the primary link has failed once more, and that results in the 5th failure detection message. Note that the 5th failure detection message and the message suggesting that the secondary link is active have the same time stamp, and so they happen in the same algorithm state–machine cycle. So although it appears that the failover did not happen immediately after 3 failures, internally, the failover process is triggered after the 3rd failure, and transition to the secondary link is completed by the 5th failure. The primary link is also restarted every 3 failures till it is functional again. In these logs, the primary link was restarted after the 6th failure, that is, 3 failures after the failover process was triggered.
Recommended action	Check the WAN settings and WAN failure detection method configured for the primary link.

PPP Logs

This section describes the WAN PPP connection logs. The PPP type can be configured from the web management interface (see *Manually Configure an IPv4 Internet Connection* on page 34).

- PPPoE Idle Timeout Logs

Table 118. System logs: WAN status, PPPoE idle time-out

Message	Nov 29 13:12:46 [SRX5308] [pppd] Starting connection Nov 29 13:12:49 [SRX5308] [pppd] Remote message: Success Nov 29 13:12:49 [SRX5308] [pppd] PAP authentication succeeded Nov 29 13:12:49 [SRX5308] [pppd] local IP address 50.0.0.62 Nov 29 13:12:49 [SRX5308] [pppd] remote IP address 50.0.0.1 Nov 29 13:12:49 [SRX5308] [pppd] primary DNS address 202.153.32.3 Nov 29 13:12:49 [SRX5308] [pppd] secondary DNS address 202.153.32.3 Nov 29 11:29:26 [SRX5308] [pppd] Terminating connection due to lack of activity. Nov 29 11:29:28 [SRX5308] [pppd] Connect time 8.2 minutes. Nov 29 11:29:28 [SRX5308] [pppd] Sent 1408 bytes, received 0 bytes. Nov 29 11:29:29 [SRX5308] [pppd] Connection terminated.
Explanation	Message 1: PPPoE connection 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: The primary DNS server that is configured on the WAN ISP Settings screen. Message 7: The secondary DNS server that is configured on the WAN ISP Settings screen. 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 while the link was up. Message 11: PPP connection terminated after idle time-out.
Recommended action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPTP Idle Timeout Logs

Table 119. System logs: WAN status, PPTP idle time-out

Message	Nov 29 11:19:02 [SRX5308] [pppd] Starting connection Nov 29 11:19:05 [SRX5308] [pppd] CHAP authentication succeeded Nov 29 11:19:05 [SRX5308] [pppd] local IP address 192.168.200.214 Nov 29 11:19:05 [SRX5308] [pppd] remote IP address 192.168.200.1 Nov 29 11:19:05 [SRX5308] [pppd] primary DNS address 202.153.32.2 Nov 29 11:19:05 [SRX5308] [pppd] secondary DNS address 202.153.32.2 Nov 29 11:20:45 [SRX5308] [pppd] No response to 10 echo-requests Nov 29 11:20:45 [SRX5308] [pppd] Serial link appears to be disconnected. Nov 29 11:20:45 [SRX5308] [pppd] Connect time 1.7 minutes. Nov 29 11:20:45 [SRX5308] [pppd] Sent 520 bytes, received 80 bytes. Nov 29 11:20:51 [SRX5308] [pppd] Connection terminated.

Table 119. System logs: WAN status, PPTP idle time-out (continued)

Explanation	Message 1: Starting PPP connection process. Message 2: Message from the server for authentication success. Message 3: Local IP address assigned by the server. Message 4: Server side IP address. Message 6: The primary DNS server that is configured on the WAN ISP Settings screen. Message 7: The secondary DNS server that is configured on the WAN ISP Settings screen. Message 7: Sensing idle link. Message 8: Idle link sensed. Message 9: Data sent and received at the LAN side while the link was up. Message 10: PPP connection terminated after idle time-out.
Recommended action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPP Authentication Logs

Table 120. System logs: WAN status, PPP authentication

Message	Nov 29 11:29:26 [SRX5308] [pppd] Starting link Nov 29 11:29:29 [SRX5308] [pppd] Remote message: Login incorrect Nov 29 11:29:29 [SRX5308] [pppd] PAP authentication failed Nov 29 11:29:29 [SRX5308] [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.

