NETGEAR®

ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N

Reference Manual

April 2013
202-10836-05

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
202-10836-05	–	April 2013	Added the following features: • SNMP access from the WAN and SNMP trap events (see *Use a Simple Network Management Protocol Manager*) • Option to define what constitutes a UDP flood attack (see *Attack Checks*) • Authentication for the L2TP server (see *Configure the L2TP Server*) • Wireless logs (see *Configure Logging, Alerts, and Event Notifications*) • 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*)
202-10836-04	1.0	July, 2012	Added the following features: • Stateless IP/ICMP Translation (see *Configure Stateless IP/ICMP Translation*) • Option to turn bandwidth profiles on and off (see *Create Bandwidth Profiles*) • Support for SNMPv3 (see *Use a Simple Network Management Protocol Manager*) The following screens provide new information: • LAN WAN Rules screen (see *Configure LAN WAN Rules*) • Router Status screen (see *Router Status Screen*) • Detailed Status screen (see *Detailed Status Screen*)
202-10836-03	1.0	April, 2012	Added the PPPoE IPv6 feature (see *Configure a PPPoE IPv6 Internet Connection*)

202-10836-02	1.0	March, 2012	Added the following menus and features: • New and improved general menu structure with IPv4 and IPv6 radio buttons • New LAN IPv6 configuration menu with the LAN Setup (IPv6) screen (see *Manage the IPv6 LAN*) and a new screen, the LAN Multi-homing (IPv6) screen (see *Configure IPv6 Multihome LAN IP Addresses on the Default VLAN*) • IPv6 DMZ (*Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic*) • IPv6 firewall rules (see *Configure LAN WAN Rules*, *Configure DMZ WAN Rules*, *Configure LAN DMZ Rules*, and *Examples of Firewall Rules*) • IPv6 attack checks (see *Attack Checks*) • IPv6/MAC bindings (see *Set Up IP/MAC Bindings*) • Simplified wireless settings submenus for easier configuration (see *Chapter 4, Wireless Configuration and Security*) • IPSec VPN IPv6 address support (see *Chapter 6, Virtual Private Networking Using IPSec and L2TP Connections*) • IPSec VPN autoinitiate support (see *Manually Add or Edit a VPN Policy*) • SSL VPN IPv6 address support (see *Chapter 7, Virtual Private Networking Using SSL Connections*) • User login restrictions based on IPv6 addresses (see *Configure Login Restrictions Based on IPv6 Addresses*) • IPv6 remote management access (see *Configure Remote Management Access*) • IPv6 address resolution for NTP servers (see *Configure Date and Time Service*) • IPv6 diagnostics (see *Diagnostics Utilities*) • Extensive list of factory default settings (see *Appendix A, Default Settings and Technical Specifications*)
202-10836-01	1.0	September 2011	First publication

Contents

Chapter 1 Introduction

Chapter 2 IPv4 and IPv6 Internet and Broadband Settings

Chapter 3 LAN Configuration

Chapter 4 Wireless Configuration and Security

Chapter 5 Firewall Protection

Chapter 6 Virtual Private Networking Using IPSec and L2TP Connections

Chapter 9 Network and System Management

Chapter 10 Monitor System Access and Performance

Chapter 11 Troubleshooting

Appendix A Default Settings and Technical Specifications

Appendix B Two-Factor Authentication

Appendix C Notification of Compliance (Wired)

Appendix D Notification of Compliance (Wireless)

Index

Introduction

1

This chapter provides an overview of the features and capabilities of the ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N 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 Wireless-N 8-Port Gigabit VPN Firewall FVS318N?

The ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N, hereafter referred to as the wireless VPN firewall, connects your local area network (LAN) and wireless LAN (WLAN) to the Internet through an external broadband access device such as a cable or DSL modem, satellite or wireless Internet dish, or another router. A 2.4-GHz radio supports wireless connections in 802.11n mode with support for legacy clients in 802.11b and 802.11g mode.

The wireless 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 wireless VPN firewall provides advanced IPSec and SSL VPN technologies with support for up to 12 IPSec VPN tunnels and 5 SSL VPN tunnels, as well as L2TP support for easy and secure remote connections. The use of Gigabit Ethernet WAN and LAN ports ensures high data transfer speeds.

Key Features and Capabilities

The wireless VPN firewall provides the following key features and capabilities:

- A single 10/100/1000 Mbps Gigabit Ethernet WAN port
- Built-in eight-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for fast data transfer between local network resources
- A wireless radio with up to four wireless profiles
- Both IPv4 and IPv6 support
- Advanced IPSec VPN and SSL VPN support
- L2TP tunnel support
- Advanced stateful packet inspection (SPI) firewall with multi-NAT support
- 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

Wireless Features

The wireless VPN firewall supports the following features:

- **2.4 GHz radio**. 2.4-GHz band support with 802.11b/g/n wireless modes.
- **Wireless profiles**. Support for up to four wireless profiles, each with its own SSID.
- **Access control**. The Media Access Control (MAC) address filtering feature can ensure that only trusted wireless stations can use the wireless VPN firewall to gain access to your LAN.
- **Hidden mode**. The SSID is not broadcast, assuring that only clients configured with the correct SSID can connect.
- **Secure and economical operation**. Adjustable power output allows more secure or economical operation.

Advanced VPN Support for Both IPSec and SSL

The wireless 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 12 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 five simultaneous SSL VPN connections.
  - Allows browser-based, platform-independent remote access through a number of browsers, such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.
  - Provides granular access to corporate resources based on user type or group membership.

A Powerful, True Firewall

Unlike simple NAT routers, the wireless 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.
- **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.

Security Features

The wireless 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 wireless 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 wireless 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 eight-port 10/100/1000 Mbps switch and 10/100/1000 WAN port, the wireless VPN firewall can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit Ethernet network. The LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

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

- **IP address sharing by NAT**. The wireless 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 wireless 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 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 wireless VPN firewall supports QoS.
- **Layer 2 Tunneling Protocol (L2TP)**. A tunneling protocol that is used to support virtual private networks (VPNs).

Easy Installation and Management

You can install, configure, and operate the wireless 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 wireless 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 wireless 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 wireless 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 wireless 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 wireless VPN firewall incorporates built-in diagnostic functions such as ping, traceroute, DNS lookup, and remote reboot.
- **Remote management**. The wireless 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 wireless 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 wireless 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 wireless VPN firewall product package contains the following items:

- ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N
- One 12V 1A power supply unit for your region
- Rubber feet
- Ethernet cable
- *ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N Installation Guide*
- *Resource CD*, including:
  - Application Notes and other helpful information
  - 30-day trial license for the 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 wireless VPN firewall are described in the following sections.

Front Panel

Viewed from left to right, the wireless VPN firewall front panel contains the following ports:

- LAN Ethernet ports. Eight switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.
- WAN Ethernet port. One independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet port with an RJ-45 connector.

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 detail in the following table. Some LED explanation is provided on the front panel.

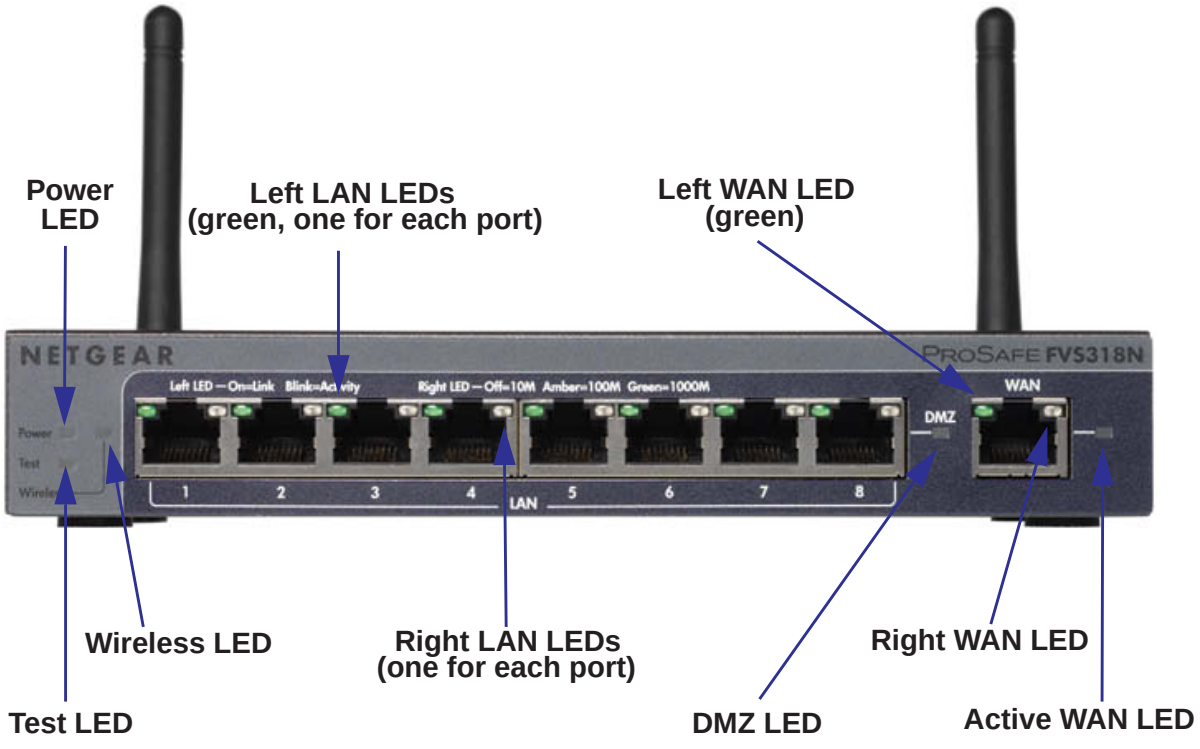

Figure 1.

The following table describes the function of each LED.

Table 1. LED descriptions

LED	Activity	Description
Power LED	On (green)	Power is supplied to the wireless VPN firewall.
	Off	Power is not supplied to the wireless VPN firewall.
Test LED	On (amber) during startup.	Test mode. The wireless VPN firewall is initializing. After approximately two minutes, when the wireless 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 wireless VPN firewall is writing to flash memory (during upgrading or resetting to defaults).
	Off	The wireless VPN firewall has booted successfully.
LAN Ports		
Left LED	Off	The LAN port has no link.
	On (green)	The LAN port has detected a link with a connected Ethernet device.
	Blinking (green)	Data is being transmitted or received by the LAN port.
Right LED	Off	The LAN port is operating at 10 Mbps.
	On (amber)	The LAN port is operating at 100 Mbps.
	On (green)	The LAN port is operating at 1000 Mbps.
DMZ LED	Off	Port 8 is operating as a normal LAN port.
	On (green)	Port 8 is operating as a dedicated hardware DMZ port.
WAN Port		
Left LED	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the wireless VPN firewall.
	On (green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blinking (green)	Data is being transmitted or received by the WAN port.
Right LED	Off	The WAN port is operating at 10 Mbps.
	On (amber)	The WAN port is operating at 100 Mbps.
	On (green)	The WAN port is operating at 1000 Mbps.
Active LED	Off	There is no link to the Internet.
	On (green)	There is a link to the Internet.

Rear Panel

The rear panel of the wireless VPN firewall includes the antennas, a cable lock receptacle, a console port, a Reset button, a DC power connection, and a power switch.

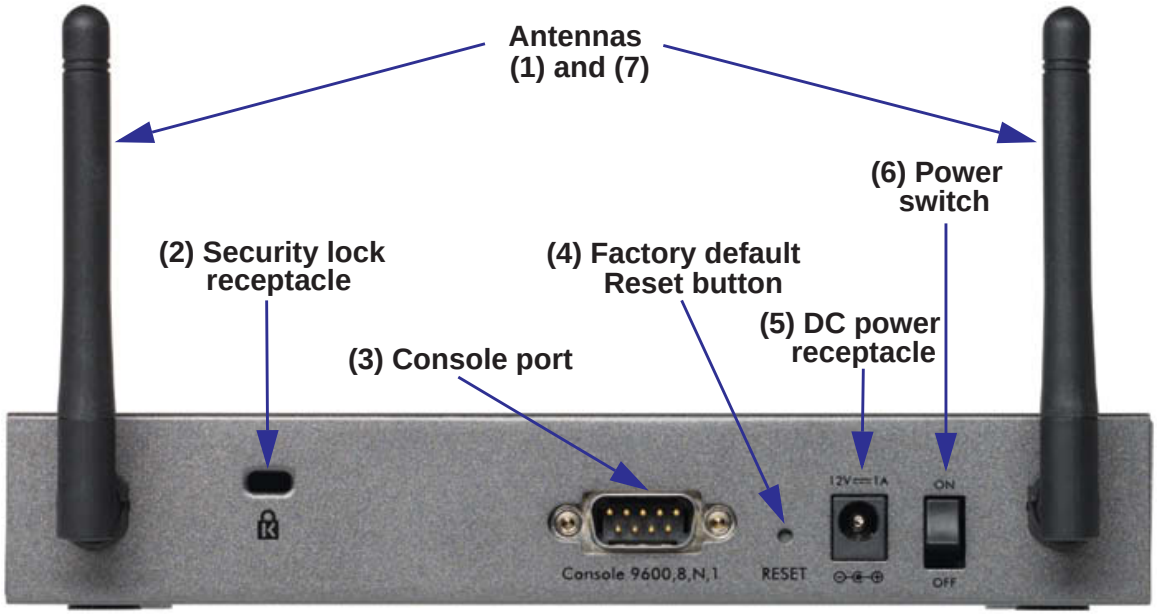

Figure 2.

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

1. Dipole antenna.
2. Cable security lock receptacle.
3. Console port. Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd.
4. Factory default Reset button. Using a sharp object, press and hold this button for about eight seconds until the front panel Test LED flashes to reset the wireless VPN firewall to factory default settings. All configuration settings are lost, and the default password is restored.
5. DC power plug receptacle. Power input is 12VDC, 1A. The power plug is localized to the country of sale.
6. Power On/Off switch.
7. Dipole antenna.

Bottom Panel with Product Label

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

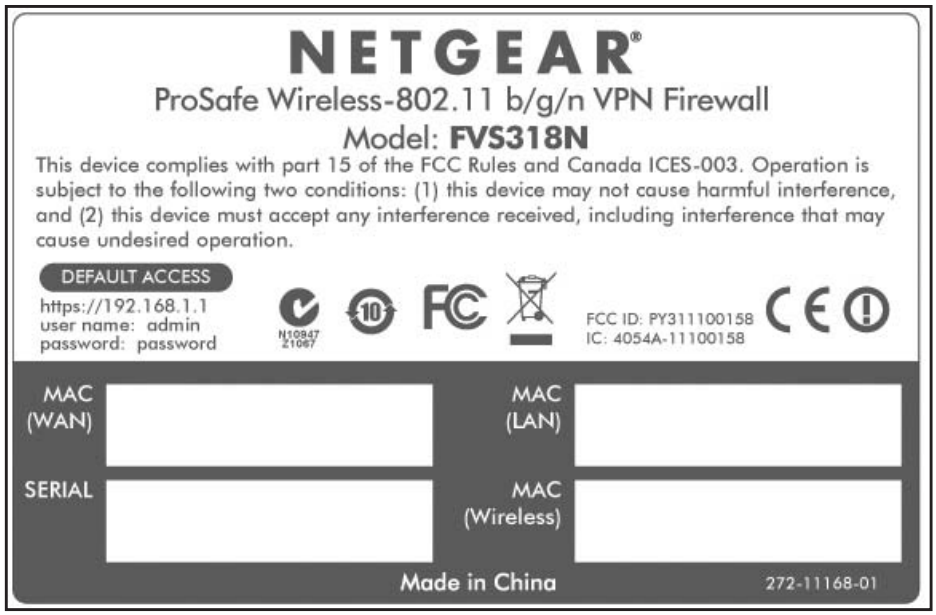

Figure 3.

Choose a Location for the Wireless VPN Firewall

The wireless 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 wireless VPN firewall in a wiring closet or equipment room.

Consider the following when deciding where to position the wireless 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 one 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 wireless VPN firewall, see *Appendix A, Default Settings and Technical Specifications*.

Log In to the Wireless VPN Firewall

Note: To connect the wireless VPN firewall physically to your network, connect the cables and restart your network according to the instructions in the *ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N Installation Guide*. A PDF of this guide is on the NETGEAR support website at *http://support.netgear.com/app/products/model/a_id/19435*.

To configure the wireless 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 wireless 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. Java is required only for the SSL VPN portal, not for the web management interface.

➢ **To log in to the wireless 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 wireless 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 wireless VPN firewall to log in to the wireless VPN firewall.

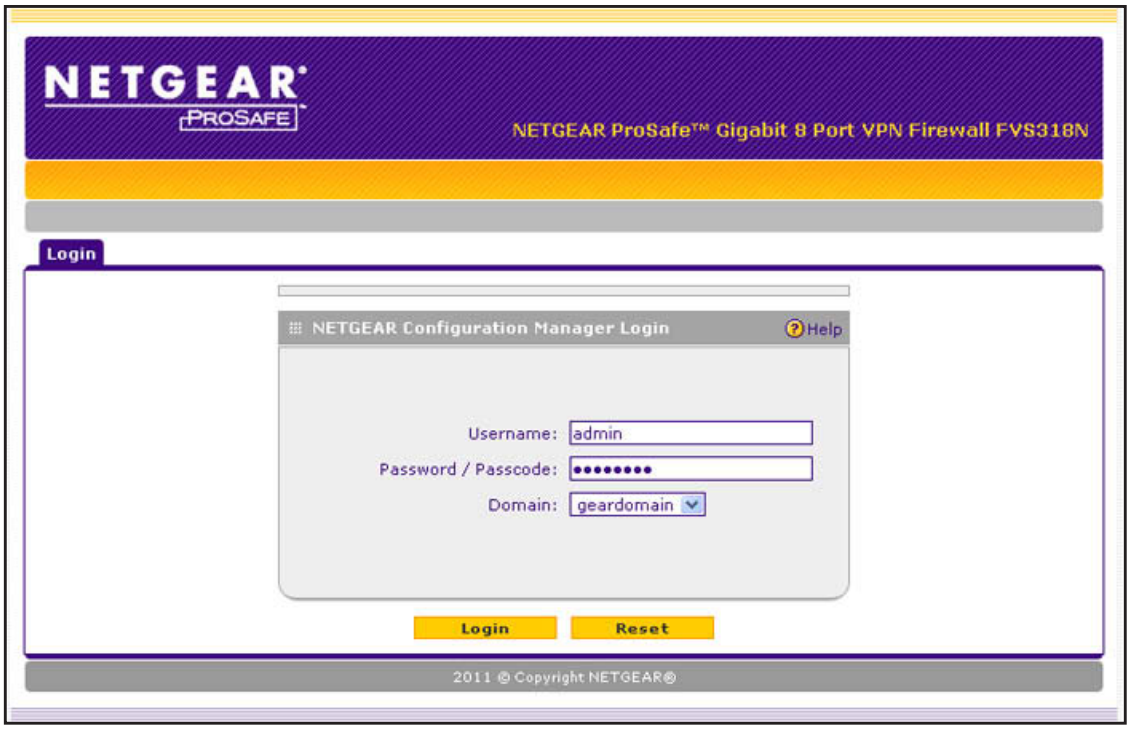

Figure 4.

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 wireless 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 359.

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

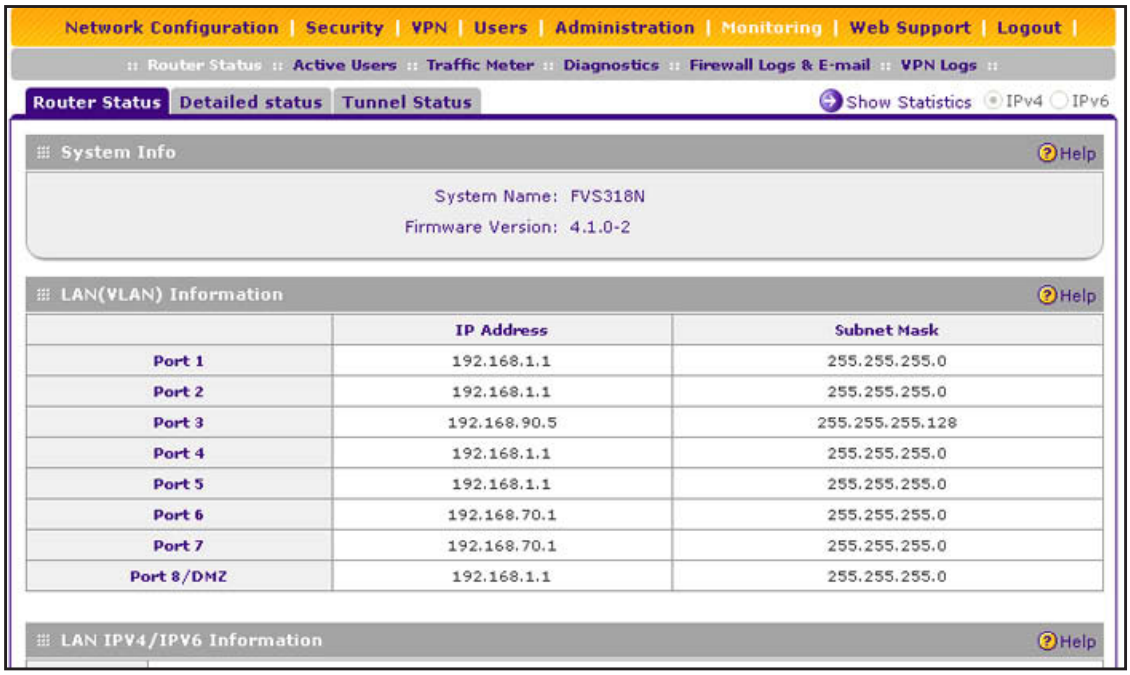

Figure 5.

Web Management Interface Menu Layout

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

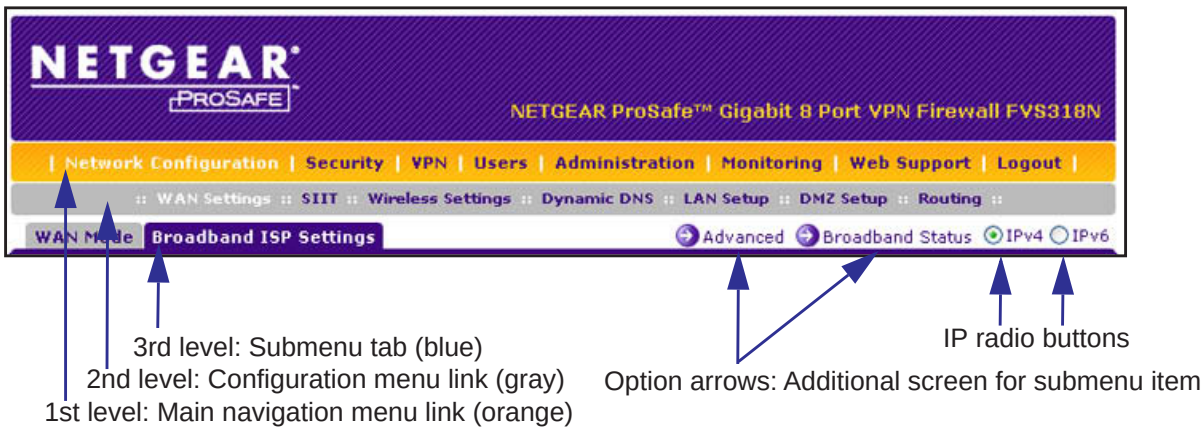

Figure 6.

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 wireless 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 7.

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 wireless 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:

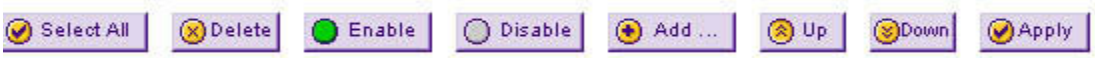

Figure 8.

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

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

Requirements for Entering IP Addresses

To connect to the wireless VPN firewall, your computer needs to be configured to obtain an IP address automatically from the wireless 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 Broadband Settings

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

Internet and WAN Configuration Tasks

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

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

Roadmap to Setting Up an IPv4 Internet Connection to Your ISP

Setting up an IPv4 Internet connection to your ISP includes five tasks, three of which are optional.

➢ **Complete these tasks:**

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

   This task is described in *Configure the IPv4 WAN Mode* on page 28.

2. **Configure the IPv4 Internet connection to your ISP**. Connect to your ISP.

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

   - *Let the Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 29
   - *Manually Configure an IPv4 Internet Connection* on page 32

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

   This task is described in *Configure Dynamic DNS* on page 36.

4. **(Optional) Configure the WAN options**. If necessary, change the factory default MTU size, port speed, and MAC address of the wireless 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 51.

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

   This task is described in *Enable the WAN Traffic Meter* on page 350.

Roadmap to Setting Up an IPv6 Internet Connection to Your ISP

Setting up an IPv6 Internet connection to your ISP includes five tasks, three of which are optional.

➢ **Complete these tasks:**

1. **Configure the IPv6 WAN mode**. Select the IPv4 / IPv6 mode to support both IPv4 and IPv6 traffic.

   This task is described in *Configure the IPv6 Routing Mode* on page 39.

2. **Configure the IPv6 Internet connection to your ISP**. Connect to your ISP.

   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 40
   - *Configure a Static IPv6 Internet Connection* on page 42
   - *Configure a PPPoE IPv6 Internet Connection* on page 44

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 47
   - *Configure ISATAP Automatic Tunneling* on page 48

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 50.

5. **(Optional) Configure the WAN options**. If necessary, change the factory default MTU size, port speed, and MAC address of the wireless 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 51.

Configure the IPv4 Internet Connection and WAN Settings

- *Configure the IPv4 WAN Mode*
- *Let the Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection*
- *Manually Configure an IPv4 Internet Connection*
- *Configure Dynamic DNS*

To set up your wireless 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 Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 29
- *Manually Configure an IPv4 Internet Connection* on page 32

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 39).

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 wireless 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 wireless 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 wireless 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 359).

Configure the IPv4 Routing Mode

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

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

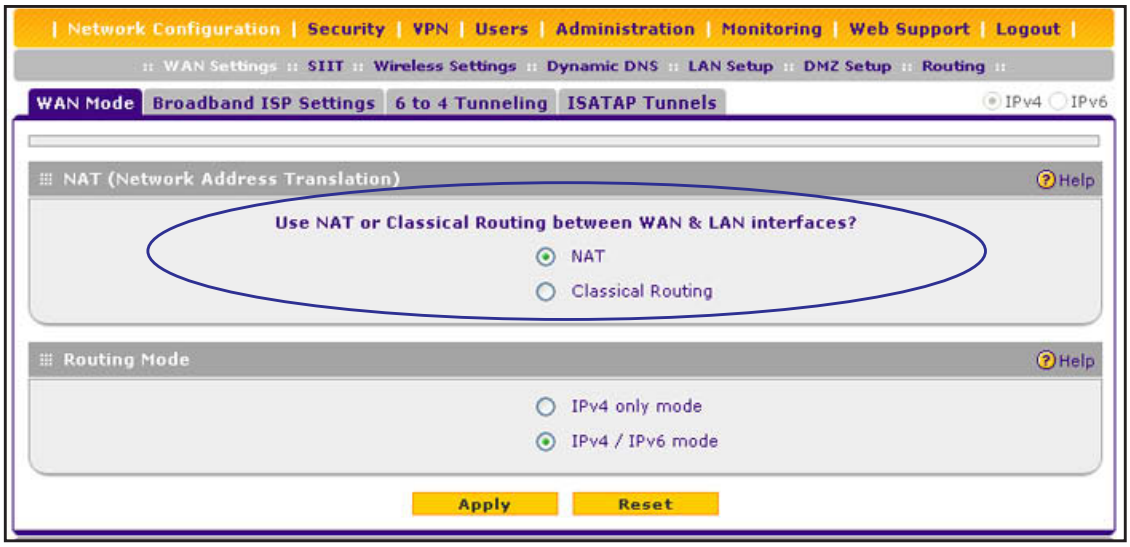

Figure 9.

2. 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.