Resolved DNS Names

This section describes the logs of DNS name resolution messages.

Table 121. System logs: DNS name resolution messages

Message	2000 Jan 1 05:12:00 [SRX5308] [dnsmasq] [DNSRESOLV]:teamf1.com from 192.168.11.2
Explanation	This log is generated when the DNS name (that is, teamf1) is resolved.
Recommended action	None

VPN Log Messages

This section explains logs that are generated by IPSec VPN and SSL VPN policies. These logs are generated automatically and do not need to be enabled.

IPSec VPN Logs

This section describes the log messages generated by IPSec VPN policies.

Note: The same IPSec VPN log messages can appear in the logs that are accessible when you select the **VPN** check box on the Firewall Logs & E-mail screen (see *Configure Logging, Alerts, and Event Notifications* on page 362) and in the logs on the IPSec VPN Logs screen (see *View the VPN Logs* on page 380).

Table 122. System logs: IPSec VPN tunnel, tunnel establishment

Messages 1 through 5	2000 Jan 1 04:01:39 [SRX5308] [wand] [IPSEC] IPSEC Restarted 2000 Jan 1 04:02:09 [SRX5308] [wand] [FW] Firewall Restarted 2000 Jan 1 04:02:29 [SRX5308] [IKE] IKE stopped_ 2000 Jan 1 04:02:31 [SRX5308] [IKE] IKE started_ 2000 Jan 1 04:02:31 [SRX5308] [wand] [IPSEC] IPSEC Restarted
Messages 6 and 7	2000 Jan 1 04:07:04 [SRX5308] [IKE] Adding IPSec configuration with identifier "pol1"_ 2000 Jan 1 04:07:04 [SRX5308] [IKE] Adding IKE configuration with identifier "pol1"_
Messages 8 through 19	2000 Jan 1 04:13:39 [SRX5308] [IKE] Configuration found for 20.0.0.1[500]._ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Received request for new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Beginning Identity Protection mode._ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: RFC XXXX_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: DPD_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] DPD is Enabled_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] For 20.0.0.1[500], Selected NAT-T version: RFC XXXX_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Setting DPD Vendor ID_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: KAME/racoon_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] NAT-D payload matches for 20.0.0.2[500]_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] NAT-D payload matches for 20.0.0.1[500]_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] NAT not detected _
Messages 20 and 21	2000 Jan 1 04:13:39 [SRX5308] [IKE] ISAKMP-SA established for 20.0.0.2[500]-20.0.0.1[500] with spi:c56f7a1d42baf28a:68fcf85e3c148bd8_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Sending Informational Exchange: notify payload[INITIAL-CONTACT]_

Table 122. System logs: IPSec VPN tunnel, tunnel establishment (continued)

Messages 22 and 23	2000 Jan 1 04:13:40 [SRX5308] [IKE] Responding to new phase 2 negotiation: 20.0.0.2[0]<=>20.0.0.1[0]_ 2000 Jan 1 04:13:40 [SRX5308] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_
Messages 24 and 25	2000 Jan 1 04:13:41 [SRX5308] [IKE] IPSec-SA established: ESP/Tunnel 20.0.0.1->20.0.0.2 with spi=34046092(0x207808c)_ 2000 Jan 1 04:13:41 [SRX5308] [IKE] IPSec-SA established: ESP/Tunnel 20.0.0.2->20.0.0.1 with spi=87179451(0x53240bb)_
Explanation	Message 1–5: IPSec, IKE, and VPN firewall restart. Message 6–7: IPSec and IKE configurations are added with the identifier “pol1.” Message 8–19: New phase 1 negotiation starts by determining the configuration for the WAN host. Dead Peer Detection (DPD) is enabled and set. NAT payload matching and NAT detection are done. Message 20–21: ISAKMP-SA is established between the 2 WANs and information is exchanged. Message 22–23: New phase 2 negotiation starts by using IPSec SA configuration pertaining to the LAN hosts. Message 24–25: IPSec-SA VPN tunnel is established.
Recommended action	None