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

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

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

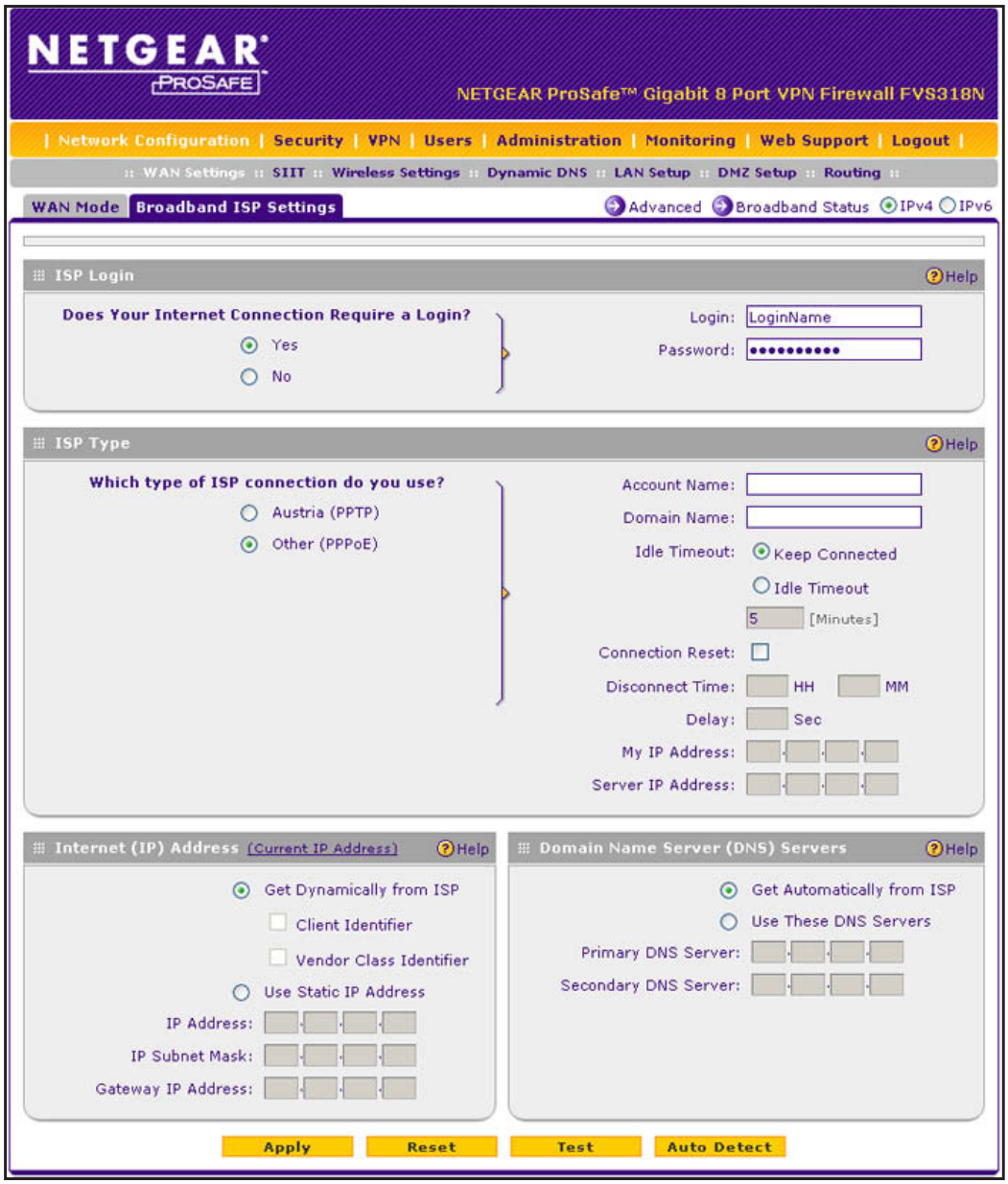

Figure 10.

2. 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 wireless VPN firewall and the cable, DSL line, or satellite or wireless Internet dish, or to check your wireless VPN firewall's MAC address. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 51 and *Troubleshoot the ISP Connection* on page 385.

3. To verify the connection, click the **Broadband Status** option arrow in the upper right of the screen to display the Connection Status pop-up screen. (The following figure shows a static IP address configuration.)

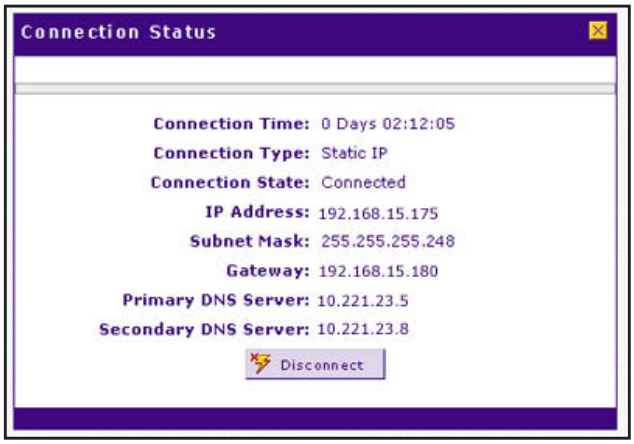

Figure 11.

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 32, or see *Troubleshoot the ISP Connection* on page 385.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 370.

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 31.

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

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings**. In the upper right of the screen, the IPv4 radio button is selected by default. The ISP Broadband Settings screen displays the IPv4 settings (see *Figure 10* on page 30).
2. Locate the ISP Login section on the screen:

Figure 12.

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.

3. 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.
4. 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:

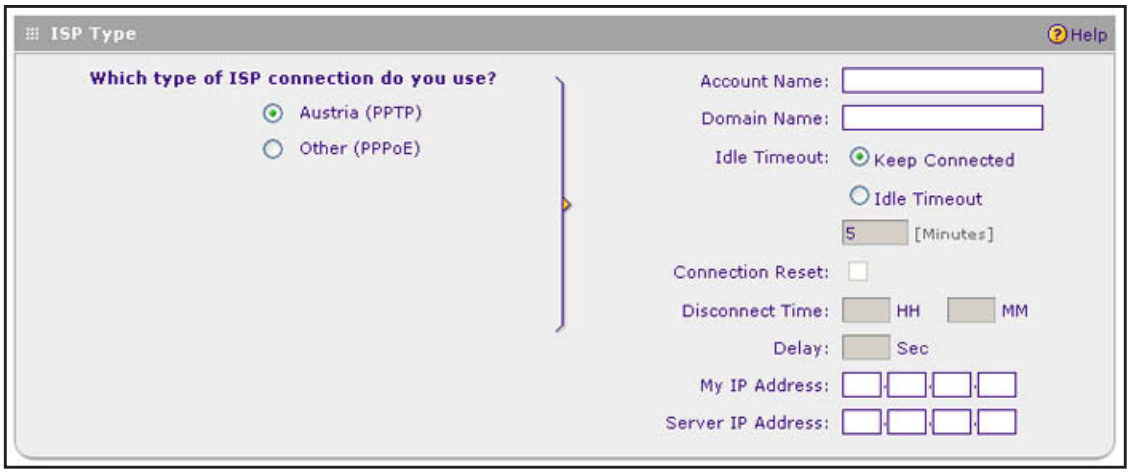

Figure 13.

5. 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 2* and *Step 3*.	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 2* and *Step 3*.	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.

6. 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.

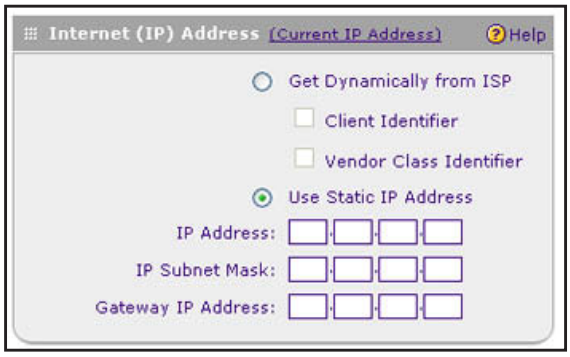

Figure 14.

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 wireless VPN firewall using DHCP network protocol.	
	Client Identifier	If your ISP requires the client identifier information to assign an IP address using DHCP, select the **Client Identifier** check box.
	Vendor Class Identifier	If your ISP requires the vendor class identifier information to assign an IP address using DHCP, select the **Vendor Class Identifier** check box.
Use Static IP Address	If your ISP has assigned you a fixed (static or permanent) IP address, select the **Use Static IP Address** radio button, and enter the following settings:	
	IP Address	The static IP address assigned to you. This address identifies the wireless 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.

7. 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.

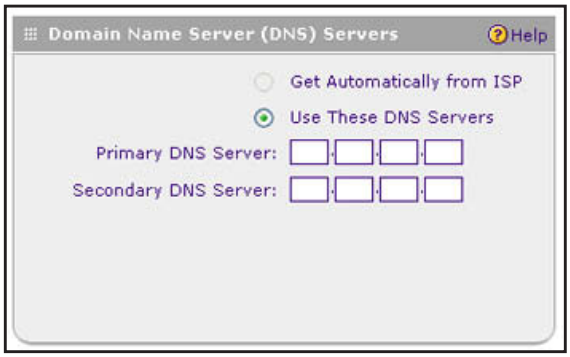

Figure 15.

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 provide 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.

8. Click **Apply** to save your changes.
9. Click **Test** to evaluate your entries. The wireless VPN firewall attempts to make a connection according to the settings that you entered.
10. To verify the connection, click the **Broadband Status** option arrow in the upper right of the screen 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.)

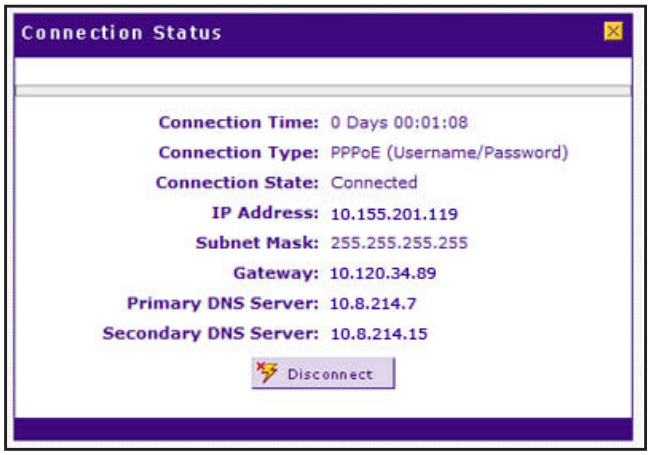

Figure 16.

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 Broadband Advanced Options screen for the WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 51).

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 wireless 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 wireless VPN firewall, when your ISP-assigned IP address changes, your wireless VPN firewall automatically contacts your DDNS service provider, logs in to your account, and registers your new 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).
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

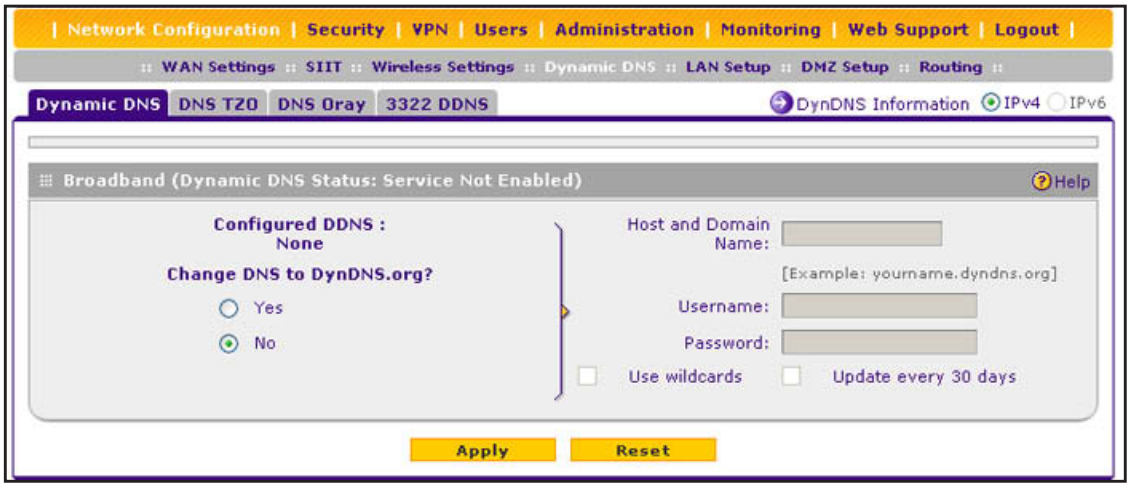

Figure 17.

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

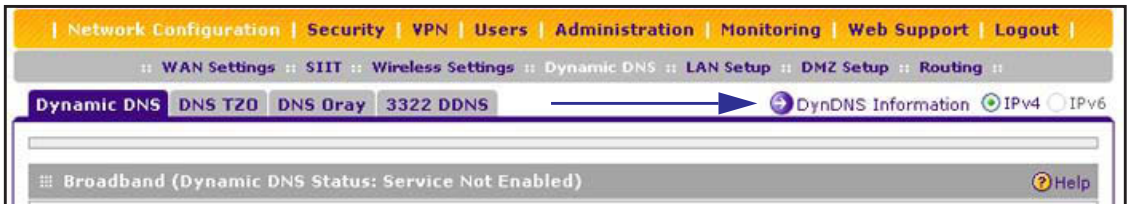

Figure 18.

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 6. DDNS service settings

Setting	Description	
Change DNS to (DynDNS, TZO, Oray, or 3322)	Select the **Yes** radio button to enable the DDNS service. The fields that display on the screen depend on the DDNS service provider that you have selected. Enter the following settings:	
	Host and Domain Name	The host and domain name for the DDNS service.
	Username or User Email Address	The user name or email address for DDNS server authentication.
	Password or User Key	The password that is used for DDNS server authentication.
	Use wildcards	If your DDNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
	Update every 30 days	If your WAN IP address does not 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.

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*

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

- **Native IPv6 network**. Your network is a native IPv6 network if the wireless 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 47).
- **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 48).

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 the WAN port with a global unicast address to enable secure IPv6 Internet connections on your wireless 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 40)
- Manual configuration of the network connection (see *Configure a Static IPv6 Internet Connection* on page 42 or *Configure a PPPoE IPv6 Internet Connection* on page 44)

Configure the IPv6 Routing Mode

By default, the wireless VPN firewall supports IPv4 only. To use IPv6, you need to enable the wireless 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 wireless VPN firewall communicates only with devices that have IPv4 addresses.
- **IPv4/IPv6 mode**. The wireless 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.

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

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

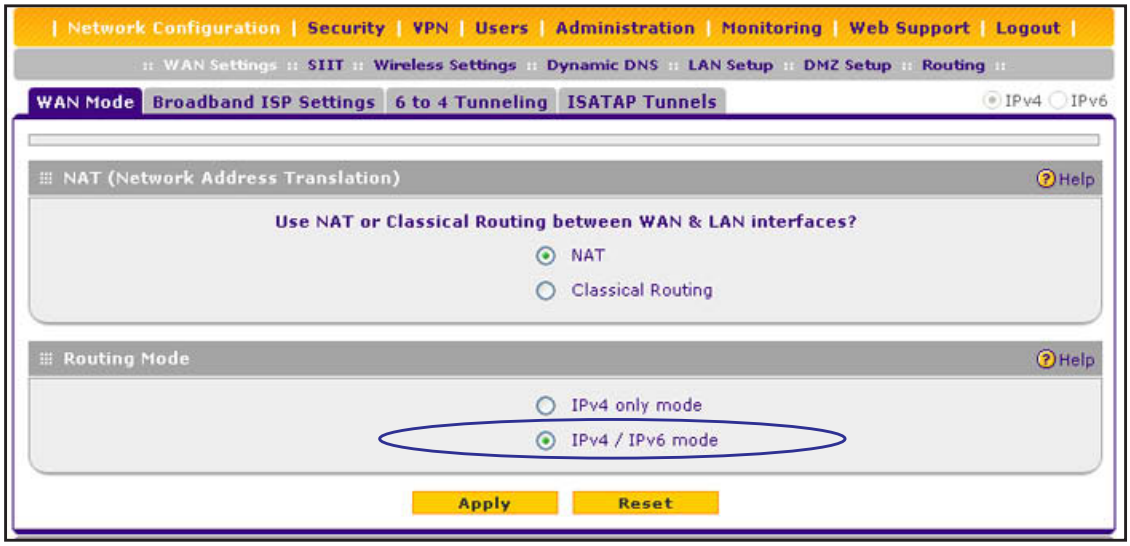

Figure 19.

2. 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 wireless VPN firewall to reboot.

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

Use a DHCPv6 Server to Configure an IPv6 Internet Connection

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

- **Stateless address autoconfiguration**. The wireless 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 wireless 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 75.

- **Stateful address autoconfiguration**. The wireless 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 the WAN port for an IPv6 connection to the Internet:**

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

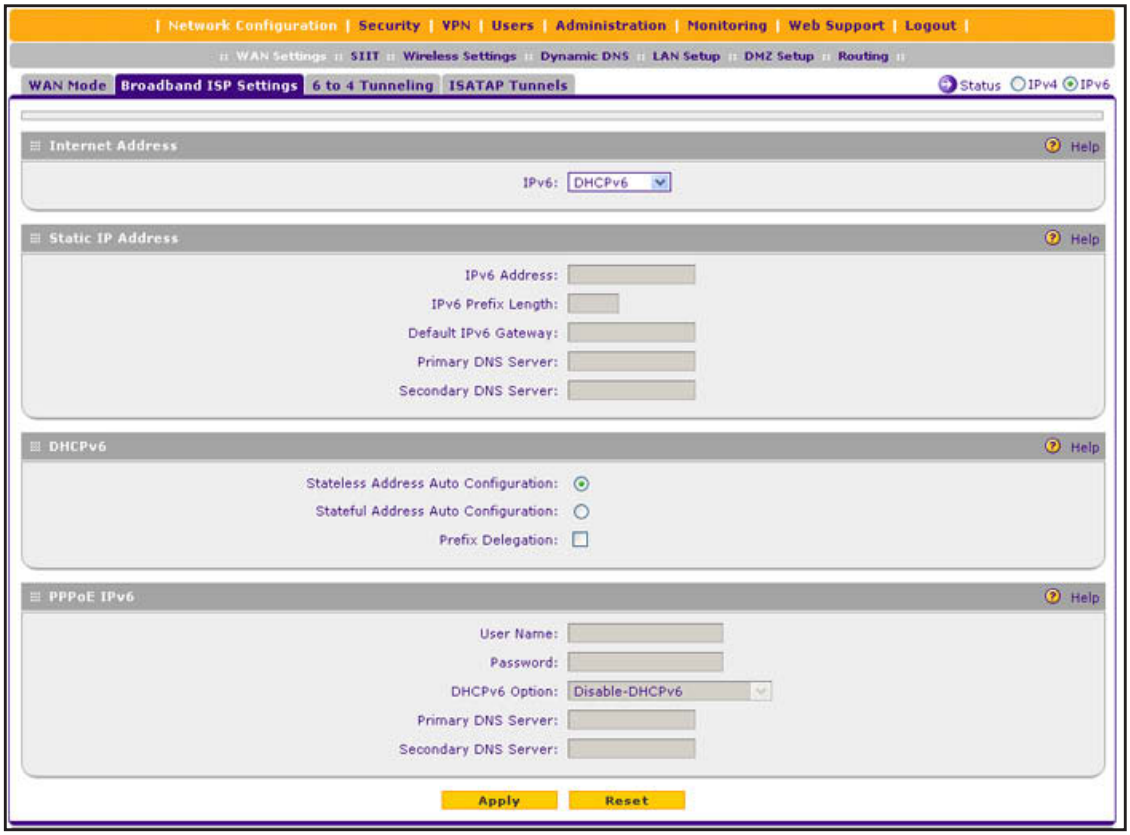

Figure 20.

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

5. 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 wireless 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 75.
   - **Prefix delegation check box is cleared**. Prefix delegation is disabled. This is the default setting.
6. Click **Apply** to save your changes.
7. To verify the connection, click the **Status** option arrow in the upper right of the screen to display the Connection Status pop-up screen. (The following figure shows a dynamic IP address configuration.)

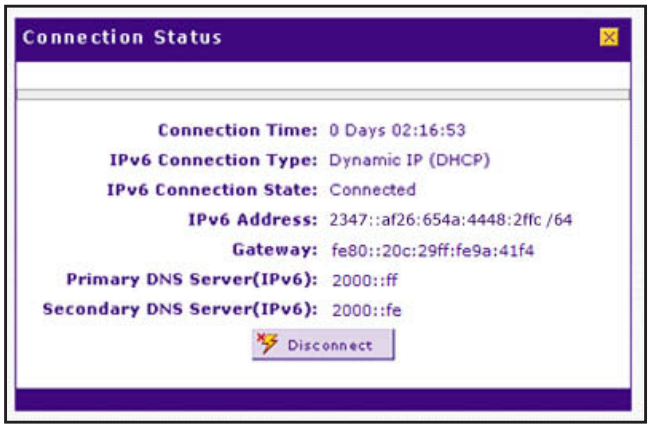

Figure 21.

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 385.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 370.

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 broadband ISP settings:**

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

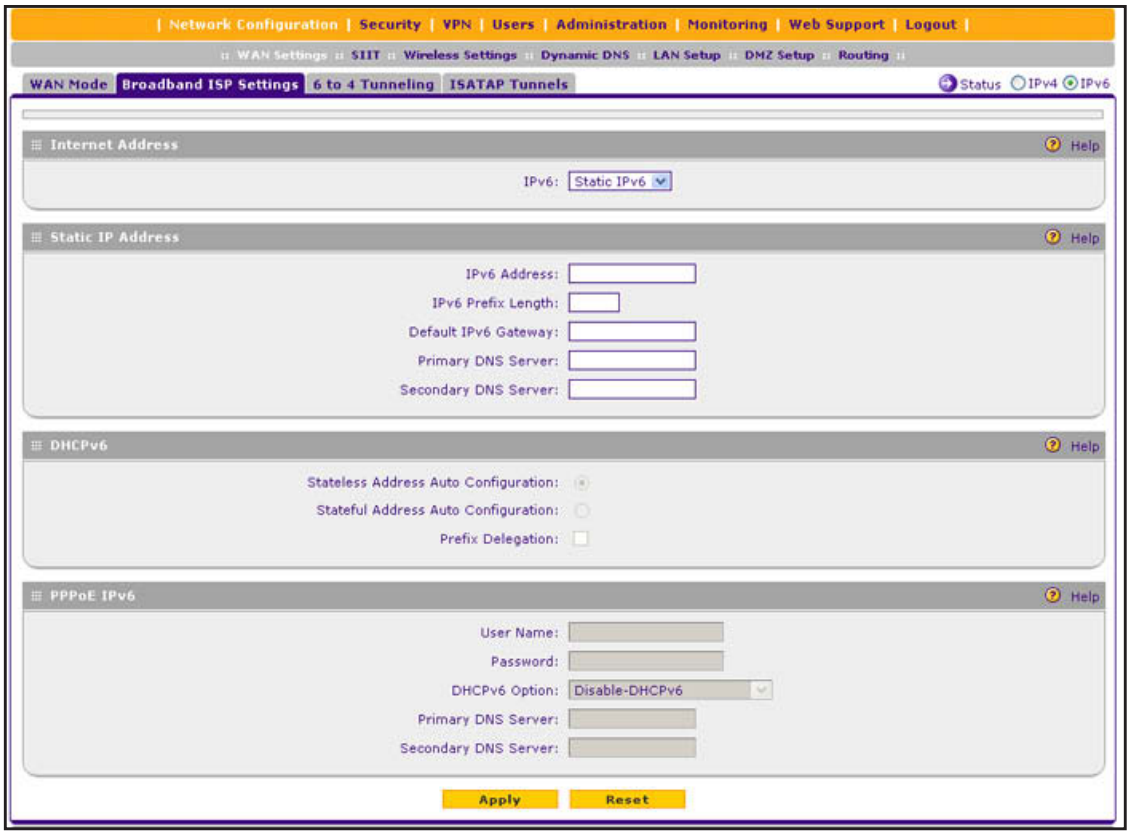

Figure 22.

3. In the Internet Address section of the screen, from the IPv6 drop-down list, select **Static IPv6**.
4. 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 7. Broadband ISP 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.

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

6. To verify the connection, click the **Status** option arrow in the upper right of the screen 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.)

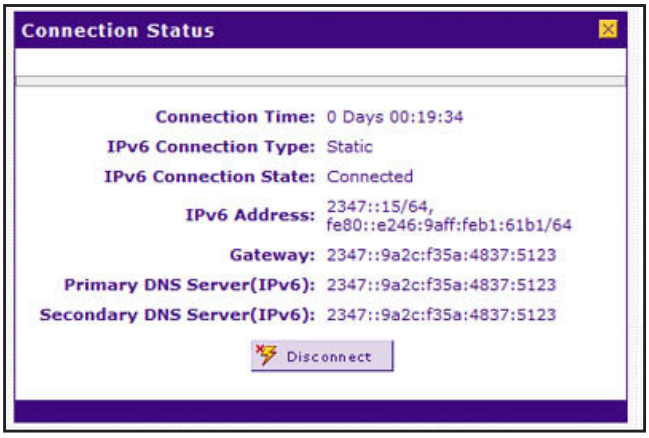

Figure 23.

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 385.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 370.

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 Broadband Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 51).

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 broadband ISP settings:**

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

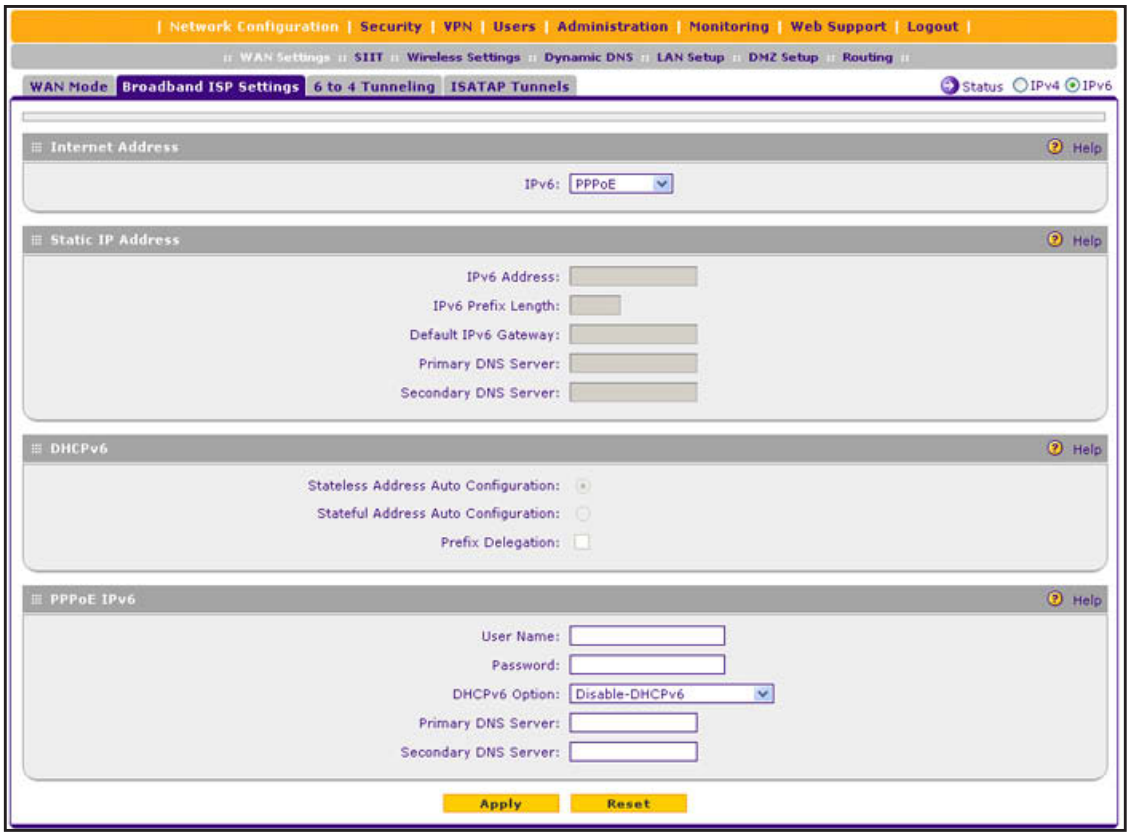

Figure 24.

3. In the Internet Address section of the screen, from the IPv6 drop-down list, select **PPPoE**.
4. 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 8. Broadband 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 8. Broadband 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 wireless 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 wireless 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 wireless VPN firewall obtains a prefix from the ISP's DHCPv6 server through prefix delegation, for example, 2001:db8::/64. The wireless 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 75.
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.

5. Click **Apply** to save your changes.
6. To verify the connection, click the **Status** option arrow in the upper right of the screen to display the Connection Status pop-up screen (see *Figure 23* on page 44, 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 385.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 370.

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 Broadband Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 51).

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 wireless VPN firewall functions as the endpoint for 6to4 tunnels in your network, make sure that the wireless VPN firewall has a static IPv4 address (see *Manually Configure an IPv4 Internet Connection* on page 32). 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 74.

Typically, 6to4 tunnel addresses start with a 2002 prefix (decimal notification). On the wireless VPN firewall, a 6to4 tunnel is indicated by sit0-WAN1 (see *View the Tunnel Status and IPv6 Addresses* on page 50).

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

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

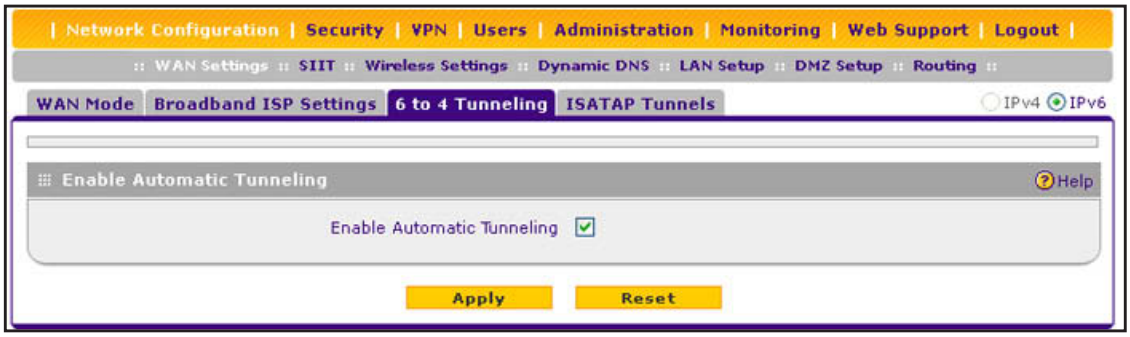

Figure 25.

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 74.

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 74.

The wireless 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.)

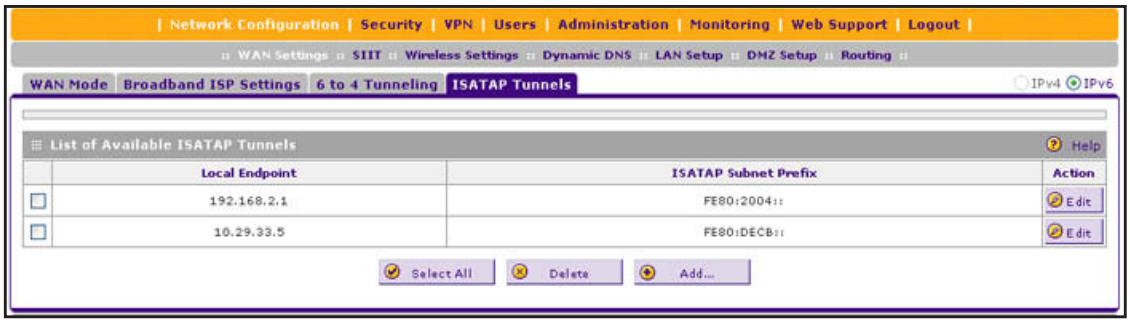

Figure 26.

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

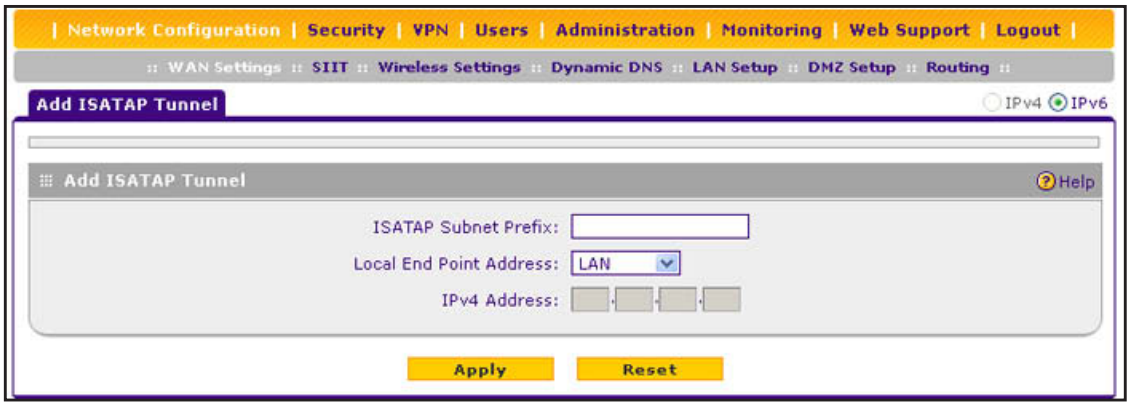

Figure 27.

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

Table 9. 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:

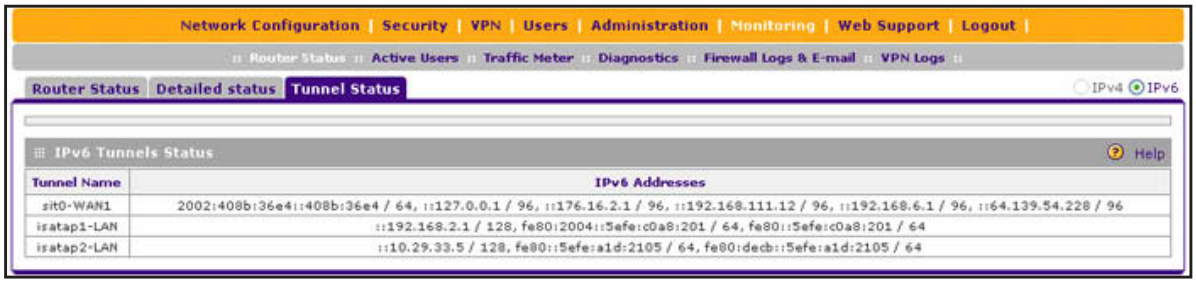

Figure 28.

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 wireless VPN firewall's LAN and IPv6-only devices on the WAN.

➢ **To configure SIIT:**

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

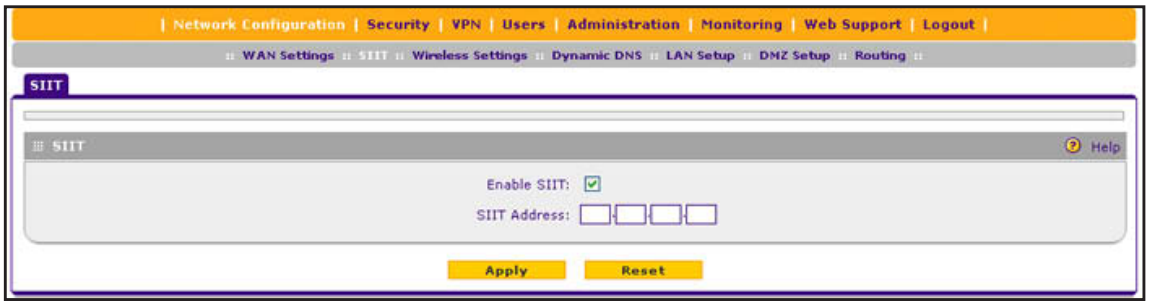

Figure 29.

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 Advanced WAN Options and Other Tasks

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

Note: Although you can access the Broadband Advanced Options screen only through the Broadband ISP Settings (IPv4) screen, the advanced options apply to both IPv4 and IPv6 WAN connections.

➢ **To configure advanced WAN options:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings**. The Broadband ISP Settings screen displays the IPv4 settings (see *Figure 10* on page 30).
2. Click the **Advanced** option arrow in the upper right of the screen. The Broadband Advanced Options screen displays:

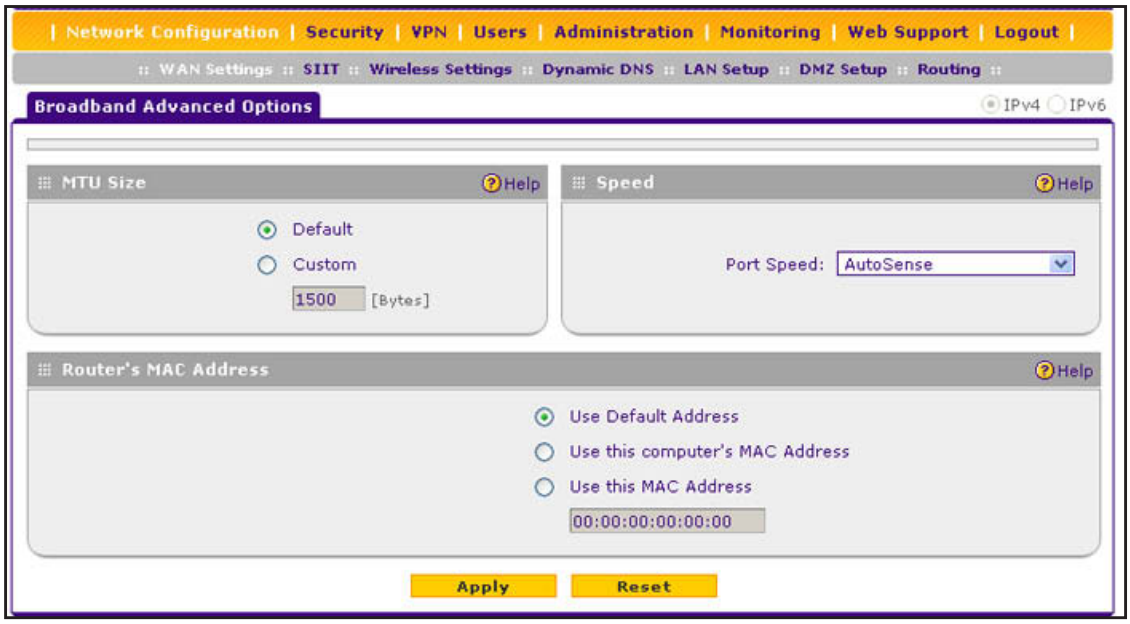

Figure 30.

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

Table 10. Broadband 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 10. Broadband Advanced Options screen settings (continued)

Setting	Description
Speed	
In most cases, the wireless 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 Half_Duplex**. Gigabit Ethernet speed at half 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 wireless 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 wireless 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.

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

Additional WAN-Related Configuration Tasks

If you want the ability to manage the wireless VPN firewall remotely, enable remote management (see *Configure Remote Management Access* on page 333). If you enable remote management, NETGEAR strongly recommends that you change your password (see *Change Passwords and Administrator and Guest Settings* on page 331).

You can also set up the traffic meter for the WAN interface. See *Enable the WAN Traffic Meter* on page 350.

Verify the Connection

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

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

What to Do Next

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

- *Chapter 3, LAN Configuration*
- *Chapter 4, Wireless Configuration and Security*
- *Configure Authentication Domains, Groups, and Users* on page 298
- *Manage Digital Certificates for VPN Connections* on page 316
- *Use the IPSec VPN Wizard for Client and Gateway Configurations* on page 196
- *Chapter 7, Virtual Private Networking Using SSL Connections*

LAN Configuration

3

This chapter describes how to configure the LAN features of your wireless 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 wireless 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 eight LAN ports of the wireless VPN firewall are assigned to the default VLAN, or VLAN 1. Therefore, by default, all eight 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 wireless 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 wireless VPN firewall, the other one to another device:

Packets coming from the IP phone to the wireless VPN firewall LAN port are tagged. Packets passing through the IP phone from the connected device to the wireless VPN firewall LAN port are untagged. When you assign the wireless VPN firewall LAN port to a VLAN, packets entering and leaving the port are tagged with the VLAN ID. However, untagged packets entering the wireless 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 27. For information about how to add and edit a VLAN profile, including its DHCP options, see *Configure a VLAN Profile* on page 60.

Assign and Manage VLAN Profiles

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

1. Select **Network Configuration > LAN Setup**. 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.)

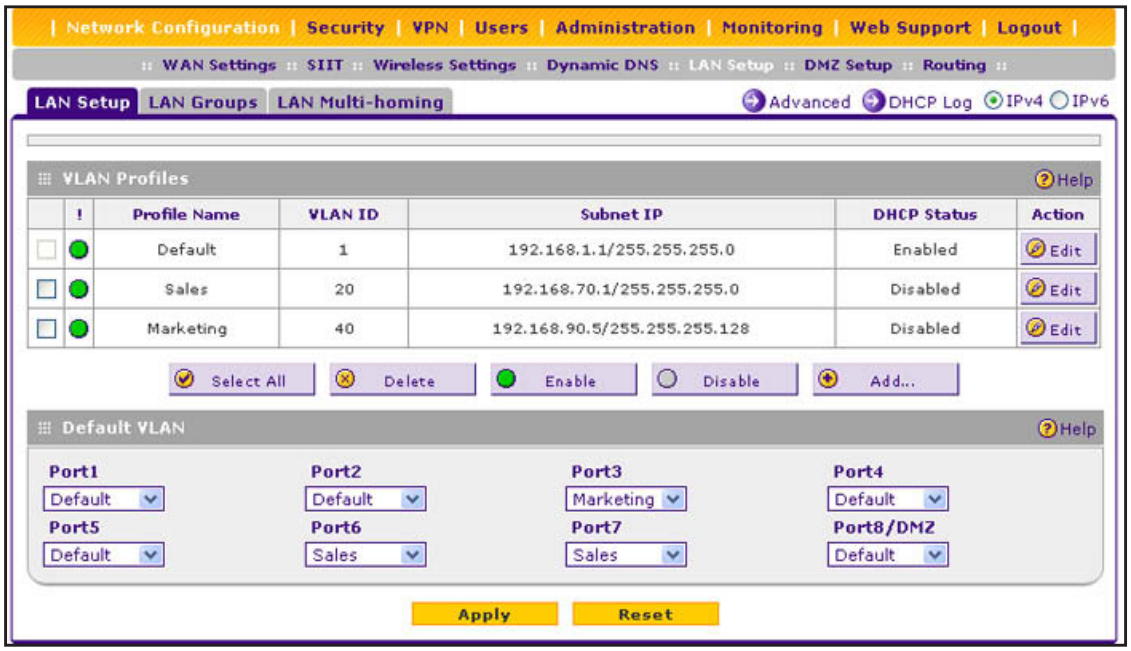

Figure 31.

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 60). The configuration of the DHCP options for the wireless VPN firewall's default VLAN, or VLAN 1, is described in *Configure the IPv4 Internet Connection and WAN Settings* on page 27. 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 wireless VPN firewall to assign IP, DNS server, WINS server, and default gateway addresses to all computers connected to the wireless VPN firewall's LAN. The assigned default gateway address is the LAN address of the wireless 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 wireless VPN firewall are satisfactory.

The wireless 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 wireless VPN firewall's LAN IP address)
- Primary DNS server (the wireless 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 wireless 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 wireless VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (as configured on the Broadband 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 wireless 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 wireless 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 Setup**. 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 57. The following information describes how to configure a VLAN profile.

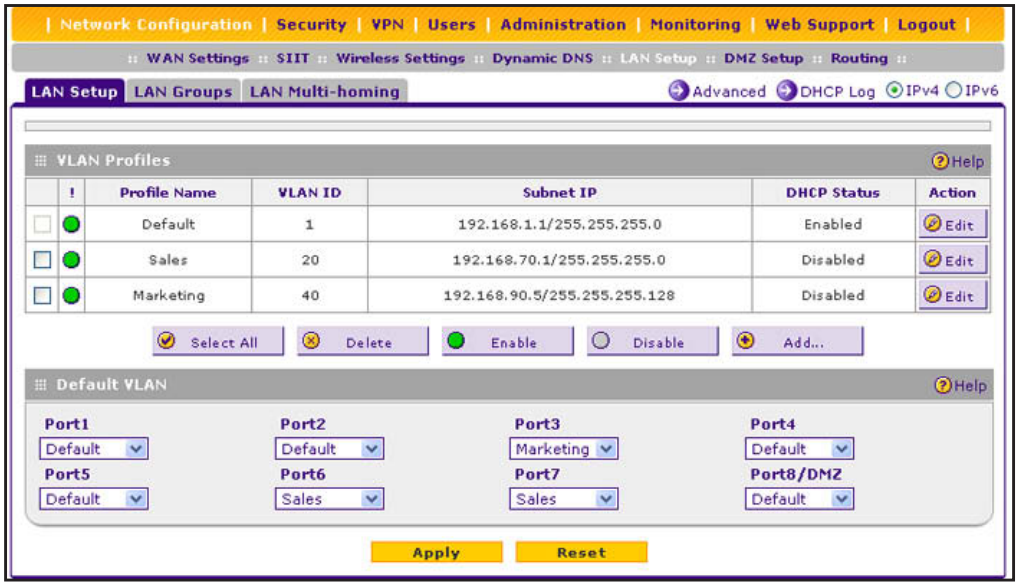

Figure 32.

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

Figure 33.

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

Table 11. 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.
Port Membership	
Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, and Port 8 / 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 wireless 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 wireless VPN firewall automatically calculates the subnet mask. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the wireless 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 11. Add VLAN Profile screen settings (continued)

Setting	Description	
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the wireless 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 wireless 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 wireless 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 wireless VPN firewall provides this address as the primary DNS server IP address. If no address is specified, the wireless 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 wireless 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 wireless 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 wireless VPN firewall serves as a relay.

Table 11. 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 wireless 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 5, Firewall Protection*.

➢ **To edit a VLAN profile:**

1. On the LAN Setup screen for IPv4 (see *Figure 32* on page 60), 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 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 VLAN profiles:**

1. On the LAN Setup screen for IPv4 (see *Figure 32* on page 60), 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 Setup**. 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 32* on page 60).
2. Click the **Advanced** option arrow in the upper middle of the LAN Setup screen. The IPv4 LAN Advanced screen displays:

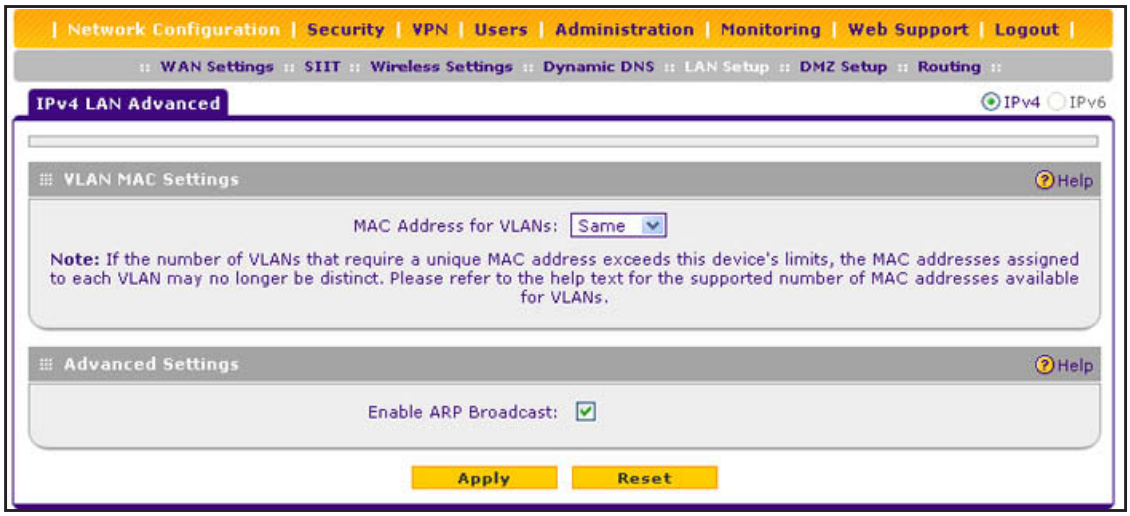

Figure 34.

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 LAN Advanced screen, the MAC addresses that are assigned to each VLAN might no longer be distinct.

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 wireless 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 Setup > 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.)

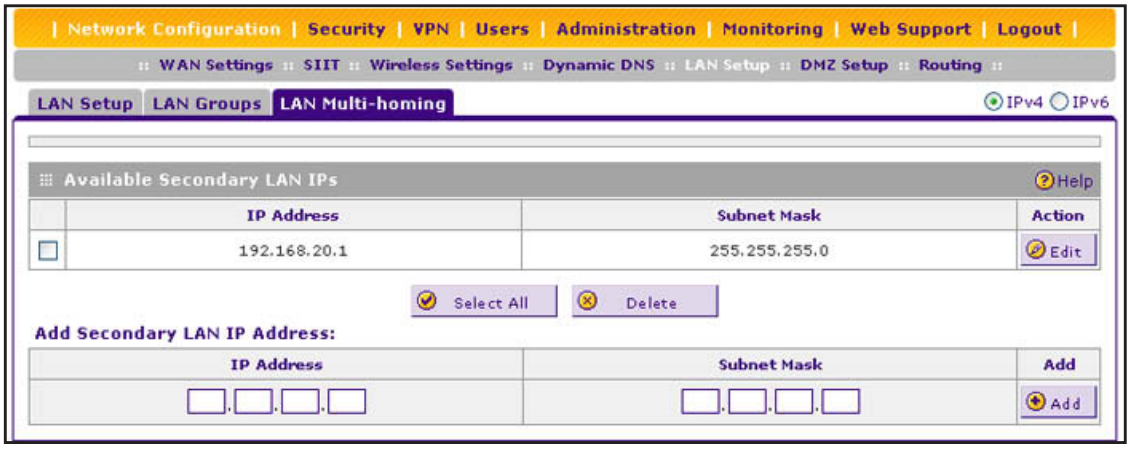

Figure 35.

The Available Secondary LAN IPs table displays the secondary LAN IP addresses added to the wireless 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)

The Known PCs and Devices table on the LAN Groups (IPv4) screen (see *Figure 36* on page 69) contains a list of all known computers and network devices that are assigned dynamic IP addresses by the wireless 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 wireless 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.
- You do not 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.

- You do not 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 131).
  - 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 179).
  - If necessary, you can also create firewall rules to apply to a single computer (see *Enable Source MAC Filtering* on page 184). 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 Setup > 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.)

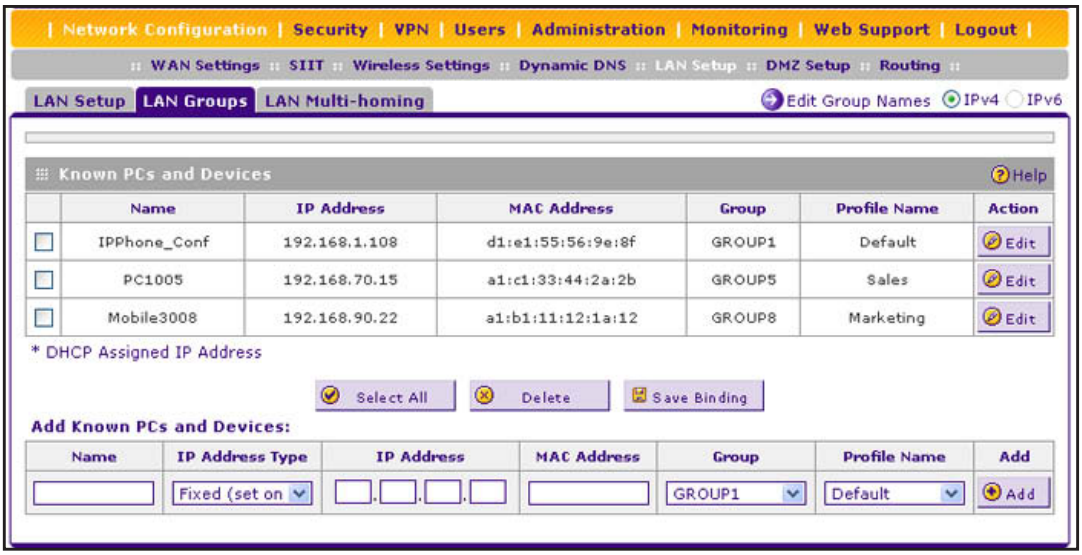

Figure 36.

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 wireless 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 12. 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 wireless VPN firewall always assigns the specified IP address to this client during the DHCP negotiation (see also *Set Up DHCP Address Reservation* on page 73). **Note:** For both types of IP addresses, the wireless VPN firewall reserves the IP address for the associated MAC address.

Table 12. 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 100* on page 187).

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 the previous figure), click the **Edit** table button of a table entry. The Edit LAN Groups screen displays (see the following figure, which contains an example).

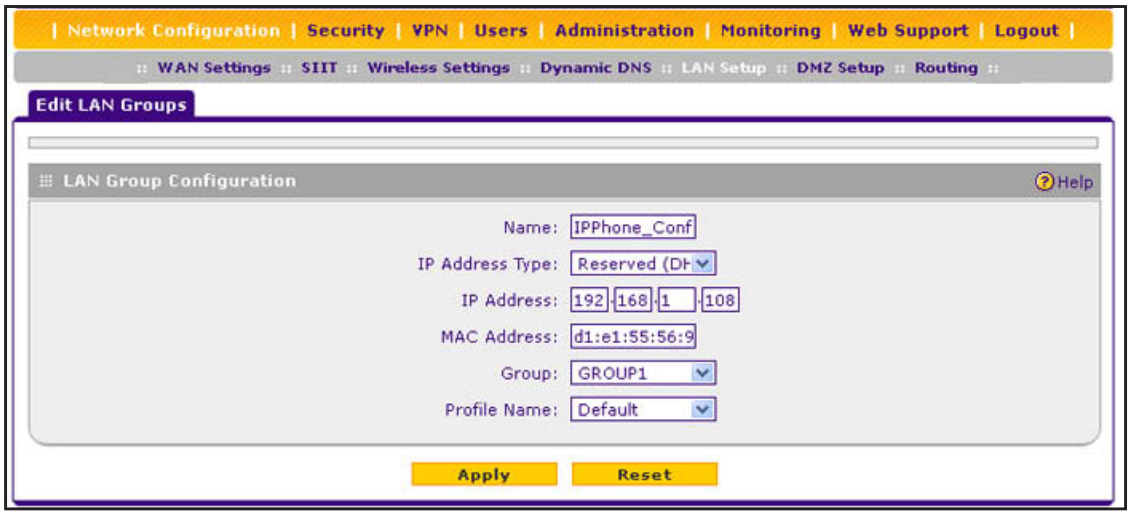

Figure 37.

2. Modify the settings as described in *Table 12* on page 70.
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 36* on page 69), 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 100* on page 187).

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 names of any of the eight available groups:**

1. Select **Network Configuration > LAN Setup > LAN Groups**. The LAN Groups screen displays (see *Figure 36* on page 69, 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.)

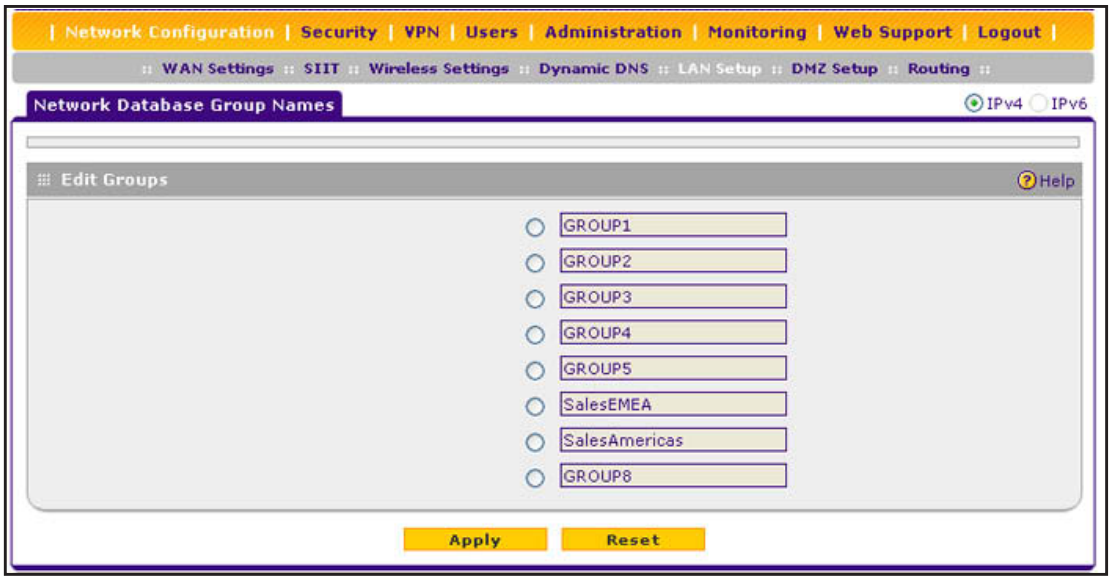

Figure 38.

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

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 wireless 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 70.

Note: The reserved address is not assigned until the next time the computer or device contacts the wireless 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 100* on page 187).

Manage the IPv6 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 wireless 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 48.

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 81).

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 wireless VPN firewall's *stateless* DHCPv6 server to assign to its IPv6 LAN clients.

Prefix delegation functions in the following way:

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

   You need to select the Prefix Delegation check box on the ISP Broadband Settings screen for IPv6 (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 40).

2. The ISP allocates a prefix to the wireless 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 81).

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 76).
   - Configure the RADVD (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 81).
   - 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 80).
   - Optionally, manually add prefixes to List of Prefixes to Advertise table on the RADVD screen (see *Advertisement Prefixes for the LAN* on page 83).

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 78).