Table 123. System logs: IPSec VPN tunnel, SA lifetime (150 sec in phase 1; 300 sec in phase 2), VPN tunnel is reestablished

Message 1	2000 Jan 1 04:32:25 [SRX5308] [IKE] Sending Informational Exchange: delete payload[]_
Messages 2 through 6	2000 Jan 1 04:32:25 [SRX5308] [IKE] purged IPSec-SA proto_id=ESP spi= 181708762._ 2000 Jan 1 04:32:25 [SRX5308] [IKE] purged IPSec-SA proto_id=ESP spi= 153677140._ 2000 Jan 1 04:32:25 [SRX5308] [IKE] an undead schedule has been deleted: 'pk_recvupdate'._ 2000 Jan 1 04:32:25 [SRX5308] [IKE] IPSec configuration with identifier "pol1" deleted successfully_ 2000 Jan 1 04:32:25 [SRX5308] [IKE] no phase 2 bounded._
Message 7	2000 Jan 1 04:32:25 [SRX5308] [IKE] Sending Informational Exchange: delete payload[]_
Messages 8 through 11	2000 Jan 1 04:32:25 [SRX5308] [IKE] Purged ISAKMP-SA with spi= d67f2be9ca0cb241:8a094623c6811286._ 2000 Jan 1 04:32:25 [SRX5308] [IKE] an undead schedule has been deleted: 'purge_remote'._ 2000 Jan 1 04:32:25 [SRX5308] [IKE] IKE configuration with identifier "pol1" deleted successfully_ 2000 Jan 1 04:32:25 [SRX5308] [IKE] Could not find configuration for 20.0.0.1[500]_

Table 123. System logs: IPSec VPN tunnel, SA lifetime (150 sec in phase 1; 300 sec in phase 2), VPN tunnel is reestablished (continued)

Explanation	Message 1: Informational exchange for deleting the payload. Message 2–6: Phase 2 configuration is purged and confirms that no phase 2 is bounded. Message 7: Informational exchange for deleting the payload. Message 8–11: Phase 1 configuration. The VPN tunnel is reestablished.
Recommended action	None

Table 124. System logs: IPSec VPN tunnel, SA lifetime (150 sec in phase 1; 300 sec in phase 2), VPN tunnel not reestablished

Message	2000 Jan 1 04:52:33 [SRX5308] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_ 2000 Jan 1 04:52:33 [SRX5308] [IKE] Configuration found for 20.0.0.1._ 2000 Jan 1 04:52:59 [SRX5308] [IKE] Phase 1 negotiation failed due to time up for 20.0.0.1[500]. b73efd188399b7f2:0000000000000000_ 2000 Jan 1 04:53:04 [SRX5308] [IKE] Phase 2 negotiation failed due to time up waiting for phase 1. ESP 20.0.0.1->20.0.0.2 _ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Configuration found for 20.0.0.1._ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Initiating new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Beginning Identity Protection mode._ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Setting DPD Vendor ID_ 2000 Jan 1 04:53:36 [SRX5308] [IKE] Phase 2 negotiation failed due to time up waiting for phase 1. ESP 20.0.0.1->20.0.0.2 _
Explanation	Phase 1 and phase 2 negotiations failed because of a mismatch of the WAN IP address in the IPSec VPN policy and the WAN IP address of the remote host attempting to establish the IPSec VPN tunnel.
Recommended action	None

Table 125. System logs: IPSec VPN tunnel, Dead Peer Detection and keep-alive (default 30 sec)

Messages 1 through 4	2000 Jan 1 04:13:39 [SRX5308] [IKE] Received request for new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Beginning Identity Protection mode._
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: RFC XXXX_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: DPD_
Message 5	2000 Jan 1 04:13:39 [SRX5308] [IKE] DPD is Enabled_
Message 6	2000 Jan 1 04:13:39 [SRX5308] [IKE] For 20.0.0.1[500], Selected NAT-T version: RFC XXXX_
Message 7	2000 Jan 1 04:13:39 [SRX5308] [IKE] Setting DPD Vendor ID_

Table 125. System logs: IPSec VPN tunnel, Dead Peer Detection and keep-alive (default 30 sec) (continued)