Configure the IPv6 LAN

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

1. Select **Network Configuration > LAN Setup**.
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.)

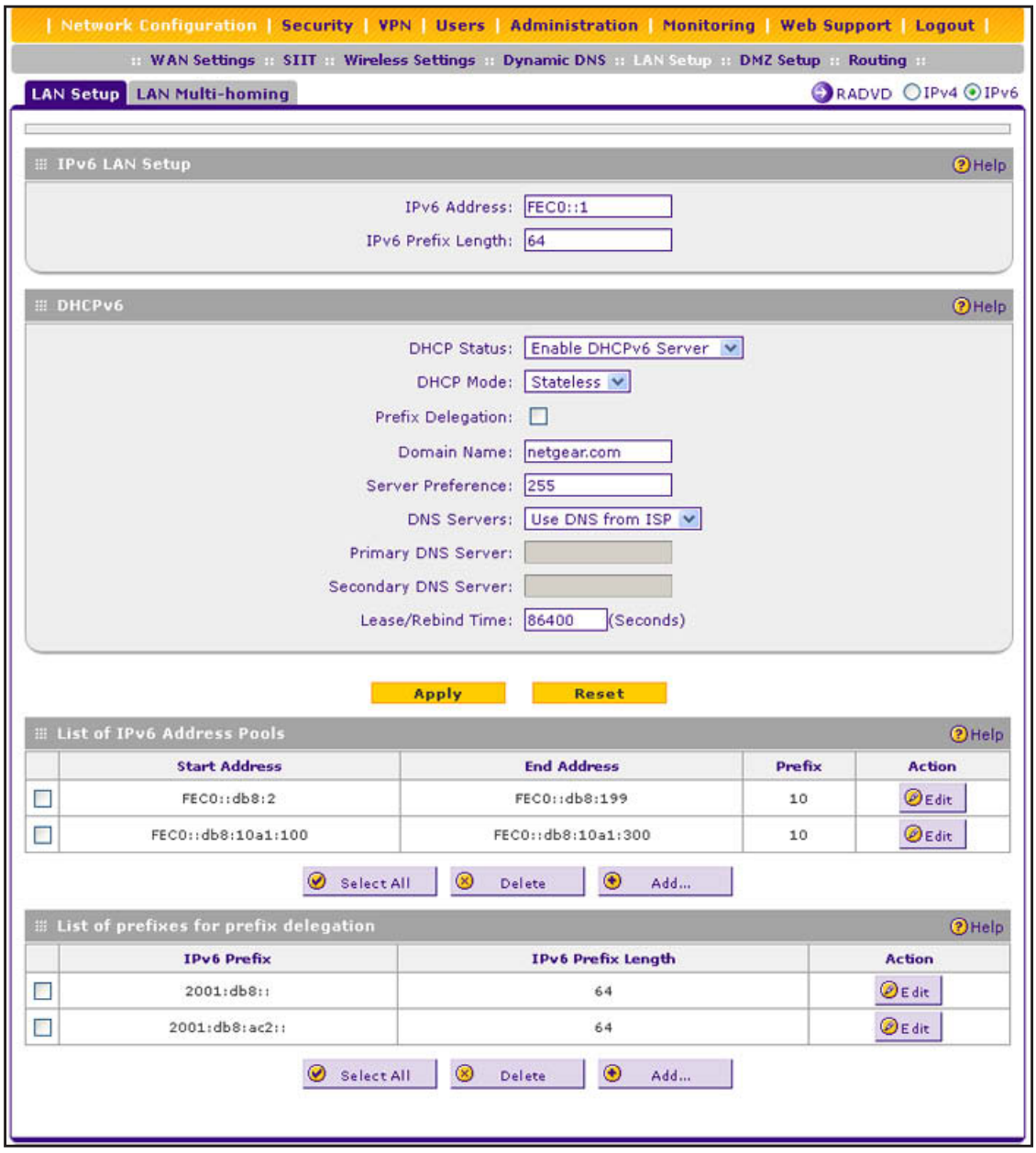

Figure 39.

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 13. 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 81). 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 78).
	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 ISP Broadband Settings screen for IPv6 is also selected (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 40) to enable the wireless 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 81). • **Prefix delegation check box is cleared**. Prefix delegation is disabled in the LAN. This is the default setting.

Table 13. LAN Setup screen settings for IPv6 (continued)

Setting	Description		
DHCP Status (continued)	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.	
	DNS Servers	Select one of the DNS server options from the drop-down lists: • **Use DNS Proxy**. The wireless VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers that you configured on the Broadband ISP Settings (IPv6) screen (see *Configure a Static IPv6 Internet Connection* on page 42). • **Use DNS from ISP**. The wireless VPN firewall uses the ISP's DNS servers that you configured on the Broadband ISP Settings (IPv6) screen (see *Configure a Static IPv6 Internet Connection* on page 42). • **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:

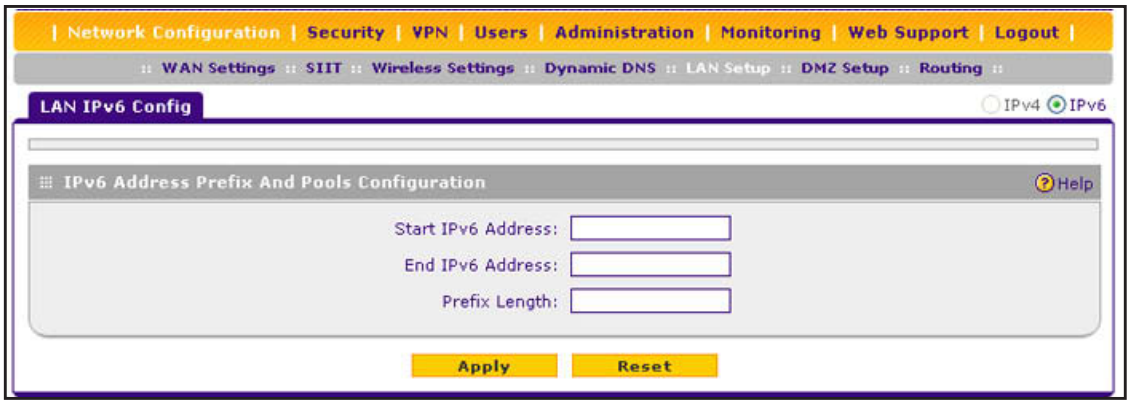

Figure 40.

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

Table 14. 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 39* on page 76), 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 39* on page 76), 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 Broadband Settings screen for IPv6 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:

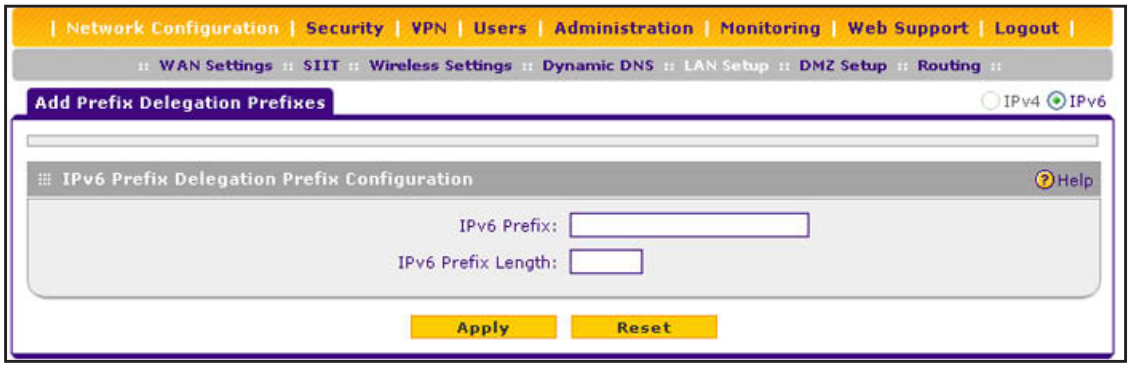

Figure 41.

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 39* on page 76), 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 39* on page 76), 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 wireless 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 15. 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 Setup**.

2. In the upper right of the screen, select the **IPv6** radio button. The LAN Setup screen displays the IPv6 settings (see *Figure 39* on page 76.)
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.)

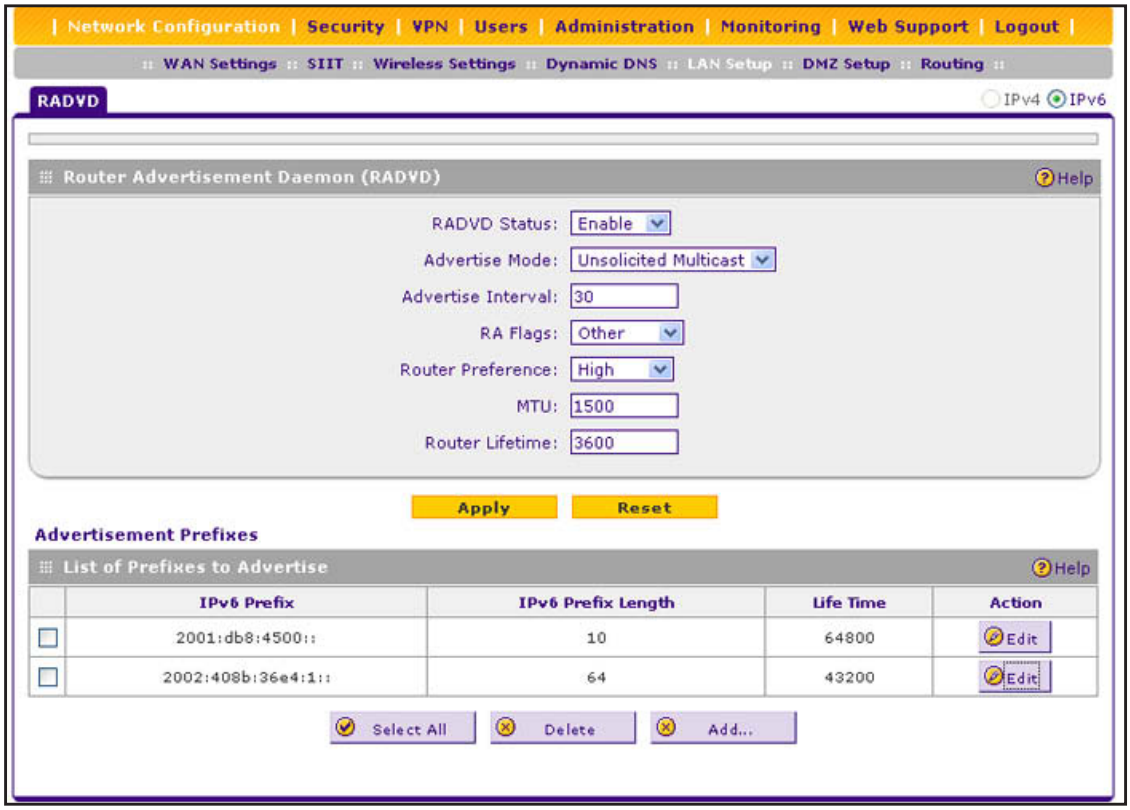

Figure 42.

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

Table 16. 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 wireless VPN firewall advertises unsolicited multicast packets at a rate that is specified by the advertisement interval. • **Unicast only**. The wireless 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 16. 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 wireless 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 wireless VPN firewall is treated as a nonpreferred router in the LAN. • **Medium**. The wireless VPN firewall is treated as a neutral router in the LAN. • **High**. The wireless 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 Advertisement Prefix screen displays:

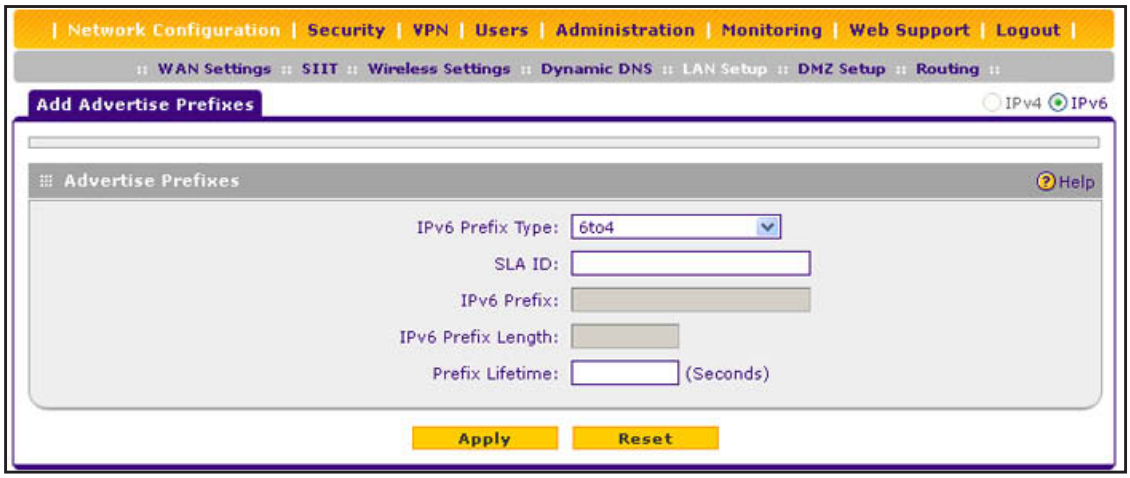

Figure 43.

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

Table 17. Add Advertisement Prefix 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 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 SLA ID field is masked out.
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 wireless 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 42* on page 82), 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 42* on page 82), 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 wireless 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 Setup > 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.)

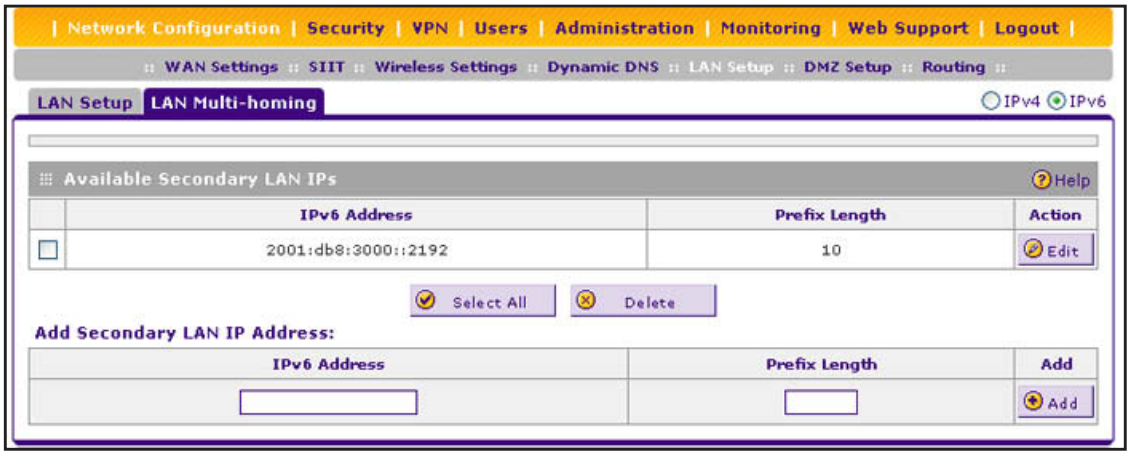

Figure 44.

The Available Secondary LAN IPs table displays the secondary LAN IP addresses added to the wireless 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 wireless 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 wireless 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 146 and *Configure LAN DMZ Rules* on page 154, respectively.

Note: When you enable the DMZ port for IPv4 traffic, IPv6 traffic, or both, the DMZ LED next to LAN port 8 (see *Front Panel* on page 16) 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 8; see *Front Panel* on page 16) 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:

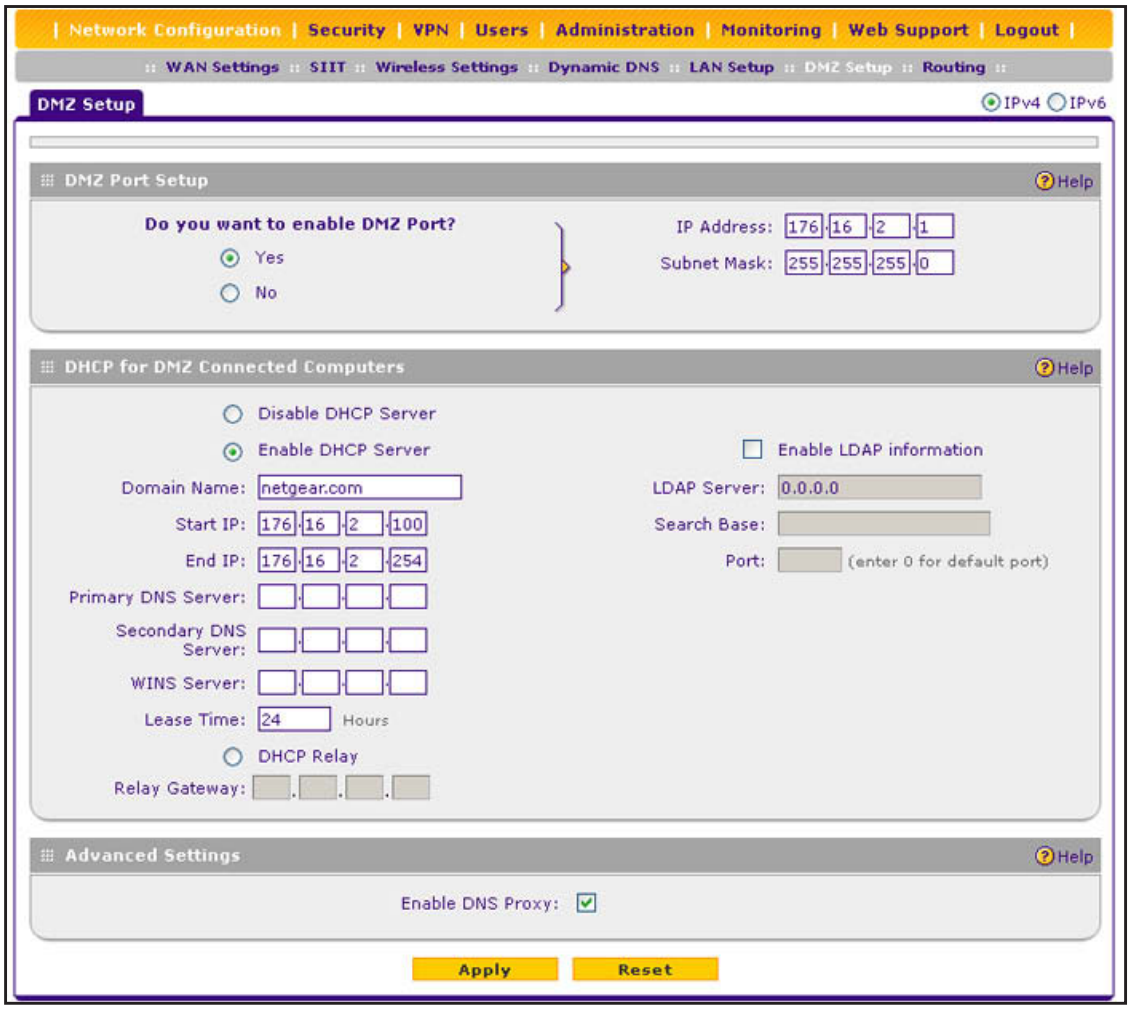

Figure 45.

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

Table 18. 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.

Table 18. DMZ Setup screen settings for IPv4 (continued)

Setting	Description	
Do you want to enable DMZ Port? (continued)	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.
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 wireless 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 wireless 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 wireless 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 wireless VPN firewall provides this address as the primary DNS server IP address. If no address is specified, the wireless 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 wireless 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.

Table 18. DMZ Setup screen settings for IPv4 (continued)

Setting	Description	
DHCP Relay	To use the wireless 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 wireless VPN firewall serves as a relay.
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 wireless 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 8; see *Front Panel* on page 16) 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 94).
- **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 93).

➢ **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:

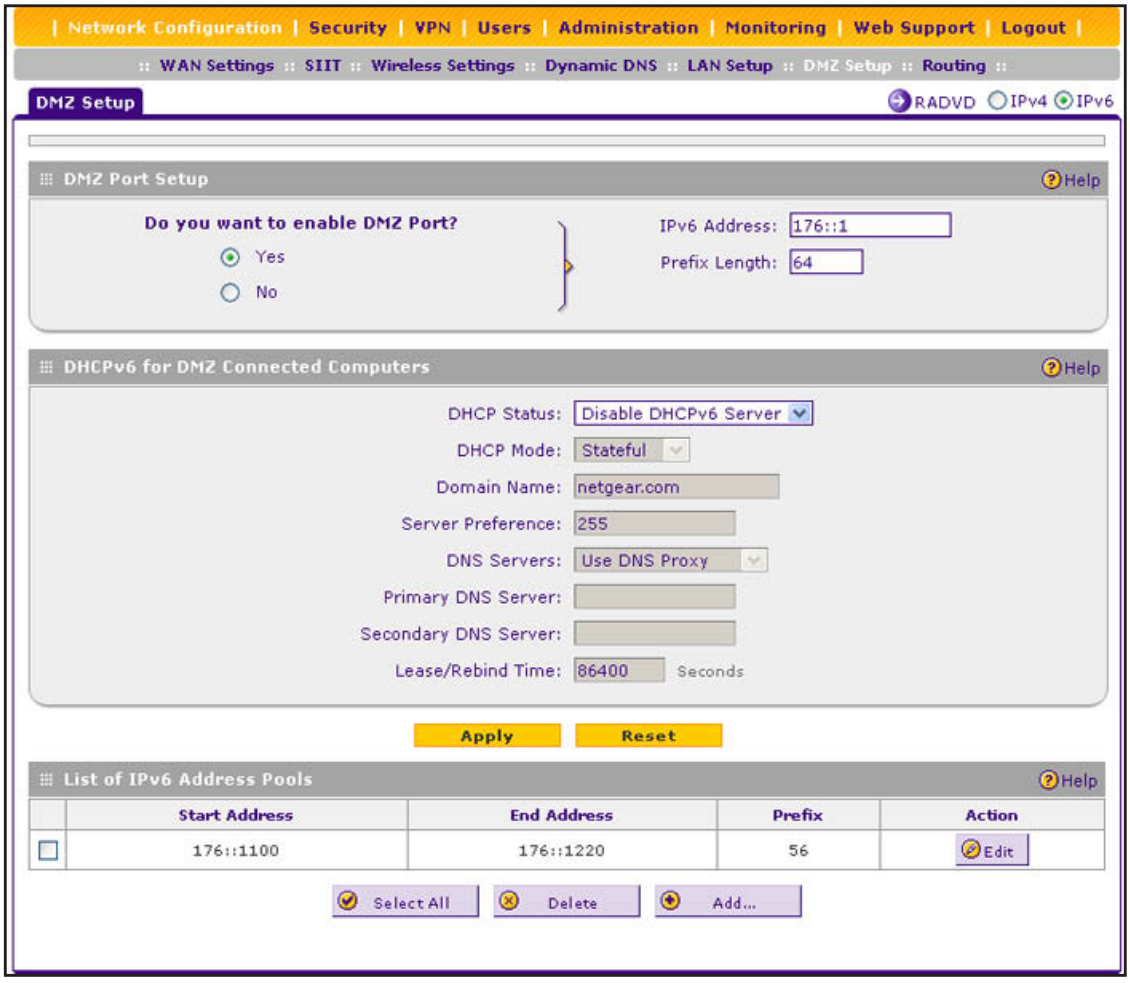

Figure 46.

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

Table 19. 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 94). • **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 93).
	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 19. 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 wireless VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers that you configured on the Broadband ISP Settings (IPv6) screen (see *Configure a Static IPv6 Internet Connection* on page 42). • **Use DNS from ISP**. The wireless VPN firewall uses the ISP's DNS servers that you configured on the Broadband ISP Settings (IPv6) screen (see *Configure a Static IPv6 Internet Connection* on page 42). • **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 46* on page 91), under the List of IPv6 Address Pools table, click **Add**. The DMZ IPv6 Config screen displays:

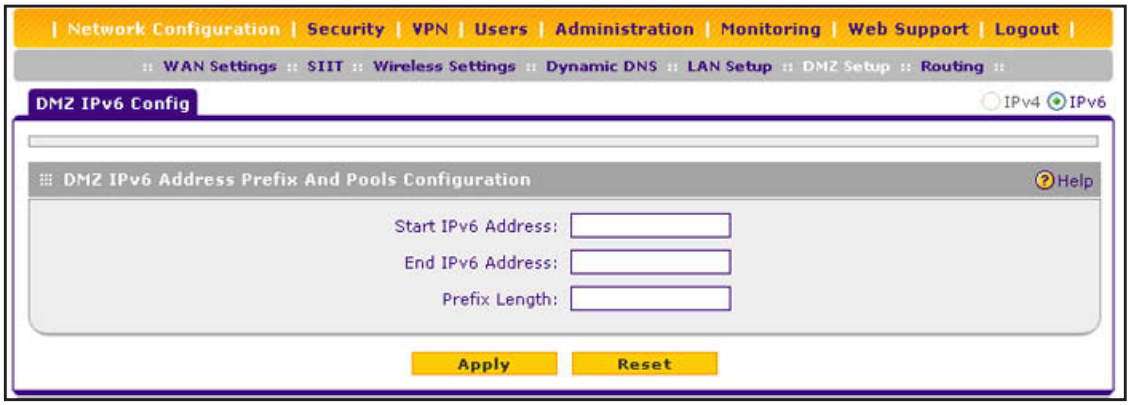

Figure 47.

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

Table 20. 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 46* on page 91), 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 46* on page 91), 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 wireless 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 21. 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 46* on page 91).
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.)

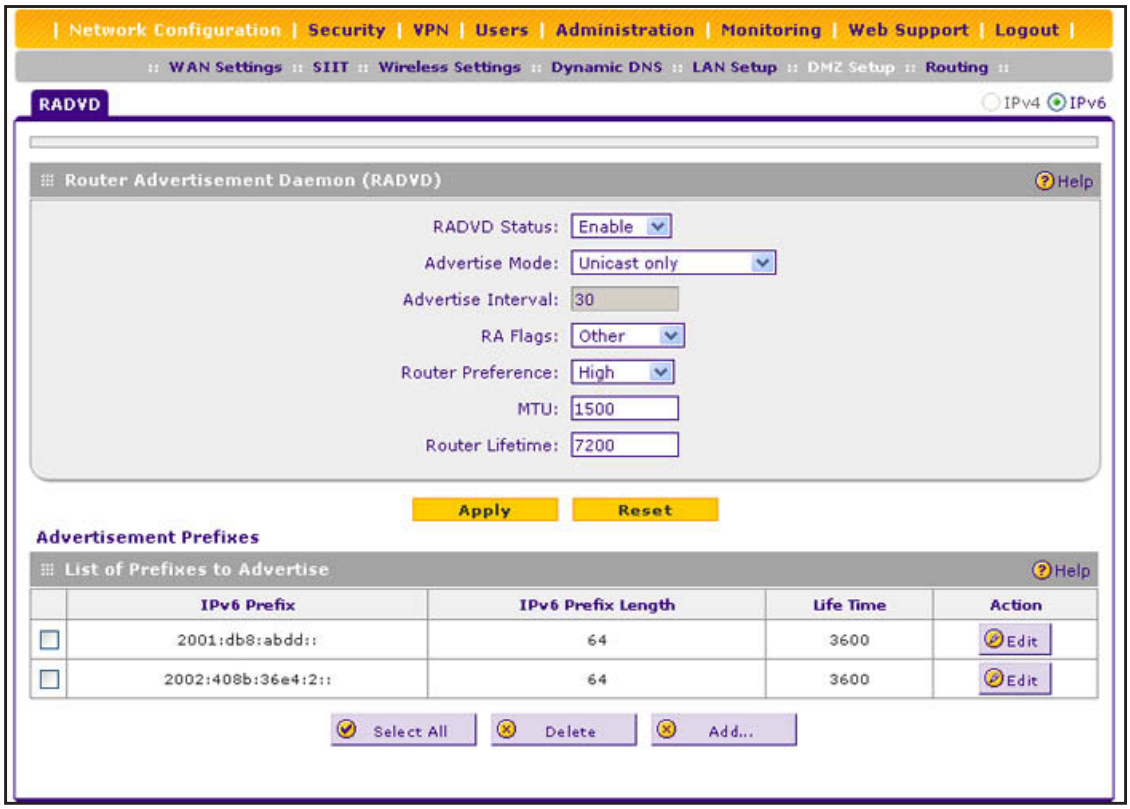

Figure 48.

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

Table 22. 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 wireless VPN firewall advertises unsolicited multicast packets at a rate that is specified by the advertisement interval. • **Unicast only**. The wireless 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 22. 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 wireless 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 wireless VPN firewall is treated as a nonpreferred router in the DMZ. • **Medium**. The wireless VPN firewall is treated as a neutral router in the DMZ. • **High**. The wireless 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:

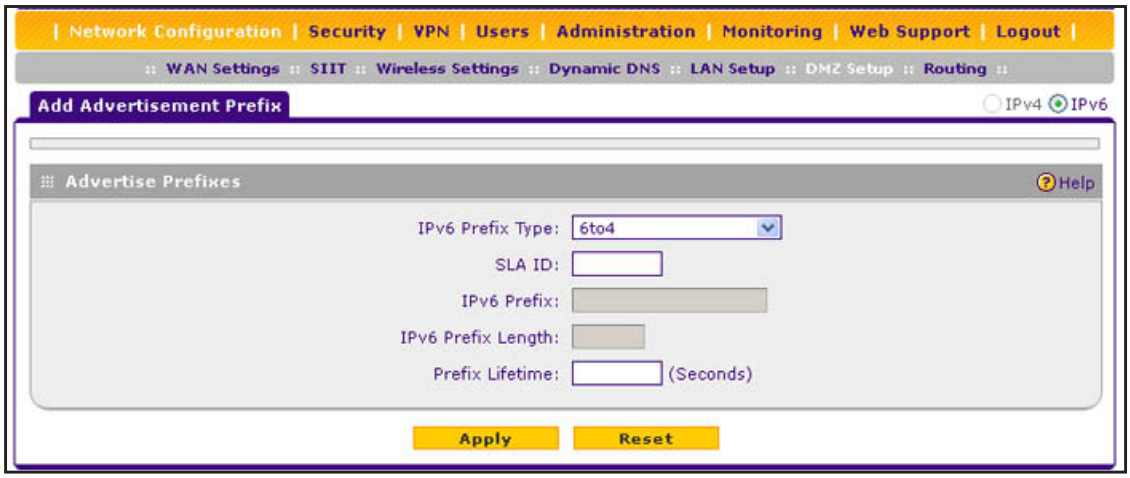

Figure 49.

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

Table 23. 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 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 SLA ID field is masked out.
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 wireless 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 48* on page 96), 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 48* on page 96), 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 wireless VPN firewall. Under normal circumstances, the wireless 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 wireless 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 66). 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.)