Explanation	Message 1–4: After receiving a request for phase 1 negotiation, a Dead Peer Detection Vendor ID is received. Message 5: DPD is enabled. Message 7: The DPD vendor ID is set.
Recommended action	None

Table 126. System logs: IPSec VPN tunnel, Dead Peer Detection and keep-alive (default 30 sec), VPN tunnel torn down

Message 1 Message 2 Message 3	2000 Jan 1 06:01:18 [SRX5308] [VPNKA] Keep alive to peer 192.168.10.2 failed 3 consecutive times and 5 times cumulative_ 2000 Jan 1 06:01:19 [SRX5308] [IKE] DPD R-U-THERE sent to "20.0.0.1[500]"_ 2000 Jan 1 06:01:19 [SRX5308] [IKE] DPD R-U-THERE-ACK received from "20.0.0.1[500]"_
Explanation	Message 1: When the remote host connection is removed and when there are no packets from the remote host, the VPN firewall sends packets to keep the remote host alive. As the connection itself is removed, keep-alive fails. Message 2: The VPN firewall sends packets to check whether the peer is dead. Message 3: The VPN firewall receives an acknowledgment that the peer is dead. The connection is removed.
Recommended action	None

Table 127. System logs: IPSec VPN tunnel, client policy, disconnection from the client side

Message	2000 Jan 1 02:34:45 [SRX5308] [IKE] Deleting generated policy for 20.0.0.1[0]_ 2000 Jan 1 02:34:45 [SRX5308] [IKE] an undead schedule has been deleted: 'pk_recvupdate'._ 2000 Jan 1 02:34:45 [SRX5308] [IKE] Purged IPSec-SA with proto_id=ESP and spi=3000608295(0xb2d9a627)._ 2000 Jan 1 02:34:45 [SRX5308] [IKE] Purged IPSec-SA with proto_id=ESP and spi=248146076(0xeca689c)._ 2000 Jan 1 02:34:45 [SRX5308] [IKE] Purged ISAKMP-SA with proto_id=ISAKMP and spi=da1f2efbf0635943:4eb6fae677b2e4f4._ 2000 Jan 1 02:34:46 [SRX5308] [IKE] ISAKMP-SA deleted for 20.0.0.2[500]-20.0.0.1[500] with spi:da1f2efbf0635943:4eb6fae677b2e4f4_
Explanation	Phase 2 and phase 1 policies are deleted when the client is disconnected.
Recommended action	None

Table 128. System logs: IPSec VPN tunnel, client policy behind a NAT device

Message 3 Message 6	2000 Jan 1 01:54:21 [SRX5308] [IKE] Floating ports for NAT-T with peer 20.0.0.1[4500]_ 2000 Jan 1 01:54:21 [SRX5308] [IKE] NAT-D payload matches for 20.0.0.2[4500]_ 2000 Jan 1 01:54:21 [SRX5308] [IKE] NAT-D payload does not match for 20.0.0.1[4500]_ 2000 Jan 1 01:54:21 [SRX5308] [IKE] Ignore REPLAY-STATUS notification from 20.0.0.1[4500]._ 2000 Jan 1 01:54:21 [SRX5308] [IKE] Ignore INITIAL-CONTACT notification from 20.0.0.1[4500] because it is only accepted after phase 1._ 2000 Jan 1 01:54:21 [SRX5308] [IKE] NAT detected: Peer is behind a NAT device_
Explanation	These logs are generated when the remote WAN host is connected through a device such as the VPN firewall. NAT is detected before phase 1 is established. Message 3: NAT-D does not match the remote host. Message 6: The VPN firewall confirms that the remote host or the peer is behind a NAT device.
Recommended action	None

SSL VPN Logs

This section describes the log messages that are generated by SSL VPN policies.

Table 129. System logs: SSL VPN tunnel, WAN host and interface

Message	2000 Jan 1 03:44:55 [SRX5308] [sslvpntunnel] id=SRX5308 time="2000-1-1 3:44:55" fw=20.0.0.2 pri=6 rule=access-policy proto= "SSL VPN Tunnel" src=20.0.0.1 user=sai dst=20.0.0.2 arg="" op="" result="" rcvd= "" msg="SSL VPN Tunnel"
Explanation	An SSL VPN tunnel is established for ID SRX5308 with the WAN host 20.0.0.1 through WAN interface 20.0.0.2 and logged in with the user name “sai.”
Recommended action	None

Table 130. System logs: VPN log messages, port forwarding, WAN host and interface

Message	2000 Jan 1 01:30:08 [SRX5308] [portforwarding] id=SRX5308 time="2000-1-1 1:30: 8" fw=20.0.0.2 pri=6 rule=access-policy proto= "Port Forwarding" src=20.0.0.1 user=sai dst=20.0.0.2 arg="" op="" result="" rcvd="" msg="Port Forwarding"
Explanation	An SSL VPN tunnel through port forwarding is established for ID SRX5308 with the WAN host 20.0.0.1 through WAN interface 20.0.0.2 and logged in with the user name “sai.”
Recommended action	None

Table 131. System logs: VPN log messages, port forwarding, LAN host and interface

Message	2000 Jan 1 01:35:41 [SRX5308] [portforwarding] id=SRX5308 time="2000-1-1 1:35:41" fw=192.168.11.1 pri=6 rule=access-policy proto="Virtual Transport (Java)" src=192.168.11.2 user=sai dst=192.168.11.1 arg="" op="" result="" rcvd="" msg="Virtual Transport (Java)"
Explanation	An SSL VPN tunnel through port forwarding is established for ID SRX5308 from the LAN host 192.168.11.2 with interface 192.168.11.1 and logged in with the user name “sai.”
Recommended action	None

Traffic Meter Logs

Table 132. System logs: traffic meter

Message	Jan 23 19:03:44 [TRAFFIC_METER] TRAFFIC_METER: Monthly Limit of 10 MB has reached for WAN1._
Explanation	Traffic limit to WAN1 that was set as 10 Mb has been reached. This stops all the incoming and outgoing traffic, that is, if you selected the **Block All Traffic** radio button in the When Limit is Reached section on the WAN TrafficMeter screen.
Recommended action	To start the traffic, restart the traffic limit counter.

Routing Logs

- *LAN to WAN Logs*
- *LAN to DMZ Logs*
- *DMZ to WAN Logs*
- *WAN to LAN Logs*
- *DMZ to LAN Logs*
- *WAN to DMZ Logs*

This section explains the logging messages for the various network segments (such as LAN to WAN) for debugging purposes. These logs might generate a significant volume of messages.

LAN to WAN Logs

Table 133. Routing logs: LAN to WAN

Message	Nov 29 09:19:43 [SRX5308] [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 LAN to WAN has been allowed by the firewall. • For other settings, see *Table 106* on page 431.
Recommended action	None

LAN to DMZ Logs

Table 134. Routing logs: LAN to DMZ

Message	Nov 29 09:44:06 [SRX5308] [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 LAN to DMZ has been allowed by the firewall. • For other settings, see *Table 106* on page 431.
Recommended action	None

DMZ to WAN Logs

Table 135. Routing logs: DMZ to WAN

Message	Nov 29 09:19:43 [SRX5308] [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 DMZ to WAN has been dropped by the firewall. • For other settings, see *Table 106* on page 431.
Recommended action	None

WAN to LAN Logs

Table 136. Routing logs: WAN to LAN

Message	Nov 29 10:05:15 [SRX5308] [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 LAN to WAN has been allowed by the firewall. • For other settings, see *Table 106* on page 431.
Recommended action	None

DMZ to LAN Logs

Table 137. Routing logs: DMZ to WAN

Message	Nov 29 09:44:06 [SRX5308] [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 DMZ to LAN has been dropped by the firewall. • For other settings, see *Table 106* on page 431.
Recommended action	None

WAN to DMZ Logs

Table 138. Routing logs: WAN to DMZ

Message	Nov 29 09:19:43 [SRX5308] [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 WAN to DMZ has been allowed by the firewall. • For other settings, see *Table 106* on page 431.
Recommended action	None

Other Event Logs

- *Session Limit Logs*
- *Source MAC Filter Logs*
- *Bandwidth Limit Logs*

This section describes the log messages generated by other events such source MAC filtering, session limiting, and bandwidth limiting. For information about how to select these logs, see *Configure Logging, Alerts, and Event Notifications* on page 362.