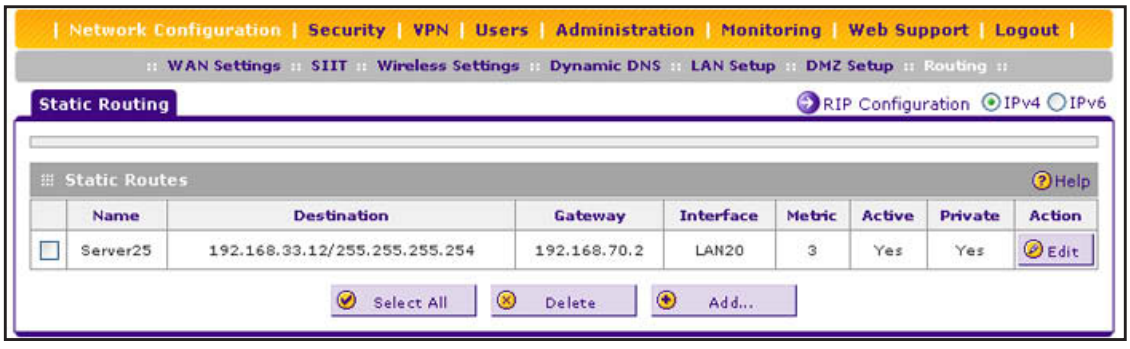

Figure 50.

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

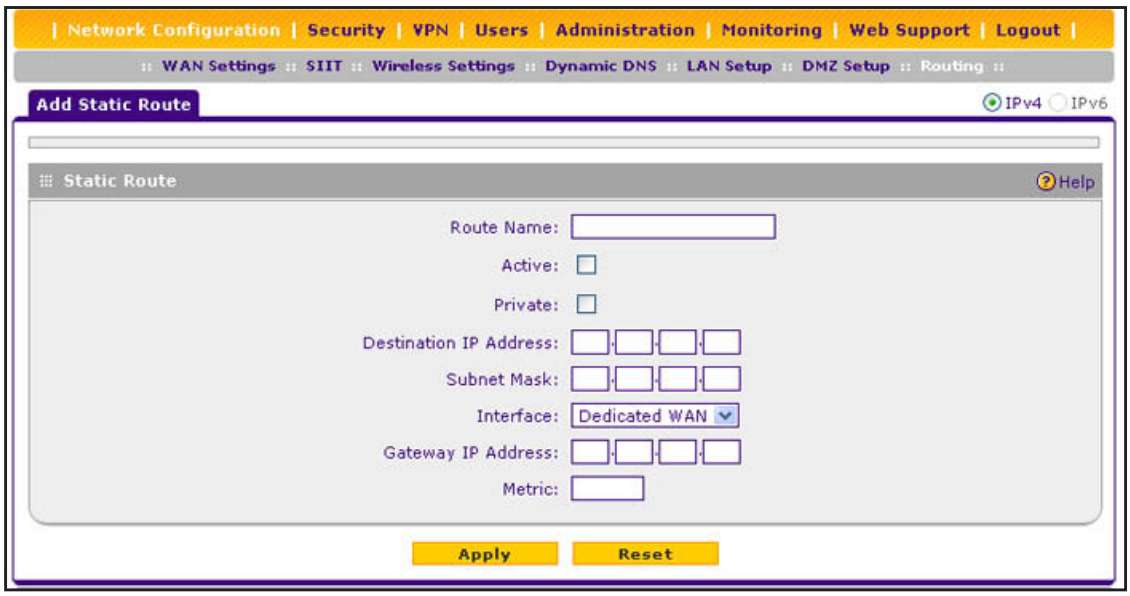

Figure 51.

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

Table 24. 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 (WAN, VLAN, or 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 50* on page 99), 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 50* on page 99), 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 50* on page 99).
  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.)

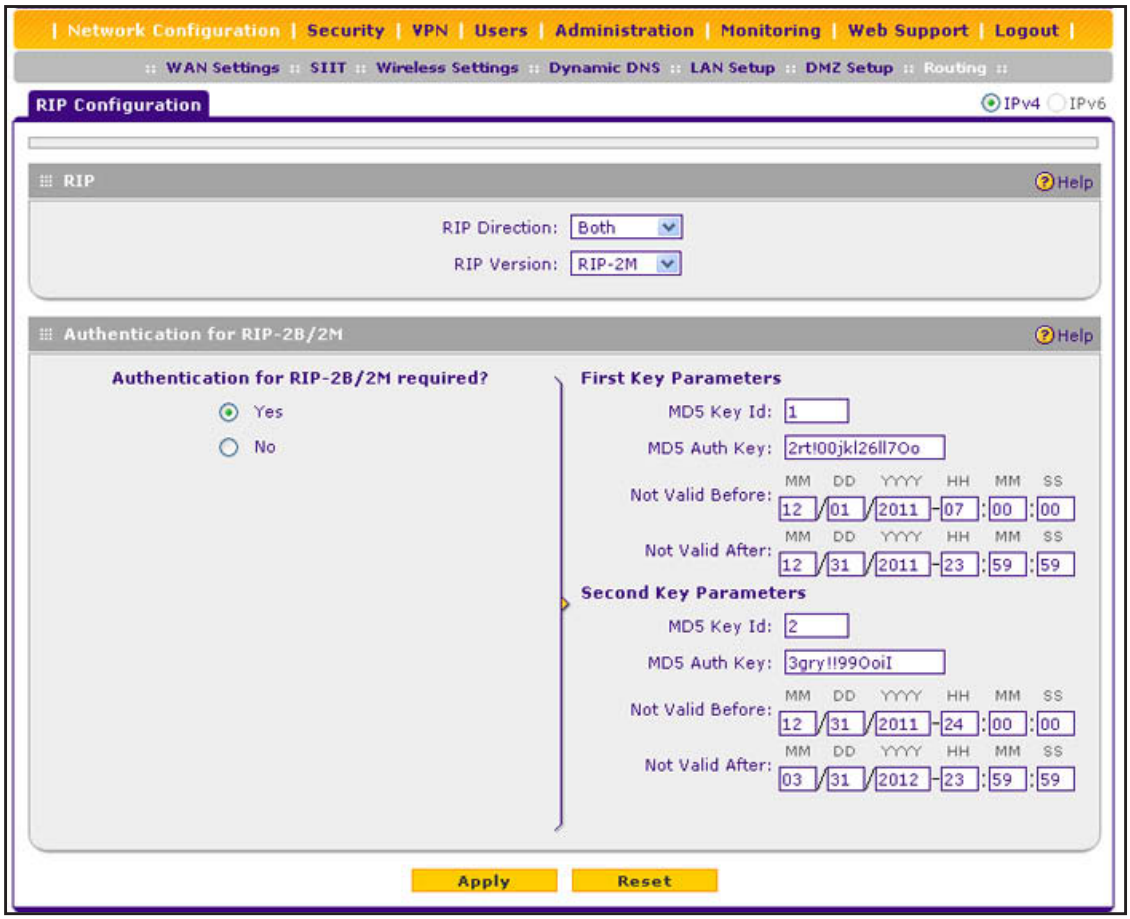

Figure 52.

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

Table 25. RIP Configuration screen settings

Setting	Description
RIP	
RIP Direction	From the RIP Direction drop-down list, select the direction in which the wireless VPN firewall sends and receives RIP packets: • **None**. The wireless 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 wireless VPN firewall accepts RIP information from other routers but does not advertise its routing table. • **Out Only**. The wireless VPN firewall advertises its routing table but does not accept RIP information from other routers. • **Both**. The wireless VPN firewall advertises its routing table and also processes RIP information received from other routers.

Table 25. RIP Configuration screen settings (continued)

Setting	Description	
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.
	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, assume the following:

- The wireless VPN firewall's primary Internet access is through a cable modem to an ISP.
- The wireless VPN firewall is on a local LAN with IP address 192.168.1.100.
- The wireless 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 wireless 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 wireless 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 wireless 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 wireless 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 wireless 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:

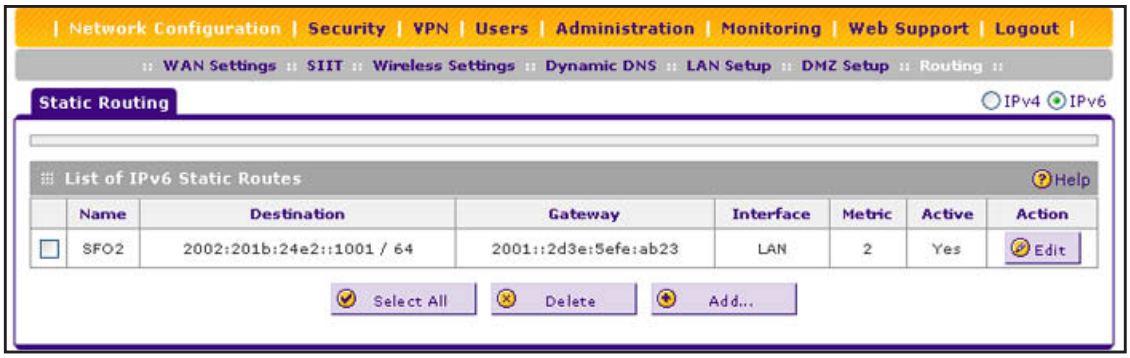

Figure 53.

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

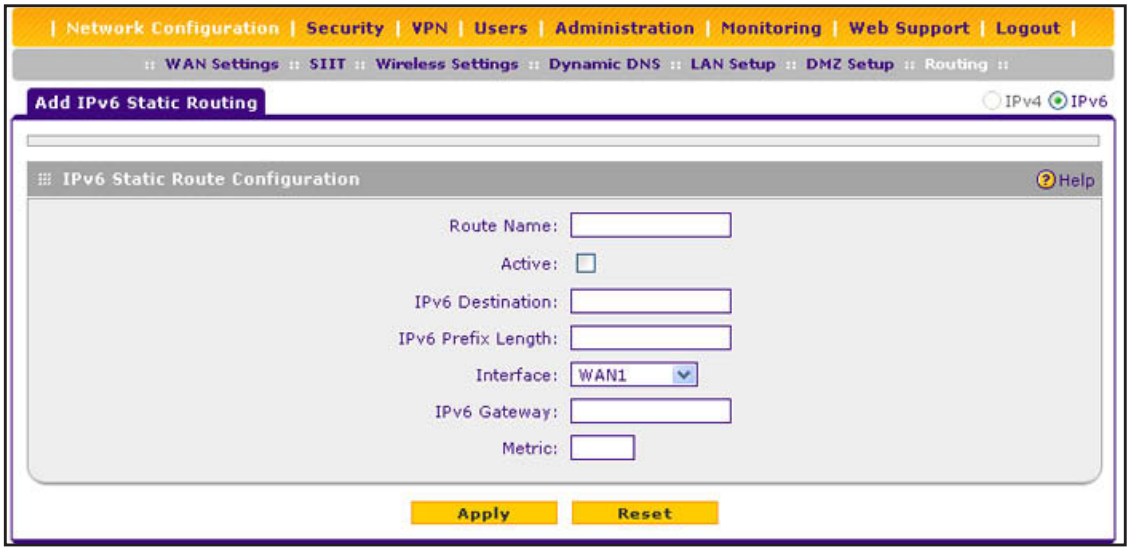

Figure 54.

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

Table 26. 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.

Table 26. Add IPv6 Static Routing screen settings (continued)

Setting	Description
Interface	From the drop-down list, select the physical or virtual network interface (WAN1, sit0 Tunnel, LAN, 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 53* on page 105), 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 53* on page 105), 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.

Wireless Configuration and Security

4

This chapter describes how to configure the wireless features of your ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N. This chapter includes the following sections:

- *Overview of the Wireless Features*
- *Configure the Basic Radio Settings*
- *Wireless Data Security Options*
- *Wireless Security Profiles*
- *Configure Advanced Radio Settings*
- *Test Basic Wireless Connectivity*

Before you set up the wireless features that are described in this chapter, connect the wireless VPN firewall and get the Internet connection working. The wireless VPN firewall should work with an Ethernet WAN connection. In planning your wireless network, consider the level of security required.

WARNING:

If you are configuring the wireless settings from a wireless computer and you change the wireless VPN firewall's SSID, channel, or wireless security settings, you lose your wireless connection when you click Apply. You then need to change the wireless settings of your computer to match the wireless VPN firewall's new settings.

Overview of the Wireless Features

The wireless VPN firewall integrates a single 2.4 GHz radio and physical access point that provides 2.4 GHz 802.11b/g/n connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. You can configure up to four wireless security profiles and SSIDs, allowing you to tailor access and security to a variety of wireless clients.

The wireless VPN firewall provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) through an antenna. Typically, an individual in-building wireless access point provides a maximum connectivity area of about a 300-foot radius. The wireless VPN firewall can support a small group of wireless users—typically 10 to 32 users.

Configure the wireless features according to the order of the following sections:

1. *Configure the Basic Radio Settings*
2. *Configure and Enable Wireless Profiles*
3. (Optional) *Configure Wi-Fi Protected Setup*
4. (Optional) *Configure Advanced Radio Settings*

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the wireless VPN firewall. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless VPN firewall. For complete performance specifications, see the Data Sheet at *http://www.netgear.com/images/FVS318N_DS_23Aug1118-36060.pdf*.

For best results, place your wireless VPN firewall according to the following general guidelines:

- Near the center of the area in which your wireless devices will operate.
- In an elevated location such as a high shelf where the wirelessly connected devices have line-of-sight access (even if through walls).
- Away from sources of interference, such as computers, microwaves ovens, and 2.4-GHz cordless phones.
- Away from large metal surfaces or water.

- Placing the antennas in a vertical position provides the best side-to-side coverage. Placing the antennas in a horizontal position provides the best up-and-down coverage.
- If you are using multiple wireless access points, configure access points to use different radio frequency channels to reduce interference. The recommended channel space between adjacent access points is five channels (for example, use channels 1 and 6, or 6 and 11, or 1 and 11).
- The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Configure the Basic Radio Settings

The radio settings apply to all wireless profiles on the wireless VPN firewall. The default wireless mode is 802.11ng. You can change the wireless mode, country, and many other radio settings on the Radio Settings screen (described in this section) and on the Advanced Wireless screen (see *Configure Advanced Radio Settings* on page 126). The default radio settings should work well for most configurations.

➢ **To configure the basic radio settings:**

1. Select **Network Configuration > Wireless Settings > Radio Settings**. The Radio Settings screen displays:

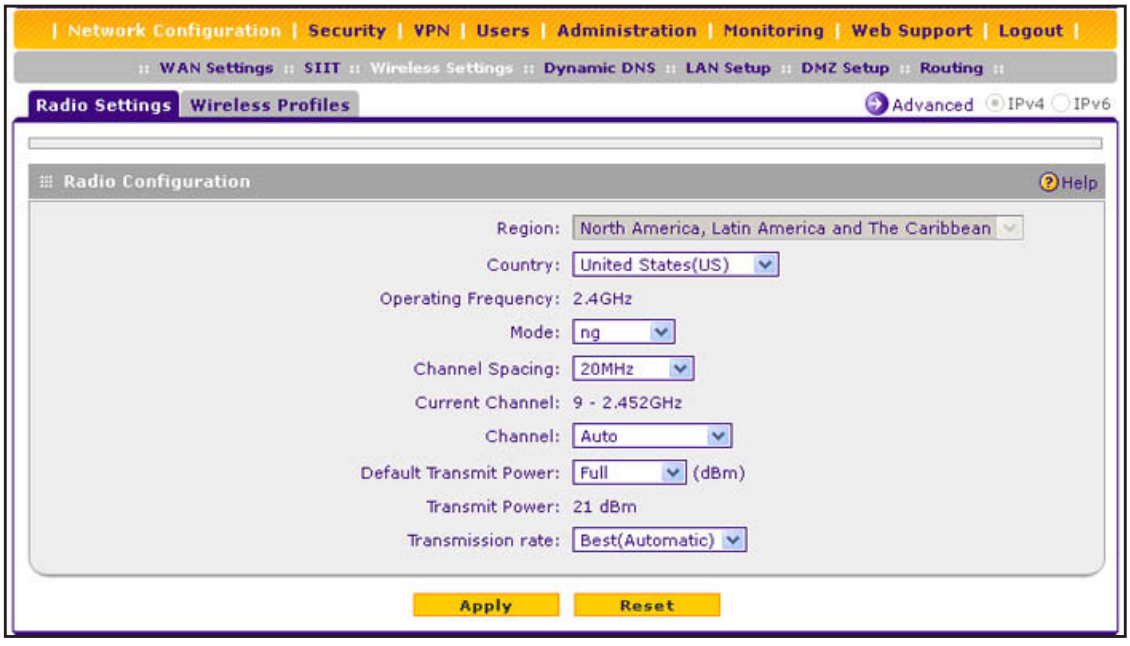

Figure 55.

2. Specify the remaining wireless settings as described the following table:

Table 27. Radio Settings screen settings

Setting	Descriptions
Region	This is a preconfigured field that you cannot change.
Country	Specify the country by making a selection from the drop-down list.
Operating Frequency	This is a nonconfigurable field. The radio's operating frequency is fixed at 2.4 GHz.
Mode	Specify the wireless mode in the 2.4-GHz band by making a selection from the drop-down list: • **g and b**. In addition to 802.11b- and 802.11g-compliant devices, 802.11n-compliant devices can connect to the wireless access point because they are backward compatible. • **g only**. 802.11g- and 802.11n-compliant devices can connect to the wireless access point, but 802.11n-compliant devices function below their capacity in 802.11g mode. 802.11b-compliant devices cannot connect. • **ng**. This is the default setting for most countries. 802.11g- and 802.11n-compliant devices can connect to the wireless access point. 802.11b-compliant devices cannot connect. • **n only**. Only 802.11n-compliant devices can connect to the wireless access point. **Note:** If your network uses 802.11n devices only, configure WPA2 to enable the 802.11n devices to function at full speed.
Channel Spacing	For the ng and n only modes, specify the channel spacing by making a selection from the drop-down list: • **20/40MHz**. Select this option to improve the performance. Some legacy devices (that is, devices that function only in b or g mode) can operate only in 20 MHz. • **20MHz**. Select this option if your network includes legacy devices. This is the default setting. **Note:** The channel spacing is fixed at 20 MHz for the g and b and g only modes.
Current Channel	This is a nonconfigurable field that shows the current channel if you have selected Auto from the Channel drop-down list.
Channel	Specify the channel you wish to use on your wireless LAN by making a selection from the drop-down list. The wireless channels and frequencies depend on the country and wireless mode. The default setting is Auto. **Note:** It should not be necessary to change the wireless channel unless you notice interference in the network (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see *Operating Frequency (Channel) Guidelines* following this table. **Note:** For more information about available channels and frequencies, see *Physical and Technical Specifications* on page 400.

Table 27. Radio Settings screen settings (continued)

Setting	Descriptions
Default Transmit Power	From the drop-down list, select the default transmit power: • **Full**. This is the default setting. • **Half**. • **Quarter**. • **Eighth**. • **Minimum**. If the country regulation does not allow the transmit power that you select, the power is automatically adjusted to the legally allowed power, which is then displayed in the Transmit Power field.
Transmit Power	This is a nonconfigurable field that shows the actual transmit power in dBm.
Transmission rate	Specify the transmission data rate by making a selection from the drop-down list. The default setting is Best (Automatic). **Note:** For information about the available MCS indexes and transmission data rates, see *Physical and Technical Specifications* on page 400.

WARNING:

When you have changed the country settings, the wireless VPN firewall reboots when you click Apply.

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

Operating Frequency (Channel) Guidelines

You should not need to change the operating frequency (channel) unless you notice interference problems, or are setting up the wireless VPN firewall near another wireless access point. Observe the following guidelines:

- Wireless access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available.
- If you are using multiple wireless access points, it is better if adjacent wireless access points use different channels to reduce interference. The recommended channel spacing between adjacent wireless access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).
- In infrastructure mode, wireless devices normally scan all channels, looking for a wireless access point. If more than one wireless access point can be used, the one with the strongest signal is used. This can happen only when the wireless access points use the same SSID. The FVS318N wireless VPN firewall functions in infrastructure mode by default.

Wireless Data Security Options

Indoors, computers can connect over 802.11n wireless networks at a maximum range of 300 feet. Typically, a wireless VPN firewall inside a building works best with devices within a 100 foot radius. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless VPN firewall provides highly effective security features that are covered in detail in this chapter. Deploy the security features appropriate to your needs.

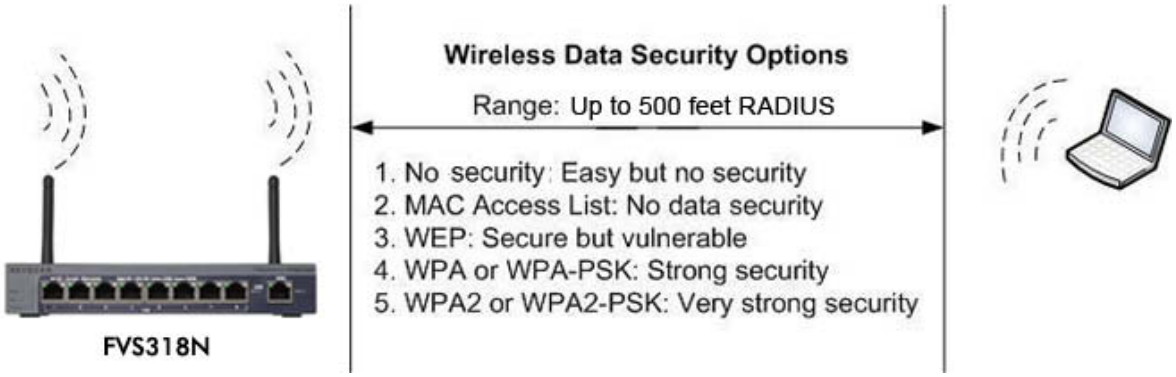

Figure 56.

There are several ways you can enhance the security of your wireless network:

- **Restrict access based by MAC address**. You can allow only trusted computers to connect so that unknown computers cannot wirelessly connect to the wireless VPN firewall. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For information about how to restrict access by MAC address, see *Restrict Wireless Access by MAC Address* on page 121.
- **Turn off the broadcast of the wireless network name (SSID)**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network discovery feature of some products, such as Windows XP, but the data is still exposed. For information about how to turn of broadcast of the SSID, see *Configure and Enable Wireless Profiles* on page 116.
- **WEP**. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP shared key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.

  For information about how to configure WEP, see *Configure and Enable Wireless Profiles* on page 116.

- **WPA**. Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) or a combination of TKIP and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. The wireless VPN firewall supports WPA with a pre-shared key (PSK), RADIUS, or a combination of PSK and RADIUS.

  For more information about how to configure WPA, see *Configure and Enable Wireless Profiles* on page 116.

- **WPA2**. Wi-Fi Protected Access version 2 (WPA2) data encryption provides strong data security with CCMP encryption or a combination of TKIP and CCMP encryption. WPA2 provides the most reliable security. Use WPA2 only if all clients in your network support WPA2. The wireless VPN firewall supports WPA2 with PSK, RADIUS, or a combination of PSK and RADIUS.

  For more information about how to configure WPA2, see *Configure and Enable Wireless Profiles* on page 116.

- **WPA+WPA2 mixed mode**. This mode supports data encryption with a combination of TKIP and CCMP for both WPA and WPA2 clients. The very strong authentication along with dynamic per frame rekeying of WPA2 make it virtually impossible to compromise. The wireless VPN firewall supports WPA+WPA2 with PSK, RADIUS, or a combination of PSK and RADIUS.

  For more information about how to configure WPA+WPA2 mixed mode, see *Configure and Enable Wireless Profiles* on page 116.

Note: TKIP provides only legacy (slower) rates of operation. To use 802.11n rates and speed, NETGEAR recommends WPA2 with CCMP.

Wireless Security Profiles

Wireless security profiles, hereafter referred to as wireless profiles, let you configure unique security settings for each SSID on the wireless VPN firewall. The wireless VPN firewall supports up to four wireless profiles (BSSIDs) that you can configure from the Wireless Profiles screen (see *Configure and Enable Wireless Profiles* on page 116).

Each wireless profile provides the following features:

- Capability to turn off the wireless profile during scheduled vacations and office shutdowns, on evenings, or on weekends. This a green feature that allows you to save energy.
- WLAN partitioning to prevent associated wireless clients (using the same wireless profile) from communicating with each other. This feature is useful for hotspots and other public access situations.
- MAC address access control list that lets you add another level of security.
- Capability to monitor the clients that are connected to the SSID of the wireless profile.

To set up a wireless profile, specify a name for the profile and the SSID, specify the type of security with authentication and data encryption, and specify whether the SSID is broadcast.

- **Network authentication**
  The wireless VPN firewall is set by default as an open system with no authentication. When you configure network authentication, bear in mind that older wireless adapters might not support WPA or WPA2. Windows XP, Windows 2000 with Service Pack 3, Windows Vista, and Windows 7 do include the client software that supports WPA. However, client software is required on the client. For information about configuring WPA2 settings, see the product documentation for your wireless adapter and WPA or WPA2 client software.

  For information about the types of network authentication that the wireless VPN firewall supports, see *Configure and Enable Wireless Profiles* on page 116.

- **Data encryption**
  Select the data encryption that you want to use. The available options depend on the network authentication setting described earlier (otherwise, the default is None). The data encryption settings are described in *Configure and Enable Wireless Profiles* on page 116.

Some concepts and guidelines regarding the SSID are:

- A basic service set (BSS) is a group of wireless devices and a single wireless access point, all using the same wireless profile or service set identifier (BSSID). The actual identifier in the BSSID is the MAC address of the wireless radio. (A wireless radio can have multiple MAC addresses, one for each wireless profile.)
- An extended service set (ESS) is a group of wireless devices, all using the same identifier (ESSID).
- Different devices within an ESS can use different channels. To reduce interference, adjacent devices should use different channels.
- Roaming is the ability of wireless devices to connect wirelessly when they physically move from one BSS to another one within the same ESS. The wireless device automatically changes to the wireless access point with the least interference or best performance.

Before You Change the SSID, WEP, and WPA Settings

For a new wireless network, print or copy the following form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the Country/Region correctly as the first step.

Store this information in a safe place:

- **SSID**
  The service set identifier (SSID) identifies the wireless local area network. You can customize it by using up to 32 alphanumeric characters. Write your SSID on the line.

  SSID: _____

  The SSID in the wireless access point is the SSID you configure on the wireless adapter card. All wireless nodes in the same network need to be configured with the same SSID.

- **WEP key size, key format, authentication type, and passphrase**
  Choose the key size by circling one: 64 or 128 bits.
  Choose the key format by circling one: ASCII or HEX.
  Choose the authentication type by circling one: Open or Shared.

  Passphrase: _____

  Note: If you select shared key, the other devices in the network cannot connect unless they are set to shared key and have the same keys in the same positions as those in the wireless VPN firewall.

- **WPA-PSK (Pre-Shared Key) and WPA2-PSK**
  Record the WPA-PSK passphrase:

  WPA-PSK passphrase: _____

  Record the WPA2-PSK passphrase:

  WPA2-PSK passphrase: _____

- **WPA RADIUS settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary _____ Secondary _____

  Port: _____

  Shared secret: _____

- **WPA2 RADIUS settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary _____ Secondary _____

  Port: _____

  Shared secret: _____

Configure and Enable Wireless Profiles

➢ **To add a wireless profile:**

1. Select **Network Configuration > Wireless Settings > Wireless Profiles**. The Wireless Profiles screen displays. (The following figure shows some examples.)

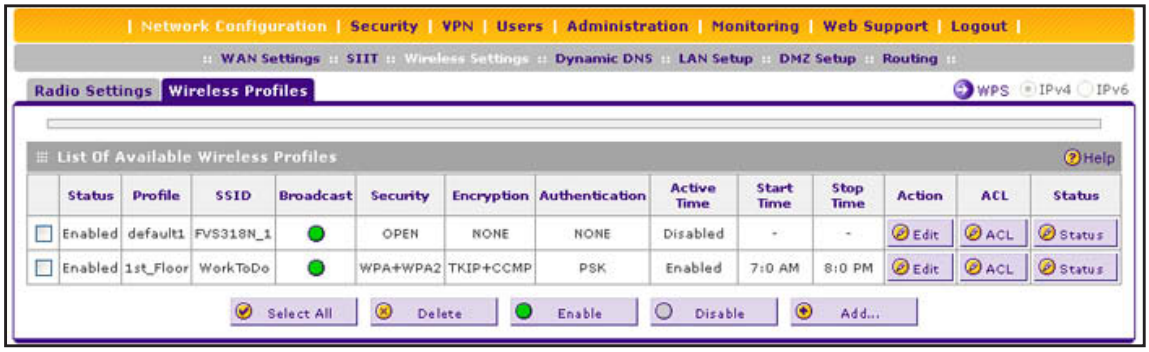

Figure 57.

The following table explains the fields of the Wireless Profiles screen:

Table 28. Wireless Profiles screen settings

Setting	Description
Status	The status of the profile: Enabled or Disabled.
Profile	The unique name of the wireless profile that makes it easy to recognize the profile.
SSID	The wireless network name (SSID) for the wireless profile.
Broadcast	Indicates whether the SSID is broadcast. A green circle indicates that the SSID is broadcast; a gray circle indicates that it is not.
Security	The configured security method for the wireless profile.
Encryption	The configured encryption method for the wireless profile.
Authentication	The configured authentication method for the wireless profile.
Active Time	Indicates whether the timer for the wireless profile is activated (Yes or No).
Start Time	The start time for the timer.
Stop Time	The stop time for the timer.

2. Under the List of Profiles table, click the **Add** table button. The Add Wireless Profiles screen displays:

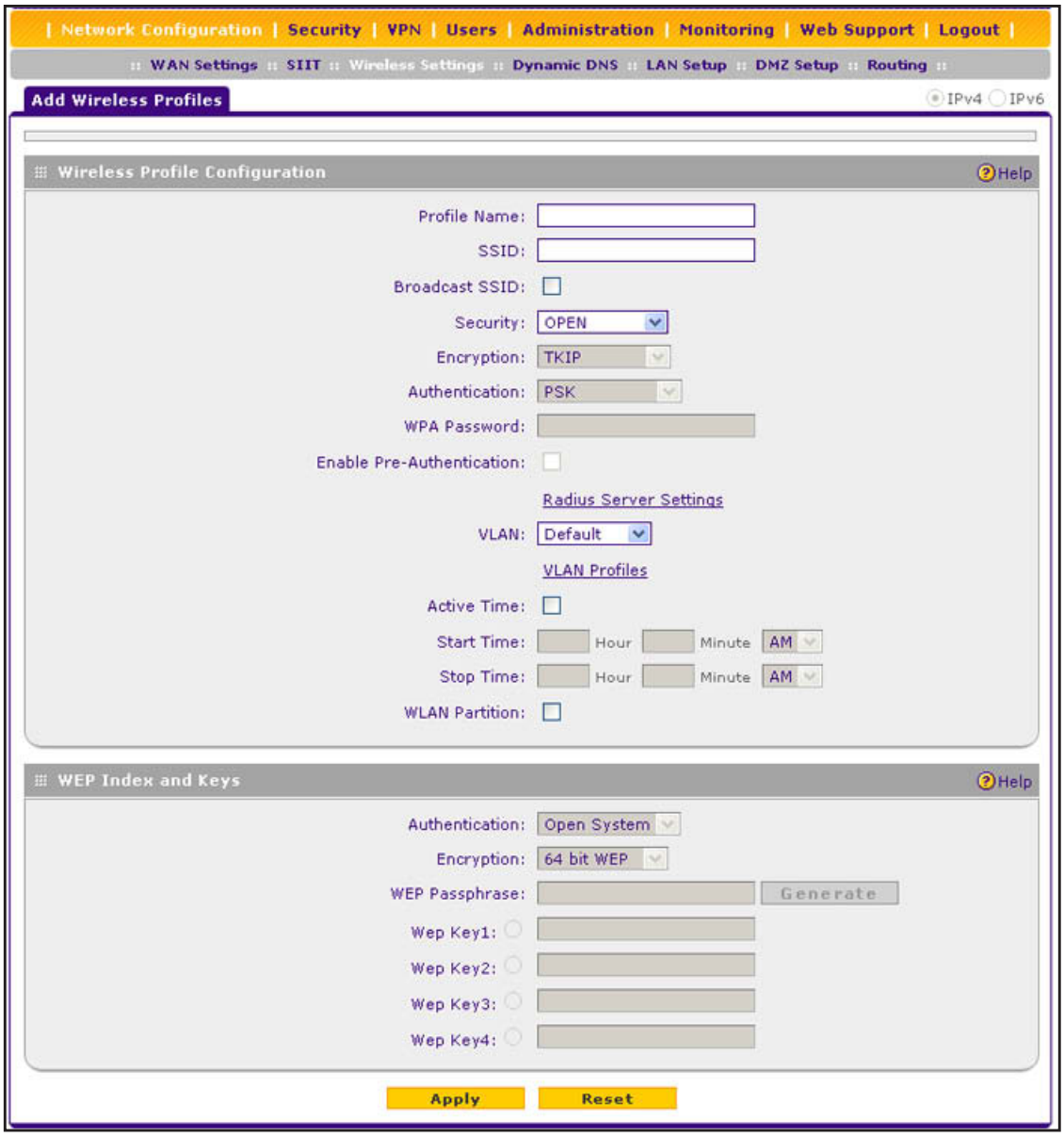

Figure 58.

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

Table 29. Add Wireless Profiles screen settings

Setting	Description
Wireless Profile Configuration	
Profile Name	The name for the default wireless profile is default1. You cannot change this name. For additional profiles, enter a unique name to make it easy to recognize the profile. You can enter a name of up to 32 alphanumeric characters.

Table 29. Add Wireless Profiles screen settings (continued)

Setting	Description
SSID	The wireless network name (SSID) for the wireless profile. The default SSID name is FVS318N_1. You can change this name by entering up to 32 alphanumeric characters. Make sure that additional SSIDs have unique names.
Broadcast SSID	Select the check box to enable the wireless VPN firewall to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless VPN firewall's SSID. To prevent the SSID from being broadcast, clear the check box.
Security	**Note:** Before you configure security, you might want to read *Wireless Data Security Options* on page 112. Specify the wireless security by making a selection from the drop-down list: • **OPEN**. This is the default setting. An open system has no authentication and no encryption, and therefore no security configuration. However, you *can* use an open system with encryption. To do so, select **WEP** from the Security drop-down list. In the WEP Index and Keys section of the screen, take the following steps: - Select **Open System** authentication. - Select the encryption. - Enter a passphrase and generate a key, or enter a key manually. • **WEP**. To configure WEP, take the following steps in the WEP Index and Keys section of the screen: - Select **Shared Key** authentication. - Select the encryption. - Enter a passphrase and generate a key, or enter a key manually. • **WPA**. To configure WPA, select the encryption and authentication. The remaining configuration depends on the selected authentication: - For WPA-PSK, select a password. - For WPA with RADIUS, configure the RADIUS server settings. - For WPA with PSK+RADIUS, select a password and configure the RADIUS server settings. • **WPA2**. To configure WPA2, select the encryption and authentication. The remaining configuration depends on the selected authentication: - For WPA2-PSK, select a password. - For WPA2 with RADIUS, configure the RADIUS server settings. As an option, you can enable RADIUS preauthentication. - For WPA2 with PSK+RADIUS, select a password and configure the RADIUS server settings. As an option, you can enable RADIUS preauthentication. • **WPA+WPA2**. To configure WPA, select the encryption and authentication. The remaining configuration depends on the selected authentication: - For WPA+WPA2 with PSK, select a password. - For WPA+WPA2 with RADIUS, configure the RADIUS server settings. - For WPA+WPA2 with PSK+RADIUS, select a password and configure the RADIUS server settings.

Table 29. Add Wireless Profiles screen settings (continued)

Setting	Description
Encryption **Note:** WPA, WPA2, and WPA+WPA2 only.	The encryption that you can select depends on the type of WPA security that you have selected: • **WPA**. You can select the following encryption from the drop-down list: - **TKIP** - **TKIP+CCMP** • **WPA2**. You can select the following encryption from the drop-down list: - **CCMP** - **TKIP+CCMP** • **WPA+WPA2**. The encryption is TKIP+CCMP.
Authentication **Note:** WPA, WPA2, and WPA+WPA2 only.	For WPA, WPA2, and WPA+WPA2 only, specify the authentication by making a selection from the drop-down list: • **PSK** • **RADIUS** • **PSK+RADIUS**
WPA Password **Note:** WPA, WPA2, and WPA+WPA2 only.	For WPA, WPA2, and WPA+WPA2 only, if you have selected PSK or PSK+RADIUS authentication, enter a pre-shared key or password.
Enable Pre-Authentication **Note:** WPA2 only.	For WPA2 only, if you have selected RADIUS authentication, configure preauthentication by selecting the check box. Preauthentication allows a client to roam from one access point to another access point without having to be reauthenticated.
Radius Server Settings **Note:** WPA, WPA2, and WPA+WPA2 only.	For WPA, WPA2, and WPA+WPA2 only, if you have selected RADIUS or PSK+RADIUS authentication, click the **Radius Server Settings** link to configure the RADIUS settings (see *RADIUS Client and Server Configuration* on page 241).
VLAN	From the drop-down list, select the VLAN to which the wireless profile should be allocated.
VLAN Profiles	Click the **VLAN Profiles** link to configure a VLAN profile (see *Configure a VLAN Profile* on page 60).
Active Time	To enable the timer, select the **Active Time** check box. When the timer is enabled, the wireless profile is turned off from the start time until the stop time. To disable the timer, clear the check box.
Start Time	Specify the start hour in the Hours field and the start minute in the Minutes field, and select **AM** or **PM** from the drop-down list.
Stop Time	Specify the stop hour in the Hours field and the stop minute in the Minutes field, and select **AM** or **PM** from the drop-down list.
WLAN Partition	To enable wireless client separation and prevent wireless clients that are connected to this wireless profile from communicating with each other, select the **WLAN Partition** check box. To disable wireless client separation, clear the check box. By default, WLAN partition is disabled.

Table 29. Add Wireless Profiles screen settings (continued)

Setting	Description
WEP Index and Keys	
Authentication	Specify the authentication by making a selection from the drop-down list: • **Open System**. Select this option to use WEP encryption without authentication. • **Shared Key**. Select this option to use WEP authentication and encryption with a shared key (passphrase).
Encryption	Select the encryption key size by making a selection from the drop-down list: • **64-bit WEP**. Standard WEP encryption, using 40/64-bit encryption. • **128-bit WEP**. Standard WEP encryption, using 104/128-bit encryption.
Passphrase	Enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive). The secret passphrase allows you to automatically generate the keys by clicking **Generate**.
Encryption Key (Key1–Key4)	Specify the active key by selecting one of the four radio buttons. Only one key can be the active key. Either enter a key manually or generate the key automatically by clicking **Generate**. The length of the key depends on the selected encryption: • **64-bit WEP**. A key length of 5 ASCII or 10 hexadecimal characters. • **128-bit WEP**. A key length of 13 ASCII or 26 hexadecimal characters. **Note:** Wireless stations need to use the key to access the wireless VPN firewall.

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

WARNING:

If you use a wireless computer to configure wireless security settings, you are disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the wireless VPN firewall from a wired computer to make further changes.

Note: For information about how to configure WPS, see *Configure Wi-Fi Protected Setup* on page 124.

➢ **To edit a wireless profile:**

1. On the Wireless Profiles screen (see *Figure 57* on page 116), click the **Edit** button in the Action column for the wireless profile that you want to modify. The Edit Profiles screen displays. This screen is identical to the Add Profiles screen.

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

Note: If WPS is enabled for the wireless profile, first disable WPS before you edit the wireless profile.

➢ **To delete one or more wireless profiles:**

1. On the Wireless Profiles screen (see *Figure 57* on page 116), select the check box to the left of each wireless profile that you want to delete, or click the **Select All** table button to select all wireless profiles. (You cannot select the default wireless profile.)
2. Click the **Delete** table button.

Note: If WPS is enabled for the wireless profile, first disable WPS before you delete the wireless profile.

➢ **To enable or disable one or more wireless profiles:**

1. On the Wireless Profiles screen (see *Figure 57* on page 116), select the check box to the left of each wireless profile that you want to enable or disable, or click the **Select All** table button to select all wireless profiles.
2. Click one of the following table buttons:
   - **Enable**. Enables the wireless profile or wireless profiles and allows wireless clients to make a connection.
   - **Disable**. Disables the wireless profile or wireless profiles and prevents wireless clients from making a connection.

Restrict Wireless Access by MAC Address

For increased security, you can restrict access to an SSID by allowing access to only specific computers or wireless stations based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the wireless VPN firewall. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

Note: For wireless adapters, you can usually find the MAC address printed on the wireless adapter.

➢ **To allow or restrict access based on MAC addresses:**

1. On the Wireless Profiles screen (see *Figure 57* on page 116), click the **ACL** button in the ACL column for the wireless profile for which you want to set up access control. The MAC Address Filtering screen displays. (The following figure shows some examples.)

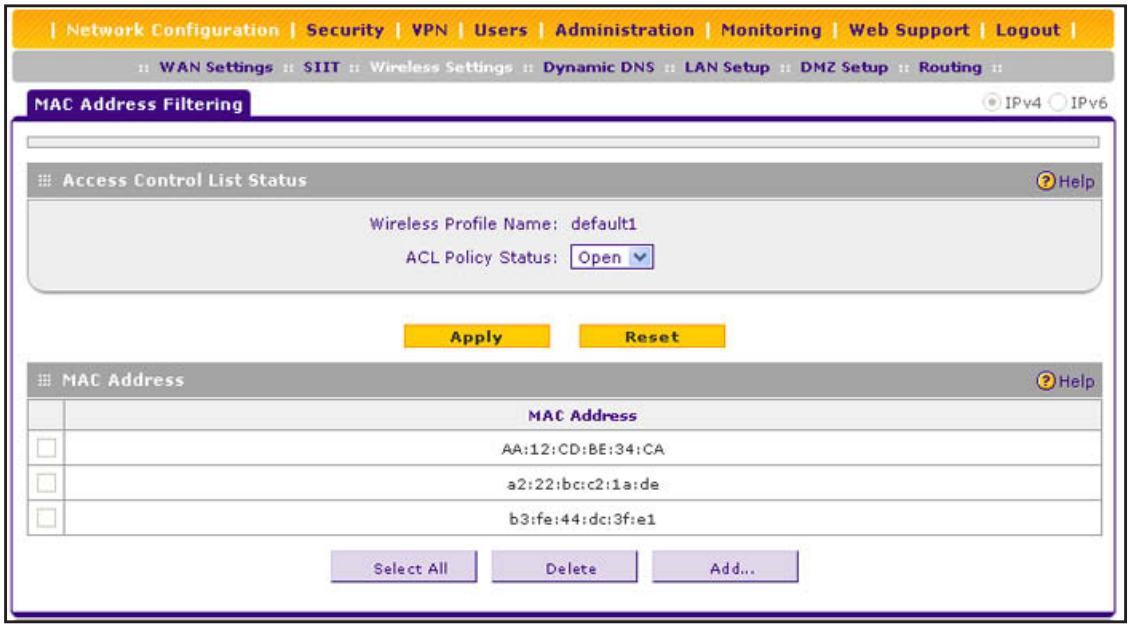

Figure 59.

2. Click **Add** to open the MAC Address screen (not shown in this manual).
3. Enter a MAC address in the MAC Address field.
4. Click **Apply** to add the MAC address to the MAC Address table on the MAC Address Filtering screen.
5. Repeat *Step 2* through *Step 4* for any other MAC address that you want to add to the MAC Address table.
6. From the ACL Policy Status drop-down list, select if access control is enabled, and if so, how the MAC addresses in the MAC Address table are treated:
   - **Open**. Access control is disabled. All MAC addresses, including the ones in the MAC Address table, are allowed access.
   - **Allow**. Only the MAC addresses in the MAC Address table are allowed access. All other MAC addresses are denied access.
   - **Deny**. The MAC addresses in the MAC Address table are denied access. All other MAC addresses are allowed access.
7. Click **Apply** to save your settings.

WARNING:

When you configure the wireless VPN firewall from a wireless computer whose MAC address is not in the access control list and when the ACL policy status is set to deny access, you lose your wireless connection when you click Apply. You then need to access the wireless VPN firewall from a wired computer or from a wireless computer that is on the access control list to make any further changes.

➢ **To remove one or more MAC addresses from the table:**

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

View the Status of a Wireless Profile

➢ **To view the status of a specific wireless profile:**

On the Wireless Profiles screen (see *Figure 57* on page 116), click the **Status** button in the Status column for the wireless profile for which you want to display the status information. The Wireless Profile Status screen displays:

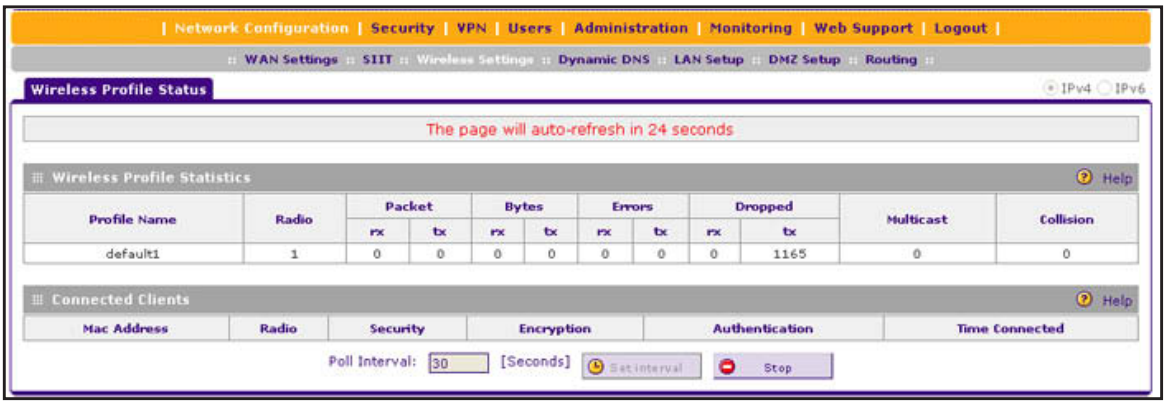

Figure 60.

To change the poll interval period, enter a new value in the Poll Interval field, and click **Set interval**. To stop polling, click **Stop**.

The following table explains the fields of the Wireless Profile Status screen.

Table 30. Wireless Profile Status screen fields

Item	Description
Wireless Profile Statistics	
Profile Name	The name of the wireless profile.
Radio	The radio to which the client is connected. By default, the radio is always 1, indicating the 2.4 GHz radio.
Packet	The number of received (rx) and transmitted (tx) packets on the access point in bytes.
Bytes	The number of received (rx) and transmitted (tx) bytes on the access point.
Errors	The number of received (rx) and transmitted (tx) errors on the access point.
Dropped	The number of received (rx) and transmitted (tx) dropped packets on the access point.
Multicast	The number of received (rx) and transmitted (tx) multicast packets on the access point.
Collisions	The number of signal collisions that occurred on the access point. A collision occurs when the access point attempts to send data at the same time as a wireless station that is connected to the access point.
Connected Clients	
MAC Address	The MAC address of the client.
Radio	The radio to which the client is connected. By default, the radio is always 1, indicating the 2.4 GHz radio.
Security	The type of security that the client is using (Open, WEP, WPA, WPA2, or WPA+WPA2).
Encryption	The type of encryption that the client is using (CCMP, TKIP, or TKIP + CCMP).
Authentication	The type of authentication that the client is using (Open, PSK, RADIUS, or PSK+RADIUS).
Time Connected	The period in minutes since the connection was established between the access point and the client.

Configure Wi-Fi Protected Setup

Push 'N' Connect using Wi-Fi Protected Setup™ (WPS) allows you to connect computers to a secure wireless network with WPA or WPA2 wireless security. The wireless VPN firewall automatically sets security for each computer or device that uses WPS to join the wireless network. To use WPS, make sure that your wireless devices are Wi-Fi certified and support WPS. NETGEAR products that use WPS call it Push 'N' Connect.

You can use a WPS button or the wireless router interface method to add wireless computers and devices to your wireless network.

Note: For a list of other Wi-Fi-certified products available from NETGEAR, go to *http://www.wi-fi.org*.

➢ **To enable WPS and initiate the WPS process on the wireless VPN firewall:**

1. Select **Network Configuration > Wireless Settings > Wireless Profiles**. The Wireless Profiles screen displays (see *Figure 57* on page 116).
2. On the Wireless Profiles screen, to the right of the Wireless Profiles tab, click the **WPS** option arrow. The WPS screen displays:

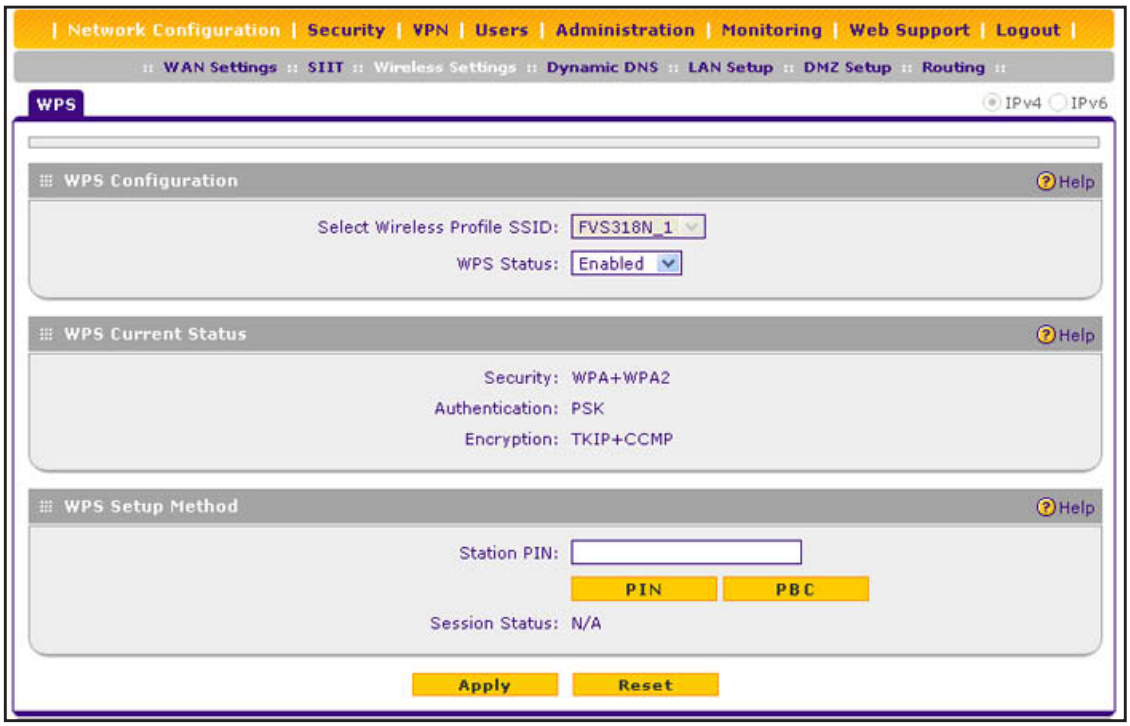

Figure 61.

3. From the Select Wireless Profile SSID drop-down list, select the name of the SSID for which you want to enable WPS. The wireless profile with which the SSID is associated needs to be configured for WPA, WPA, or WPA+WPA2 security in order to be displayed as a selection in the drop-down list.
4. From the WPS Status drop-down list, select **Enabled** to enable the WPS feature.
5. Click **Apply** to save your changes.

Note: *The Security, Authentication, and Encryption fields are nonconfigurable fields that are for information only.*

6. In the WPS Setup Method section of the screen, use one of the following methods to initiate the WPS process for a wireless device:
   - PIN method:
     a. Collect the pin of the wireless device.
     b. In the Station PIN field, enter the pin.
     c. Click the **PIN** button.
   - Push button configuration (PBC) method:
     a. Click the **PBC** button.
     b. Within two minutes, press the **WPS** button on your wireless device to enable the device to connect to the wireless VPN firewall, or follow the WPS instructions that came with the device.

   With either method, the wireless VPN firewall tries to communicate with the wireless device, set the wireless security for the wireless device, and allow it to join the wireless network.

Note: There is no physical WPS push button on the wireless VPN firewall.

Configure Advanced Radio Settings

➢ **To configure advanced radio settings:**

1. Select **Network Configuration > Wireless Settings > Radio Settings**. The Radio Settings screen displays (see *Figure 55* on page 109).
2. On the Radio Settings screen, to the right of the Wireless Profiles tab, click the **Advanced** option arrow. The Advanced Wireless screen displays:

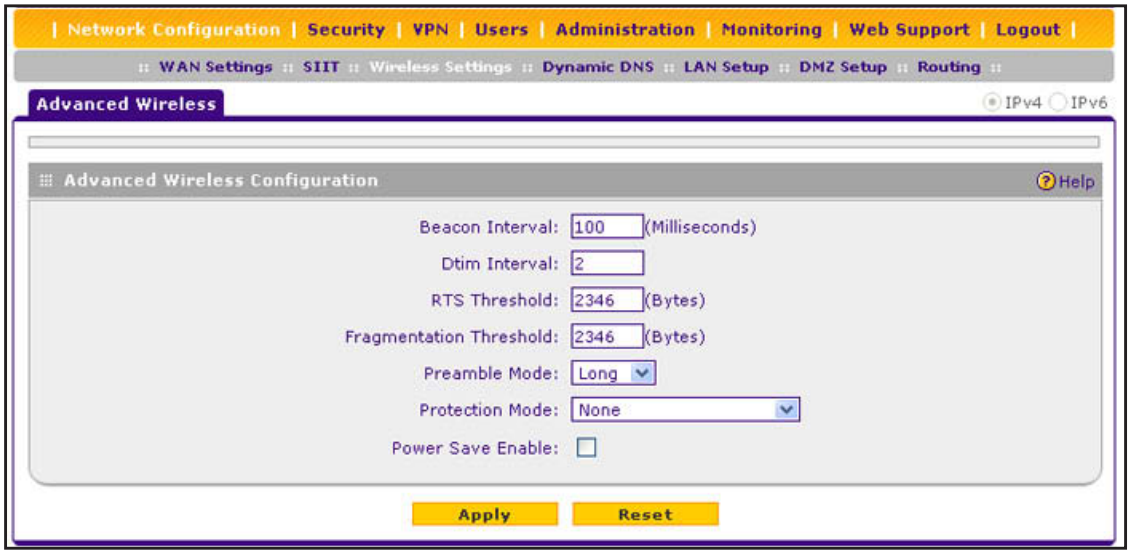

Figure 62.

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

Table 31. Advanced Wireless screen settings

Setting	Description
Beacon Interval	Enter an interval between 40 ms and 3500 ms for each beacon transmission, which allows the wireless VPN firewall to synchronize the wireless network. The default setting is 100.
DTIM Interval	Enter the Delivery Traffic Indication Message (DTIM) interval, also referred to as the data beacon rate, which indicates the period for the beacon DTIM in multiples of beacon intervals. This value needs to be between 1 and 255. The default setting is 2.
RTS Threshold	Enter the Request to Send (RTS) threshold. The default setting is 2346 bytes. If the packet size is equal to or less than the RTS threshold, the wireless VPN firewall uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism, and the data frame is transmitted immediately after the silence period. If the packet size is larger than the RTS threshold, the wireless VPN firewall uses the CSMA with Collision Avoidance (CSMA/CA) mechanism. In this situation, the transmitting station sends an RTS packet to the receiving station, and waits for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data. This method improves the performance but reduces the throughput.
Fragmentation Threshold	Enter the maximum packet size that is used for the fragmentation of data packets. Packets that are larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation threshold needs to be an even number. The default setting is 2346 bytes.
Preamble Mode	Specify the preamble mode by making a selection from the drop-down list: • **Long**. A long transmit preamble might provide a more reliable connection or a slightly longer range. This is the default mode. • **Short**. A short transmit preamble gives better performance.
Protection Mode	Specify the Clear to Send (CTS)-to-self protection mode by making a selection from the drop-down list: • **None**. CTS-to-self protection mode is disabled. This is the default mode. • **CTS-to-Self-Protection**. CTS-to-self protection mode is enabled. This mode increases the performance but reduces the throughput slightly.
Power Save Enable	To enable the Wi-Fi Multimedia (WMM) Powersave feature, select the **Power Save Enable** check box. This feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission. Clear the check box to disable the feature, which is the default setting.

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

Test Basic Wireless Connectivity

After you have configured the wireless VPN firewall as described in the previous sections, test your wireless clients for wireless connectivity before you place the wireless VPN firewall at its permanent position.

➢ **To test for wireless connectivity:**

1. Configure the 802.11b/g/n wireless clients so that they all have the same SSID that you have configured on the wireless VPN firewall. Make sure that the wireless mode on the wireless VPN firewall supports the wireless capacity of the wireless clients. (For example, 802.11b-compliant devices cannot connect to the wireless VPN firewall if the wireless mode is set to ng.)
2. Verify that your wireless clients have a link to the wireless VPN firewall. If you have enabled the DHCP server on the wireless VPN firewall (see *Configure a VLAN Profile* on page 60 (for IPv4) and *Manage the IPv6 LAN* on page 74), verify that your wireless clients are able to obtain an IP address through DHCP from the wireless VPN firewall.
3. Verify network connectivity by using a browser such as Internet Explorer 7.0 or later or Mozilla Firefox 4.0 or later to browse the Internet, or check for file and printer access on your network.

If you have trouble connecting to the wireless VPN firewall, try to connect without security by selecting **OPEN** from the Security drop-down list on the Edit Wireless Profiles screen for the profile that you are using. If that does not help you to solve the connection problem, see *Chapter 11, Troubleshooting*.

Firewall Protection

5

This chapter describes how to use the firewall features of the wireless 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 68.

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 298 and *Configure Remote Management Access* on page 333).
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 131), you can further refine your control using the following features and capabilities of the wireless VPN firewall:
   - Groups and hosts (see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 68)
   - Services (see *Outbound Rules (Service Blocking)* on page 132 and *Inbound Rules (Port Forwarding)* on page 134)
   - Schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 183)
   - Allowing or blocking sites (see *Configure Content Filtering* on page 179)
   - Source MAC filtering (see *Enable Source MAC Filtering* on page 184)
   - Port triggering (see *Configure Port Triggering* on page 190)
3. Some firewall settings might affect the performance of the wireless VPN firewall. For more information, see *Performance Management* on page 325.
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 352.

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 800 firewall rules on the wireless 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 wireless 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 wireless 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 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 173).
- **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 *Preconfigured Quality of Service Profiles* on page 178).