Session Limit Logs

Table 139. Other event logs: session limit logs

Message	2000 Jan 1 06:53:33 [SRX5308] [kernel] SESS_LIMIT[DROP] IN=LAN OUT=WAN SRC=192.168.11.2 DST=20.0.0.1 PROTO=TCP SPT=50709 DPT=21
Explanation	When two FTP sessions are established from the same LAN host at IP address 192.168.11.2 and a session limit (SESS_LIMIT) is set as 1, the FTP packets from the second session are dropped.
Recommended action	Change the session limit to 2 to prevent packets from being dropped.

Source MAC Filter Logs

Table 140. Other event logs: source MAC filter logs

Message	2000 Jan 1 06:40:10 [SRX5308] [kernel] SRC_MAC_MATCH[DROP] SRC MAC = 00:12:3f:34:41:14 IN=LAN OUT=WAN SRC=192.168.11.3 DST=209.85.153.103 PROTO=ICMP TYPE=8 CODE=0
Explanation	Because MAC address 00:12:3f:34:41:14 of LAN host with IP address 192.168.11.3 is filtered so that it cannot access the Internet, the packets sent by this MAC address to the Google server at address 09.85.153.103 are dropped.
Recommended action	Disable source MAC filtering.

Bandwidth Limit Logs

Table 141. Other event logs: bandwidth limit, outbound bandwidth profile

Message	2000 Jan 1 00:10:36 [SRX5308] [kernel] [BW_LIMIT_DROP] IN=LAN OUT=WAN SRC=192.168.100.2 DST=22.0.0.2 PROTO=ICMP TYPE=144 CODE=145 TC_INDEX=10 CLASSID=10:5
Explanation	This log is generated when an outbound packet is dropped because the packet size exceeds the specified bandwidth limit.
Recommended action	Ensure that the packet size is within the specified bandwidth limit.

Table 142. Other event logs: bandwidth limit, inbound bandwidth profile

Message	2000 Jan 1 00:08:21 [SRX5308] [kernel] [BW_LIMIT_DROP] IN=LAN OUT=WAN SRC=22.0.0.2 DST=192.168.100.2 PROTO=ICMP TYPE=112 CODE=113 TC_INDEX=10 CLASSID=10:2
Explanation	This log is generated when an inbound packet is dropped because the packet size exceeds the specified bandwidth limit.
Recommended action	Ensure that the packet size is within the specified bandwidth limit.

DHCP Logs

This section explains the log messages that are generated when a host is assigned a dynamic IP address. These messages are displayed on the DHCP Log screen (see *View the DHCP Log* on page 387).

Table 143. DHCP logs

Message 1 Message 2 Message 3 Message 4 Message 5 Message 6 Message 7	2000 Jan 1 07:27:28 [SRX5308] [dhcpd] Listening on LPF/eth0.1/00:11:22:78:89:90/192.168.11/24 2000 Jan 1 07:27:37 [SRX5308] [dhcpd] DHCPRELEASE of 192.168.10.2 from 00:0f:1f:8f:7c:4a via eth0.1 (not found) 2000 Jan 1 07:27:47 [SRX5308] [dhcpd] DHCPDISCOVER from 00:0f:1f:8f:7c:4a via eth0.1 2000 Jan 1 07:27:48 [SRX5308] [dhcpd] DHCPOFFER on 192.168.11.2 to 00:0f:1f:8f:7c:4a via eth0.1 2000 Jan 1 07:27:48 [SRX5308] [dhcpd] Wrote 2 leases to leases file. 2000 Jan 1 07:27:48 [SRX5308] [dhcpd] DHCPREQUEST for 192.168.11.2 (192.168.11.1) from 00:0f:1f:8f:7c:4a via eth0.1 2000 Jan 1 07:27:48 [SRX5308] [dhcpd] DHCPACK on 192.168.11.2 to 00:0f:1f:8f:7c:4a via eth0.1
Explanation	Message 1: The DHCP server is listening on eth0.1. Message 2: Release of the currently assigned IP address from the host by the DHCP server. Message 3: DHCP broadcast by the host is discovered by the DHCP server. Message 4: The DHCP server offers a new IP address to the host's current network interface. Message 5: Two new leases are written to the lease file. Message 6: DHCP is requested to assign the new IP address by the host. Message 7: DHCP acknowledgment to the current network interface from the server on assignment of the new IP address.
Recommended action	None