- **Bandwidth profiles**. After you have a configured a bandwidth profile (see *Create Bandwidth Profiles* on page 176), you can assign it to a rule.

Outbound Rules (Service Blocking)

The wireless 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 184 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 66* on page 142, *Figure 72* on page 149, and *Figure 78* on page 156).

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 173).	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 183).	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 69).Groups are applicable only to IPv4 rules.	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.	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
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 wireless VPN firewall marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Preconfigured Quality of Service Profiles* on page 178. **Note:** The wireless VPN firewall has preconfigured default QoS profiles; you cannot configure the QoS profiles. A QoS profile can become active only when you apply it to a nonblocking inbound or outbound firewall rule.	LAN WAN rules DMZ WAN rules

Table 33. Outbound rules overview (continued)

Setting	Description	Outbound 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 176. 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 should be assigned the address of the WAN interface or the address of a different interface. You can specify these settings only for outbound traffic of the WAN interface. The options are: • **WAN Interface Address**. All the outgoing packets on the WAN are assigned to the address of the specified WAN interface. • **Single Address**. All the outgoing packets on the WAN are assigned to the specified IP address, for example, a secondary WAN address that you have configured. **Note:** The NAT IP 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 28.) 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 36).
- 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 73).
- 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 190 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Note: The wireless 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 167), multiple concurrent connections of the same application from one host or IP address (such as multiple DNS queries from one computer) trigger the wireless 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 68* on page 145, *Figure 74* on page 152, and *Figure 80* on page 158).

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 173).	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 183).	All rules when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action.
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 enable this setting and specify a port number. If the service is using the default port, you do not need to enable 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

Table 34. Inbound rules overview (continued)

Setting	Description	Inbound 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 69). Groups are applicable only to IPv4 rules. **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
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.	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
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 176. 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:

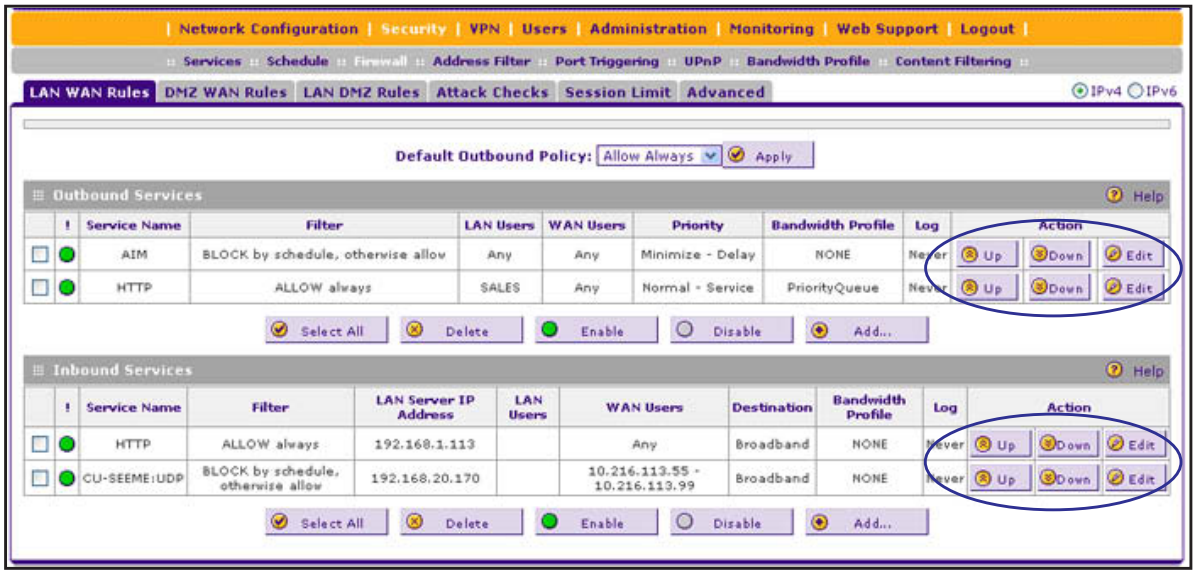

Figure 63.

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

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 wireless 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.)

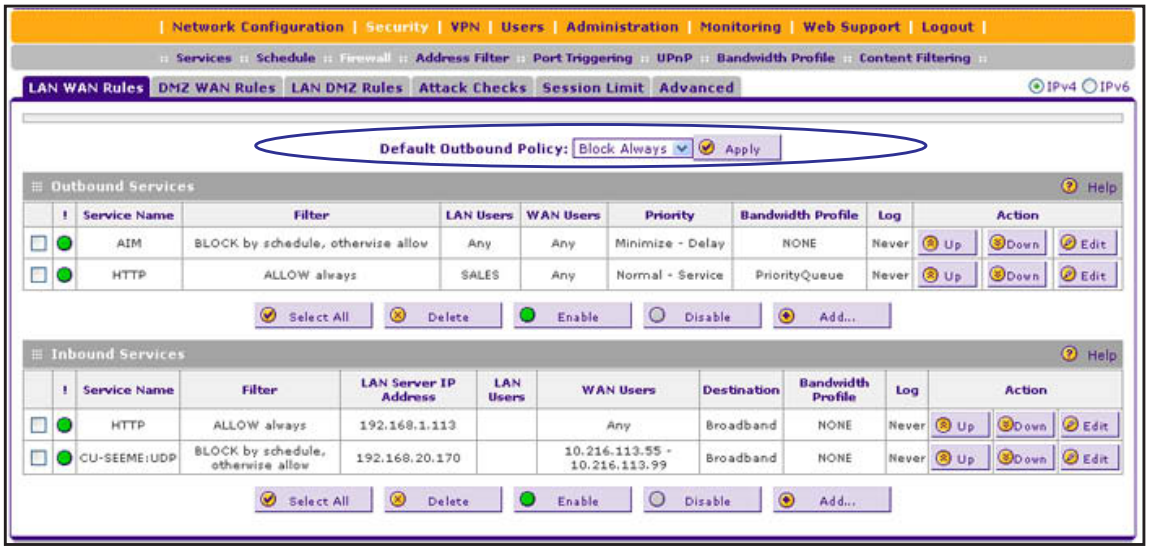

Figure 64.

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**. Allows you to 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 66* on page 142)
  - Edit LAN WAN Inbound Service screen for IPv4 (identical to *Figure 68* on page 145)

➢ **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.)

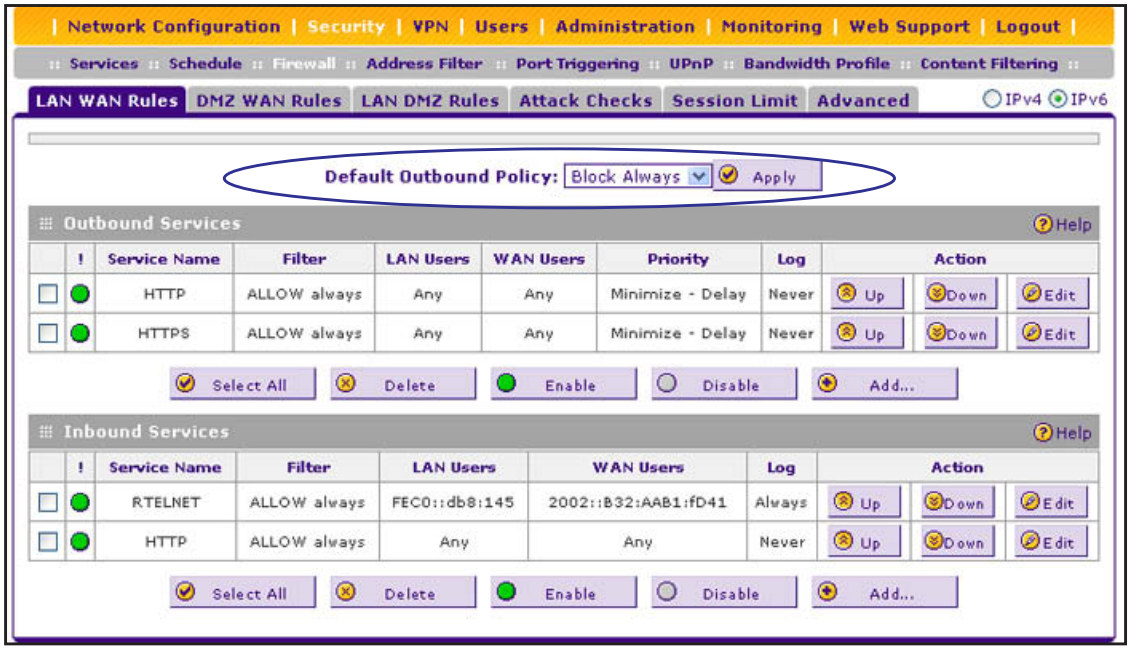

Figure 65.

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**. Allows you to 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 67* on page 143)
  - Edit LAN WAN Inbound Service screen for IPv6 (identical to *Figure 69* on page 146)

➢ **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 130).

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 64* on page 139).

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

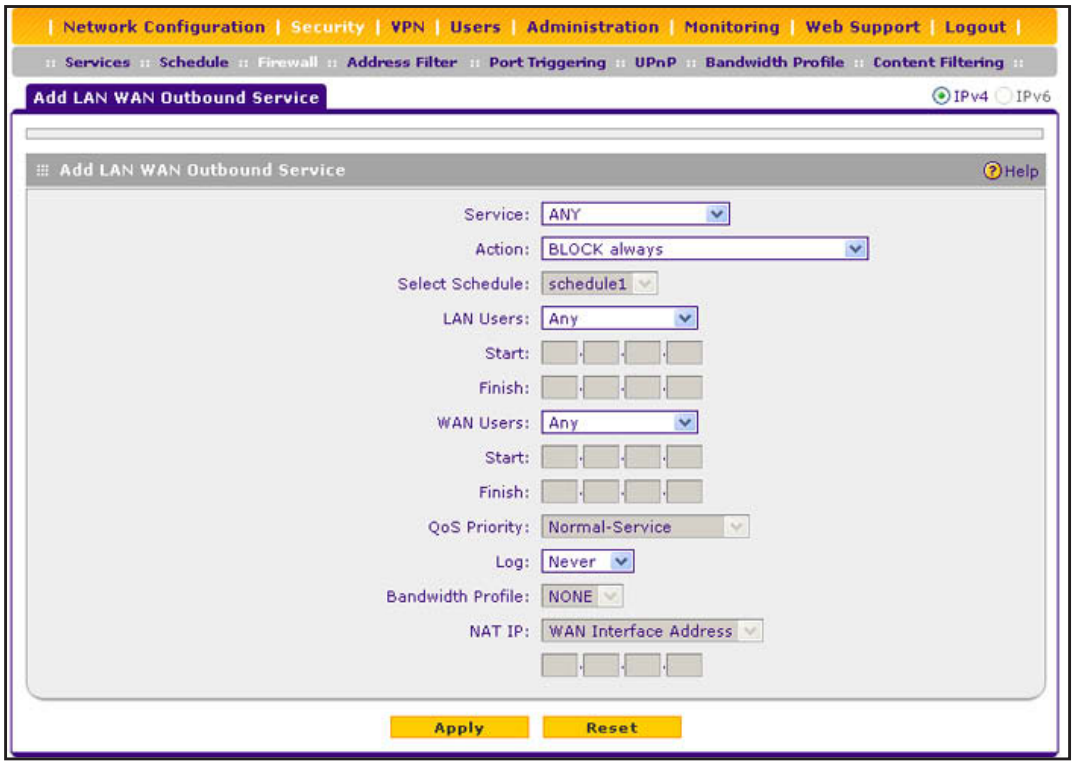

Figure 66.

2. Enter the settings as described in *Table 33* on page 132. 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 Priority
   - Bandwidth Profile
   - NAT IP (This 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.)
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 65* on page 140).
2. Click the **Add** table button under the Outbound Services table. The Add LAN WAN Outbound Service screen for IPv6 displays:

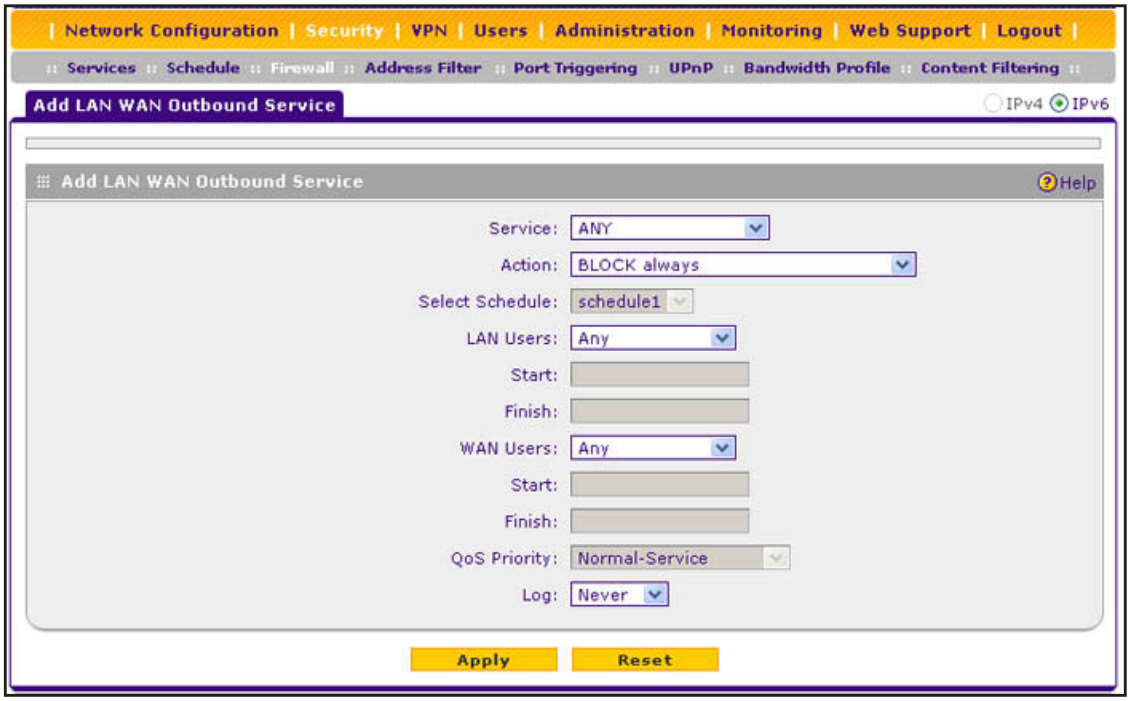

Figure 67.

3. Enter the settings as described in *Table 33* on page 132. 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. Only 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 wireless 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 64* on page 139).

   Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen for IPv4 displays (see the next figure).

2. Enter the settings as described in *Table 34* on page 136. 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 configuration is optional:

   - Translate to Port Number
   - Bandwidth Profile
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

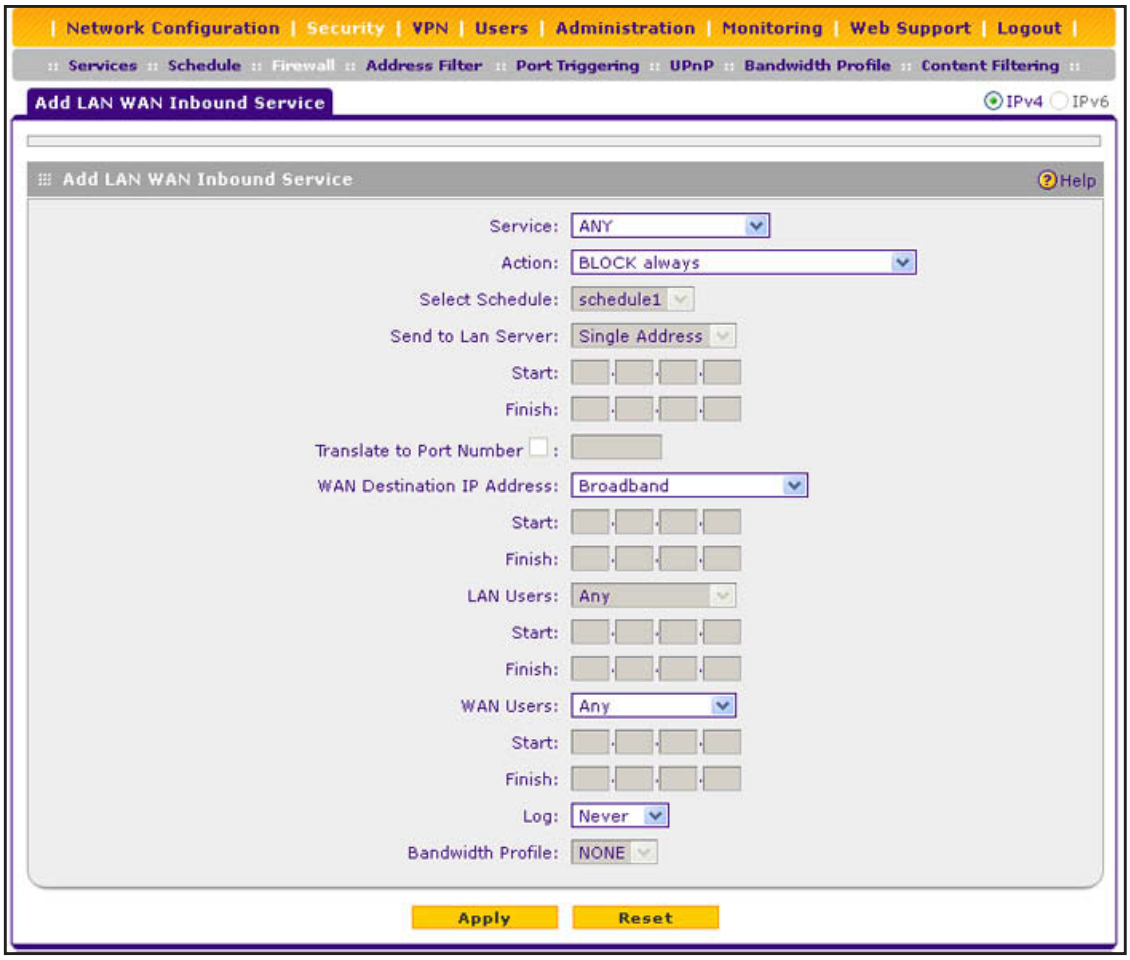

Figure 68.

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 65* on page 140).
2. Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen for IPv6 displays:

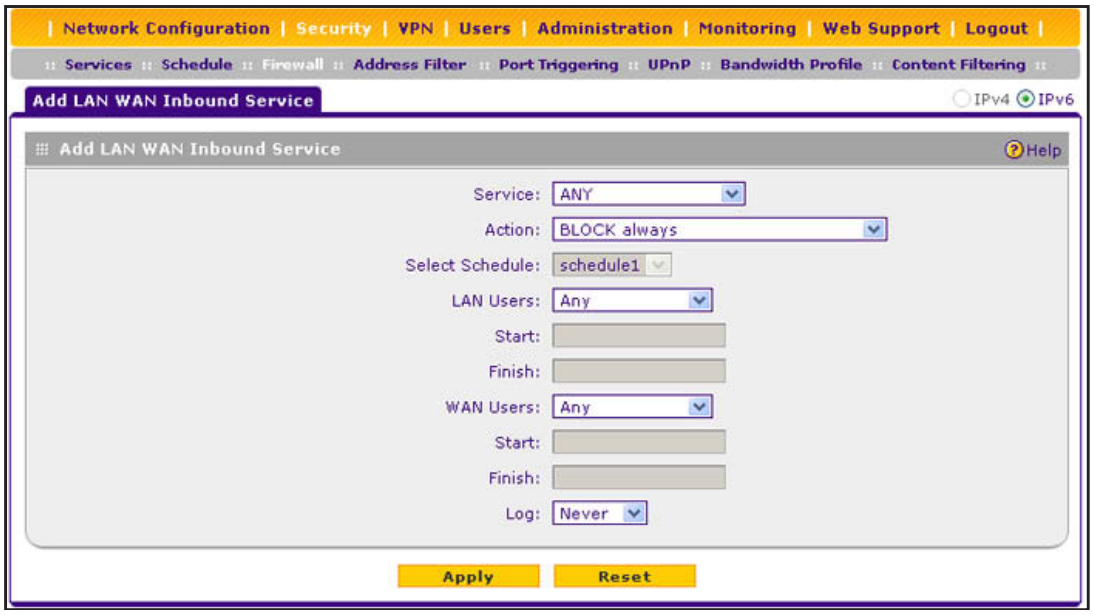

Figure 69.

3. Enter the settings as described in *Table 34* on page 136. 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 DMZ 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 wireless VPN firewall. You do so by adding outbound services rules (see *Create DMZ WAN Outbound Service Rules* on page 149).

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.)

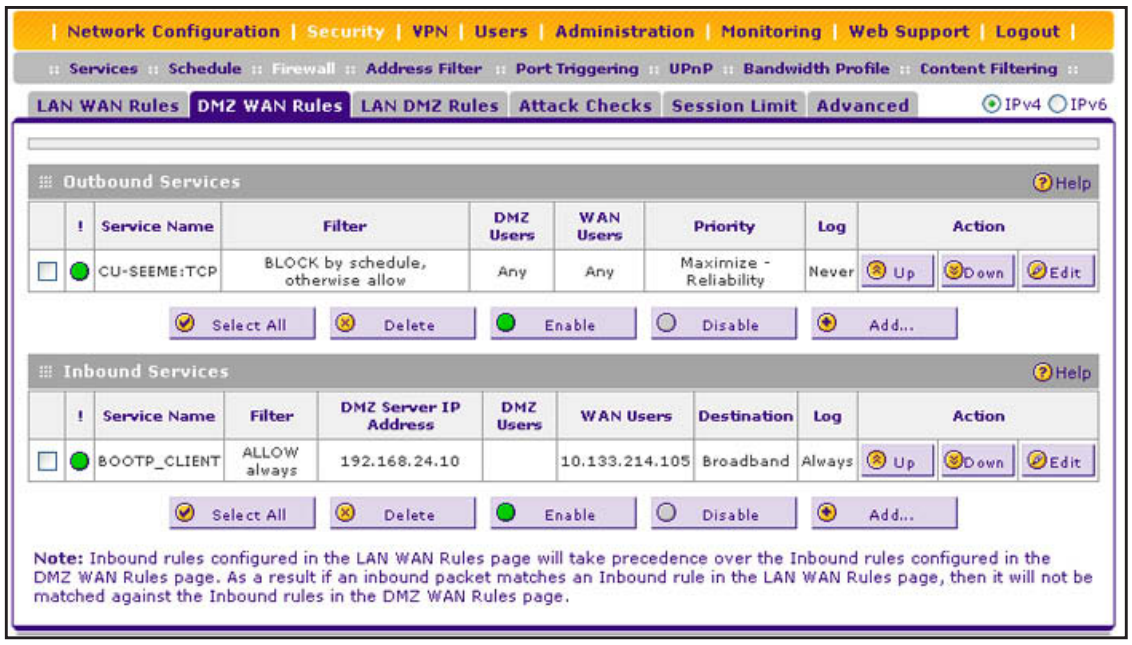

Figure 70.

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**. Allows you to 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 72* on page 149)
  - Edit DMZ WAN Inbound Service screen for IPv4 (identical to *Figure 74* on page 152)

➢ **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.)

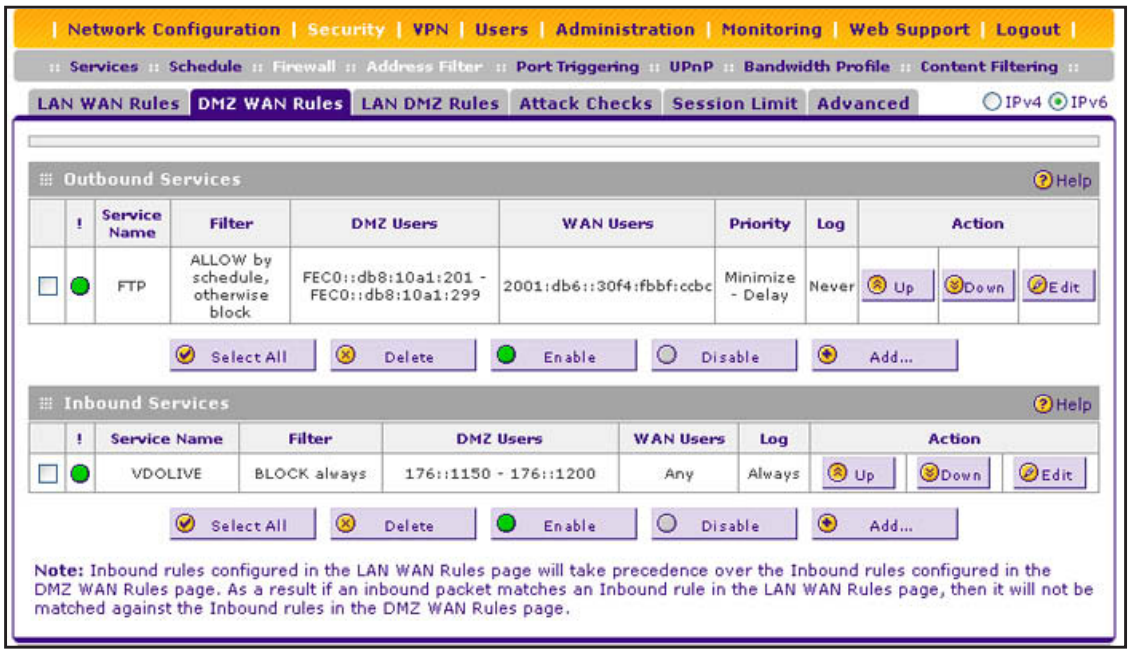

Figure 71.

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**. Allows you to 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 73* on page 150)
  - Edit DMZ WAN Inbound Service screen for IPv6 (identical to *Figure 75* on page 153)

➢ **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 70* on page 147).

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

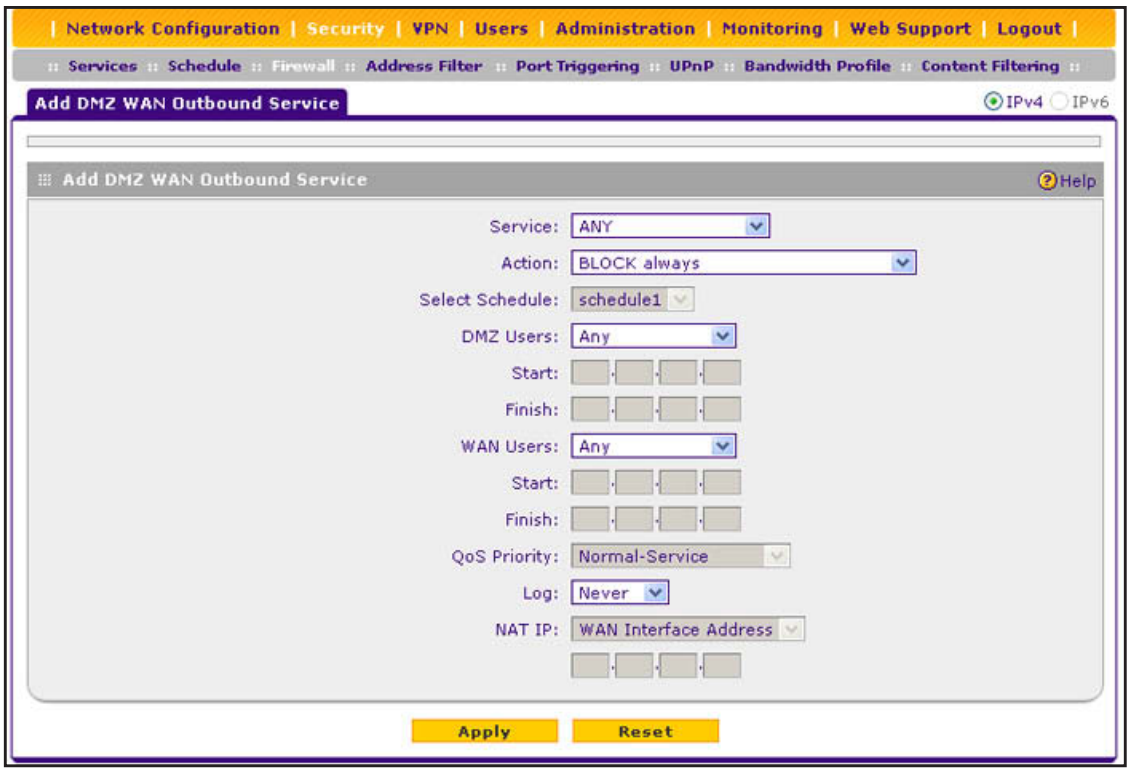

Figure 72.