Two-Factor Authentication

D

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?*
- *NETGEAR Two-Factor Authentication Solutions*

Why Do I Need Two-Factor Authentication?

In today's market, online identity theft and online fraud continue to be one of the fast-growing cybercrime activities used by many unethical hackers and cybercriminals to steal digital assets for financial gains. Many companies and corporations are losing millions of dollars and running into risks of revealing their trade secrets and other proprietary information as a result of these cybercrime activities. Security threats and hackers have become more sophisticated, and user names, encrypted passwords, and the presence of firewalls are no longer enough to protect the networks from being compromised. IT professionals and security experts have recognized the need to go beyond the traditional authentication process by introducing and requiring additional factors in the authentication process. NETGEAR has also recognized the need to provide more than just a firewall to protect the networks. NETGEAR has implemented a more robust authentication system known as two-factor authentication (2FA or T-FA) to help address the fast-growing network security issues.

What Are the Benefits of Two-Factor Authentication?

- **Stronger security**. Passwords cannot efficiently protect the corporate networks because attackers can easily guess simple passwords or users cannot remember complex and unique passwords. One-time passcode (OTP) strengthens and replaces the need to remember complex password.
- **No need to replace existing hardware**. Two-factor authentication can be added to existing NETGEAR products through a firmware upgrade.
- **Quick to deploy and manage**. The WiKID solution integrates seamlessly with the NETGEAR SSL and VPN firewall products.
- **Proven regulatory compliance**. Two-factor authentication has been used as a mandatory authentication process for many corporations and enterprises worldwide.

What Is Two-Factor Authentication?

Two-factor authentication is a security solution that enhances and strengthens security by implementing multiple factors of the authentication process that challenge and confirm the users' identities before they can gain access to the network. There are several factors that are used to validate the users to make sure that you are who you say you are. These factors are:

- Something you know—for example, your password or your PIN.
- Something you have—for example, a token with generated passcode that is 6 to 8 digits in length.
- Something you are—for example, biometrics such as fingerprints or retinal prints.

This appendix focuses on and discusses only the first two factors, something you know and something you have. This security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you have. A common example of two-factor authentication is a bank (ATM) card that has been issued by a bank institute:

- The PIN to access your account is *something you know.*
- The ATM card is *something you have.*

You need to have both of these factors to gain access to your bank account. Similar to the way ATM cards work, access to the corporate networks and data can also be strengthened using a combination of multiple factors such as a PIN and a token (hardware or software) to validate the users and reduce the incidence of online identity theft.

NETGEAR Two-Factor Authentication Solutions

NETGEAR has implemented 2 two-factor authentication solutions from WiKID. WiKID is the software-based token solution. So instead of using only Windows Active Directory or LDAP as the authentication server, administrators now can use WiKID to perform two-factor authentication on NETGEAR SSL and VPN firewall products.

The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), which is time-synchronized with the authentication server, is generated and sent to the user after the validity of a user credential has been confirmed by the server.

The request-response architecture is capable of self-service initialization by end users, dramatically reducing implementation and maintenance costs.

Here is an example of how WiKID works:

➢ **To use WiKID (for end users):**

1. Launch the WiKID token software, enter the PIN that has been provided (*something the user know*s), and click **Continue** to receive the OTP from the WiKID authentication server:

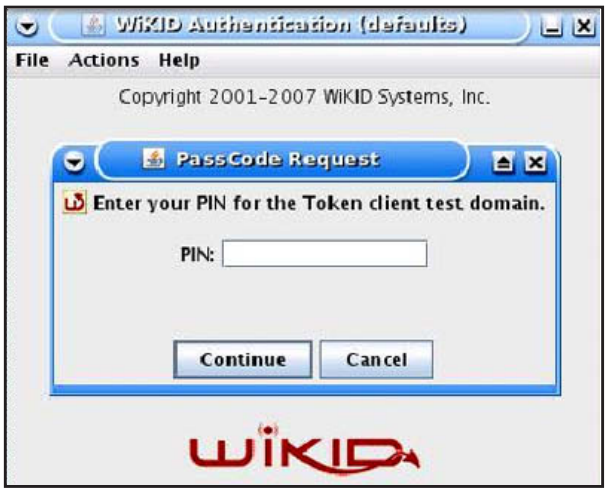

Figure 282.

2. A one-time passcode (*something the user has*) is generated.

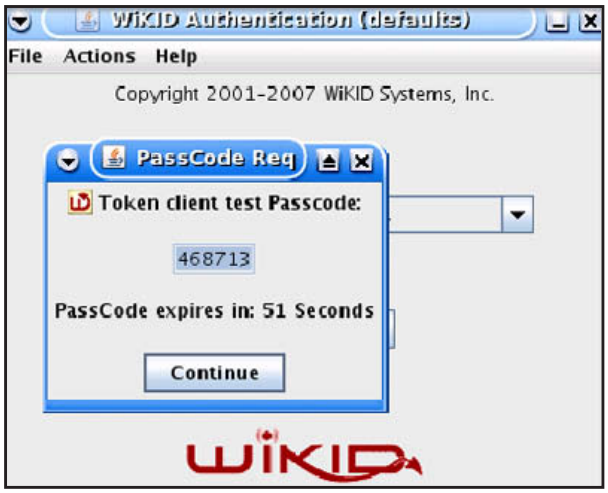

Figure 283.

Note: The one-time passcode is time-synchronized to the authentication server so that the OTP can be used only once and needs to be used before the expiration time. If a user does not use this passcode before it expires, the user needs to go through the request process again to generate a new OTP.

3. Proceed to the 2 Factor Authentication login screen, and enter the one-time passcode as the login password.

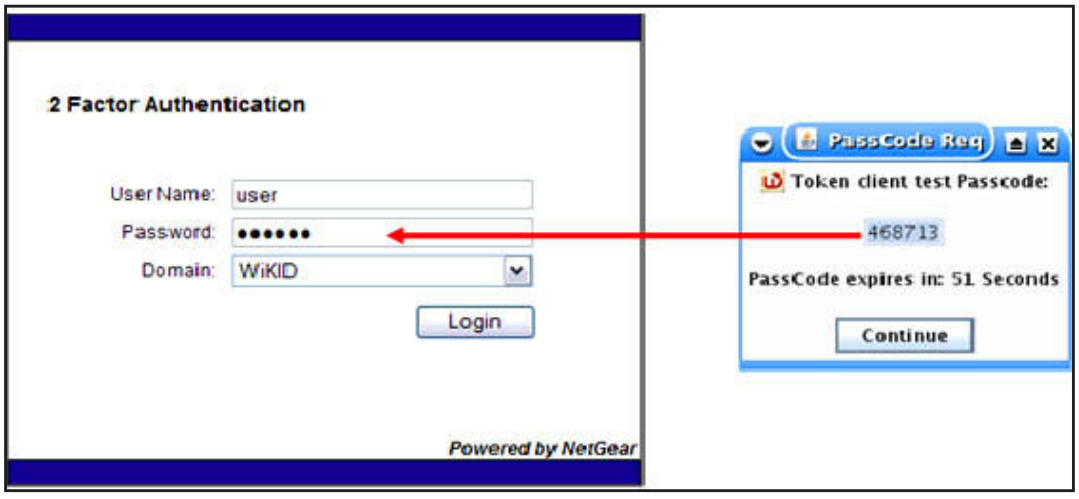

Figure 284.

Notification of Compliance

E

NETGEAR wired products

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Products bearing the CE marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSAFE Gigabit Quad WAN SSL VPN Firewall SRX5308 complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Index

Numerics

A

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X