2. Enter the settings as described in *Table 33* on page 132. 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
   - NAT IP (This 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.)
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 71* on page 148).
2. Click the **Add** table button under the Outbound Services table. The Add DMZ WAN Outbound Service screen for IPv6 displays:

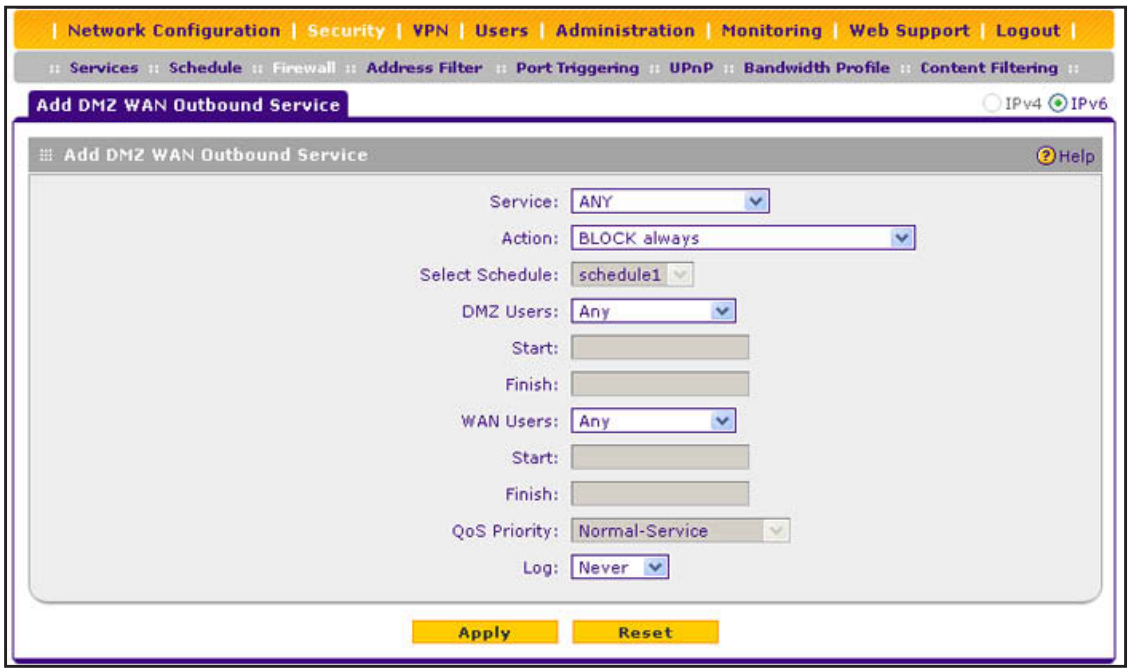

Figure 73.

3. Enter the settings as described in *Table 33* on page 132. 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 70* on page 147).

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

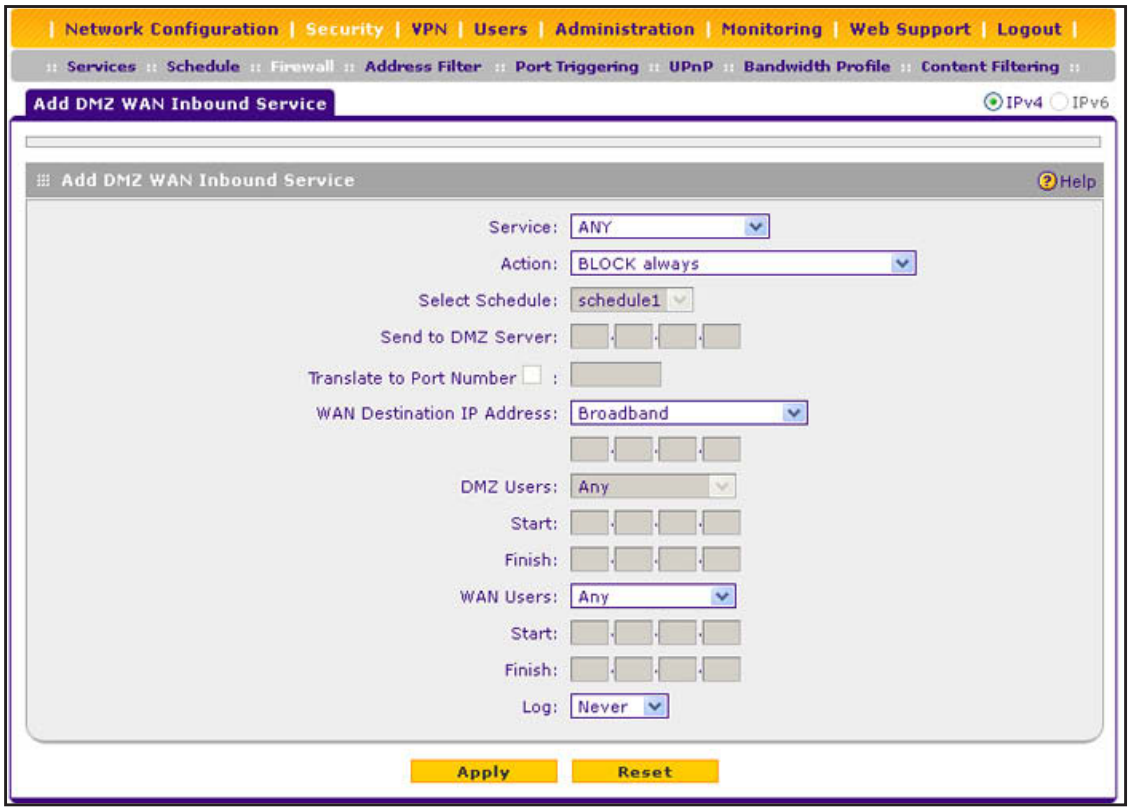

Figure 74.

2. Enter the settings as described in *Table 34* on page 136. 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 configuration is optional:

   - Translate to Port Number
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 71* on page 148).
2. Click the **Add** table button under the Inbound Services table. The Add DMZ WAN Inbound Service screen for IPv6 displays:

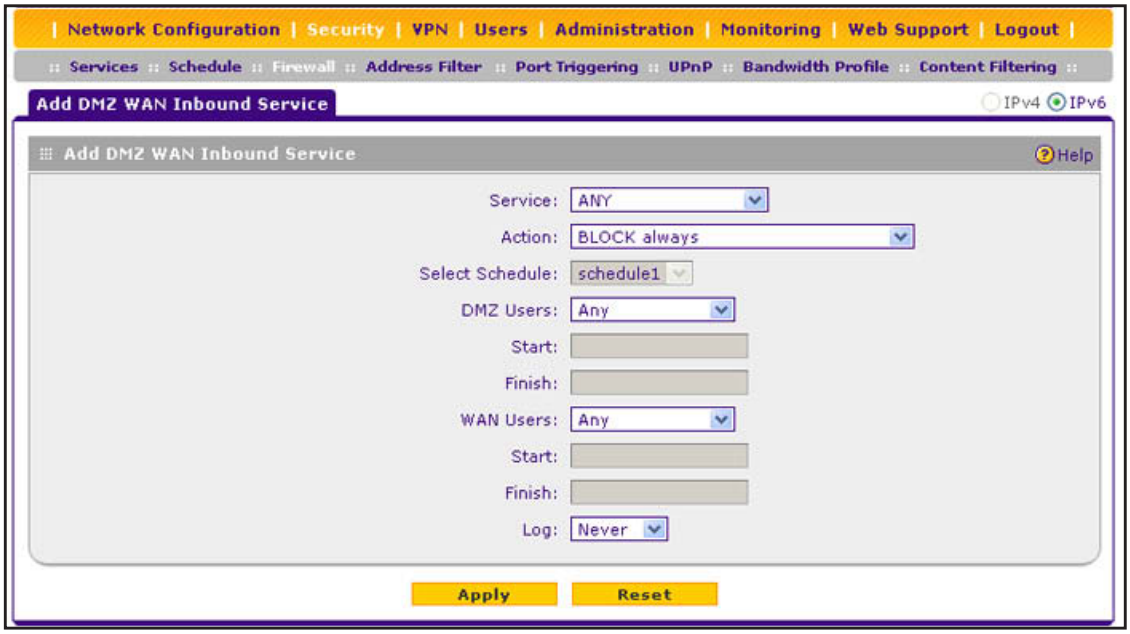

Figure 75.

3. Enter the settings as described in *Table 34* on page 136. 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

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 wireless VPN firewall. You do so by adding outbound service rules (see *Create LAN DMZ Outbound Service Rules* on page 156).

➢ **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.)

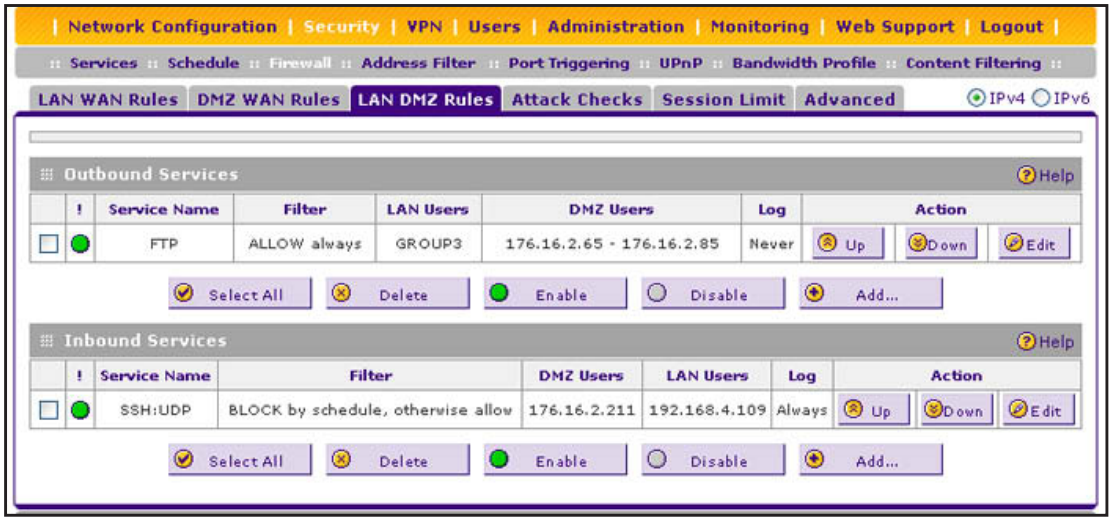

Figure 76.

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**. Allows you to 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 78* on page 156)
  - Edit LAN DMZ Inbound Service screen for IPv4 (identical to *Figure 80* on page 158)

➢ **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.)

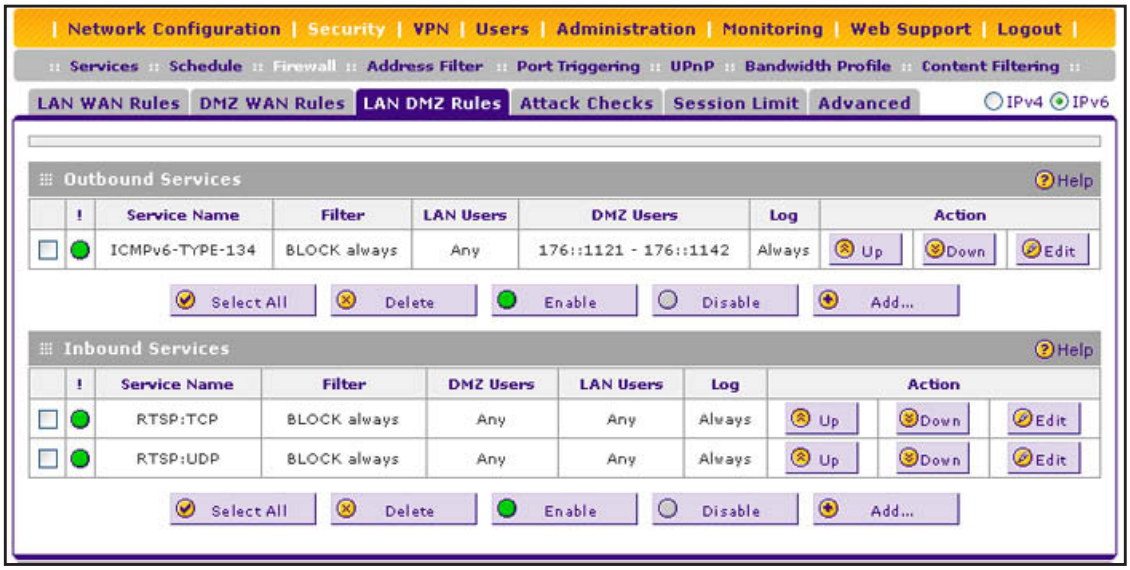

Figure 77.

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**. Allows you to 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 79* on page 157)
  - Edit LAN DMZ Inbound Service screen for IPv6 (identical to *Figure 81* on page 159)

➢ **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 76* on page 154).

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

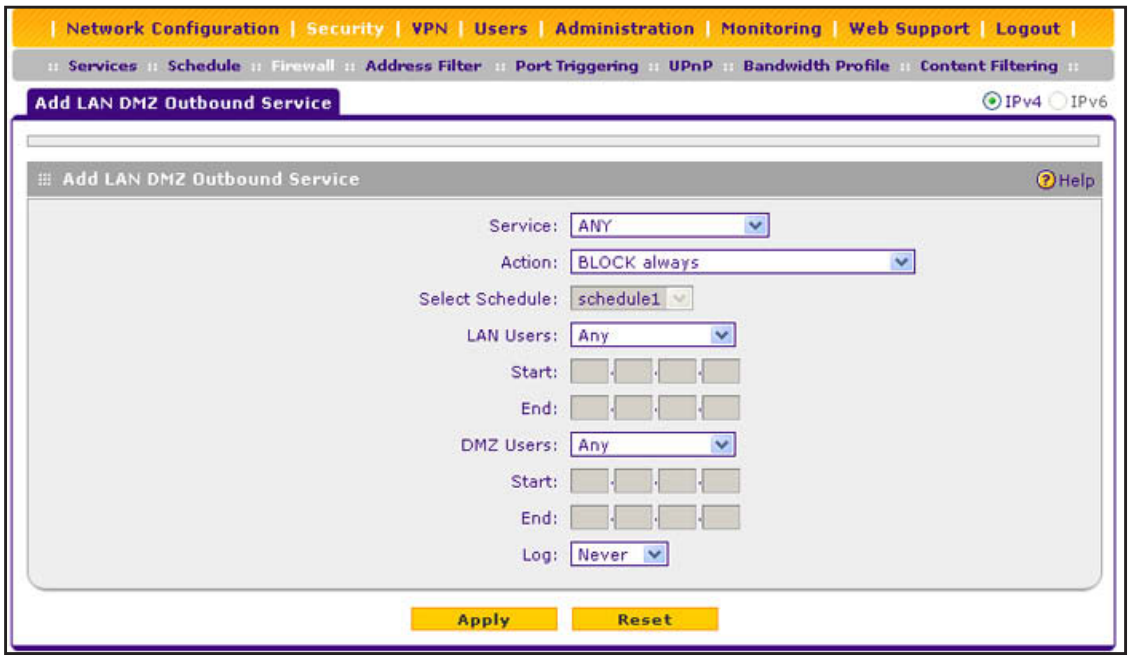

Figure 78.

2. Enter the settings as described in *Table 33* on page 132. 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 77* on page 155).
2. Click the **Add** table button under the Outbound Services table. The Add LAN DMZ Outbound Service screen for IPv6 displays:

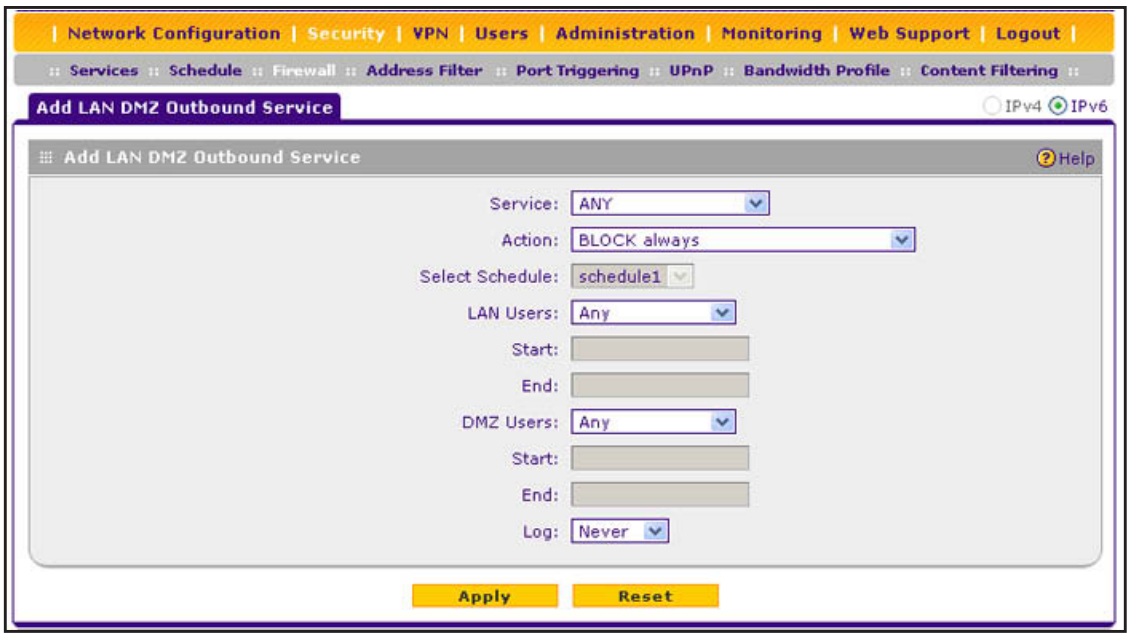

Figure 79.

3. Enter the settings as described in *Table 33* on page 132. 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 76* on page 154).

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

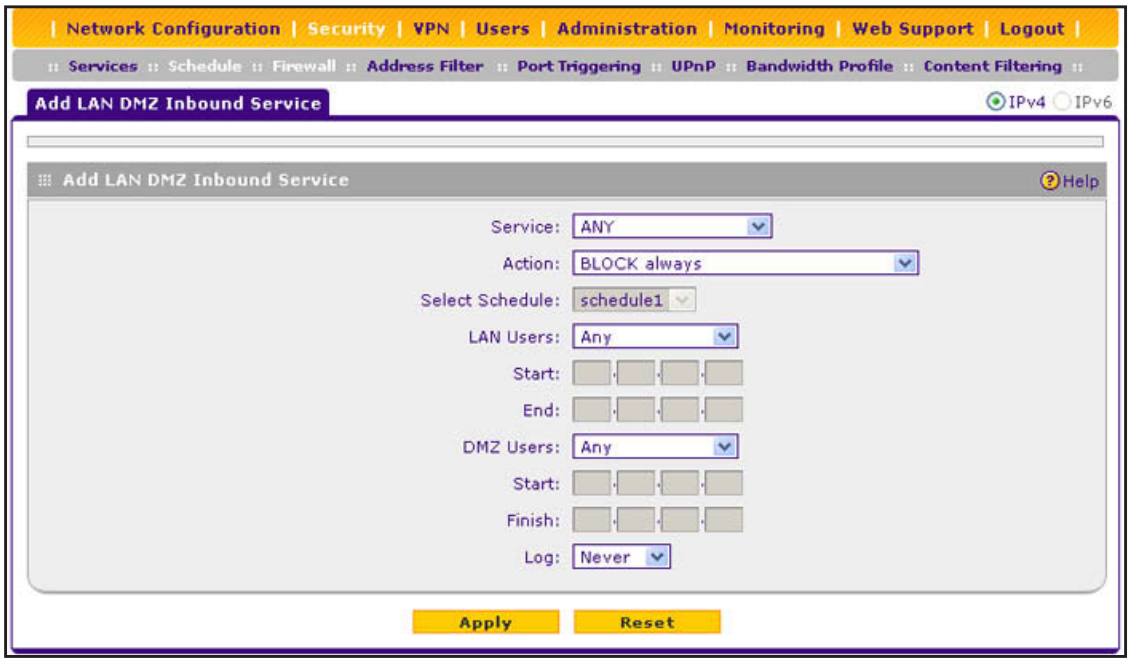

Figure 80.

2. Enter the settings as described in *Table 34* on page 136. 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 77* on page 155).
2. Click the **Add** table button under the Inbound Services table. The Add LAN DMZ Inbound Service screen for IPv6 displays:

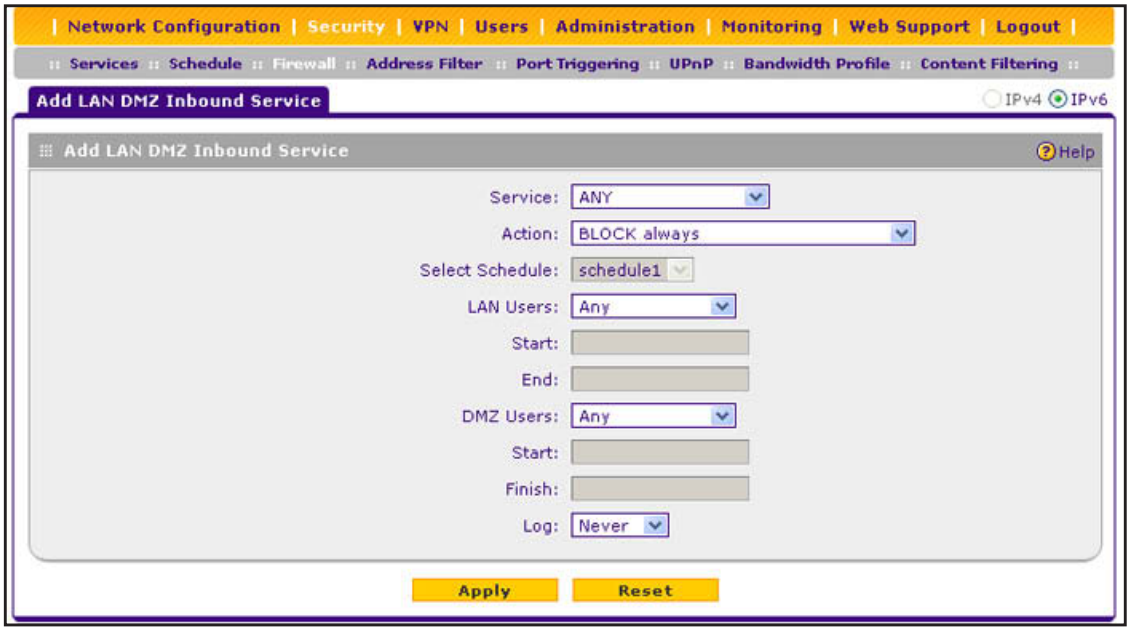

Figure 81.

3. Enter the settings as described in *Table 34* on page 136. 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.

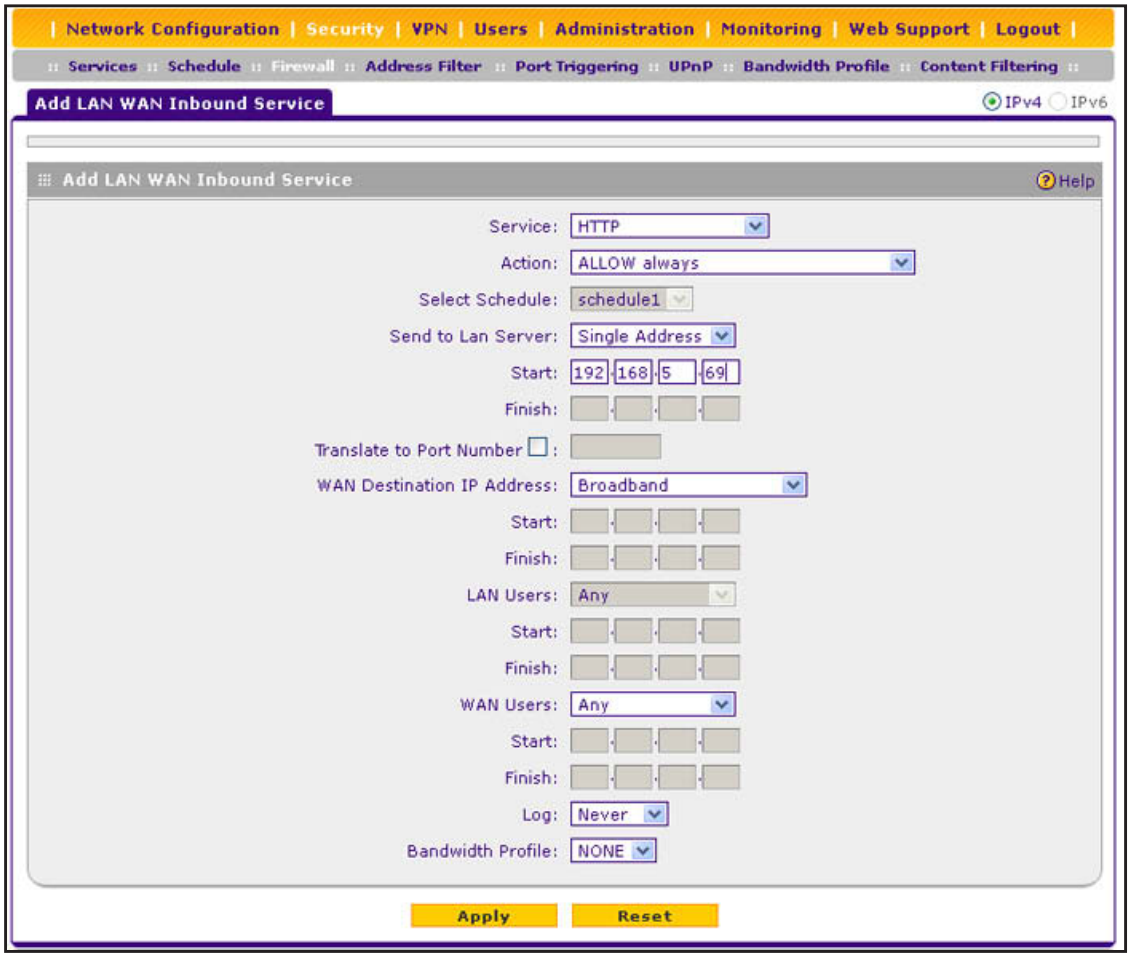

Figure 82.

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.

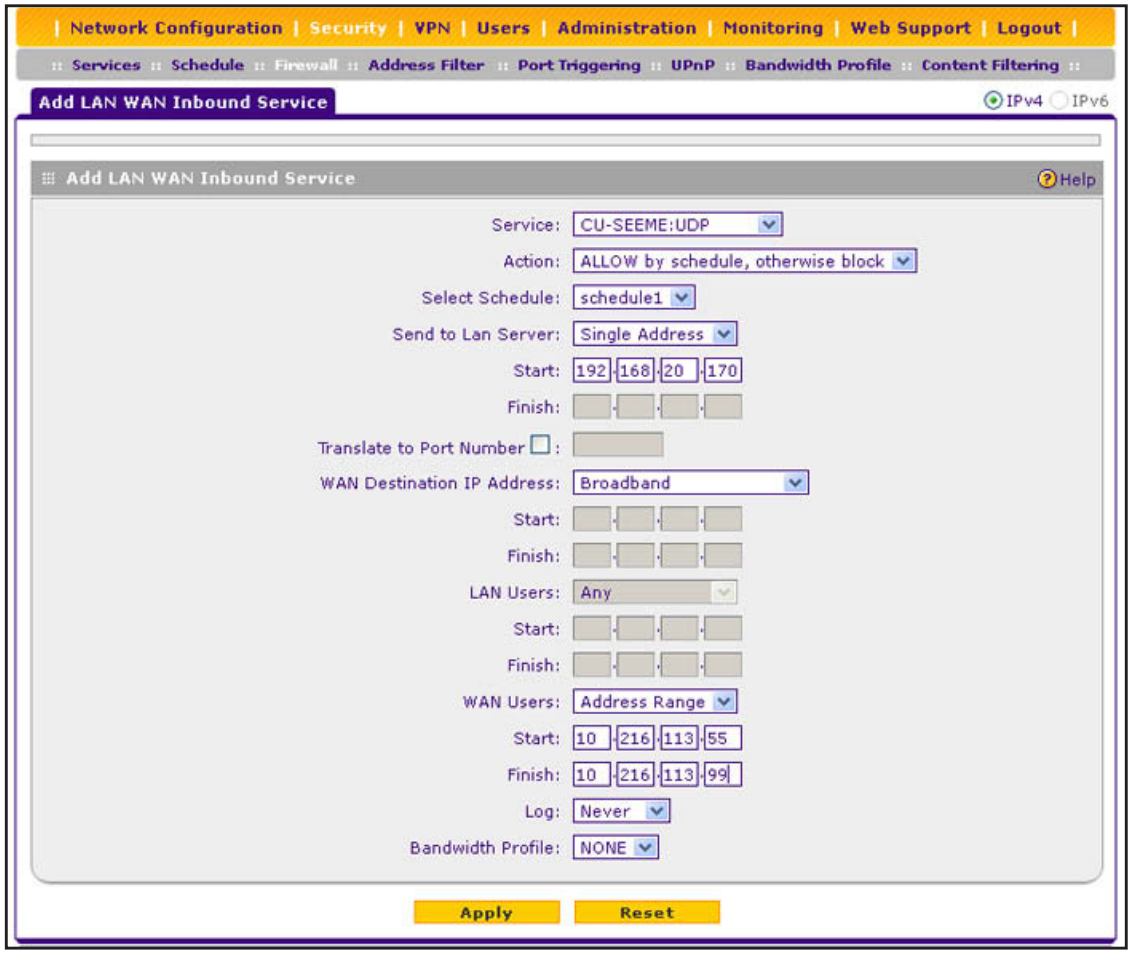

Figure 83.

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 wireless 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 wireless 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. 192.168.10.1 with subnet 255.255.255.0
- Web server computer on the wireless VPN firewall's LAN:
  - LAN IP address. 192.168.1.2
  - DMZ IP address. 192.168.10.2
  - Access to the web server is the (simulated) public IP address. 10.1.0.52

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

➢ **To configure the wireless 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:

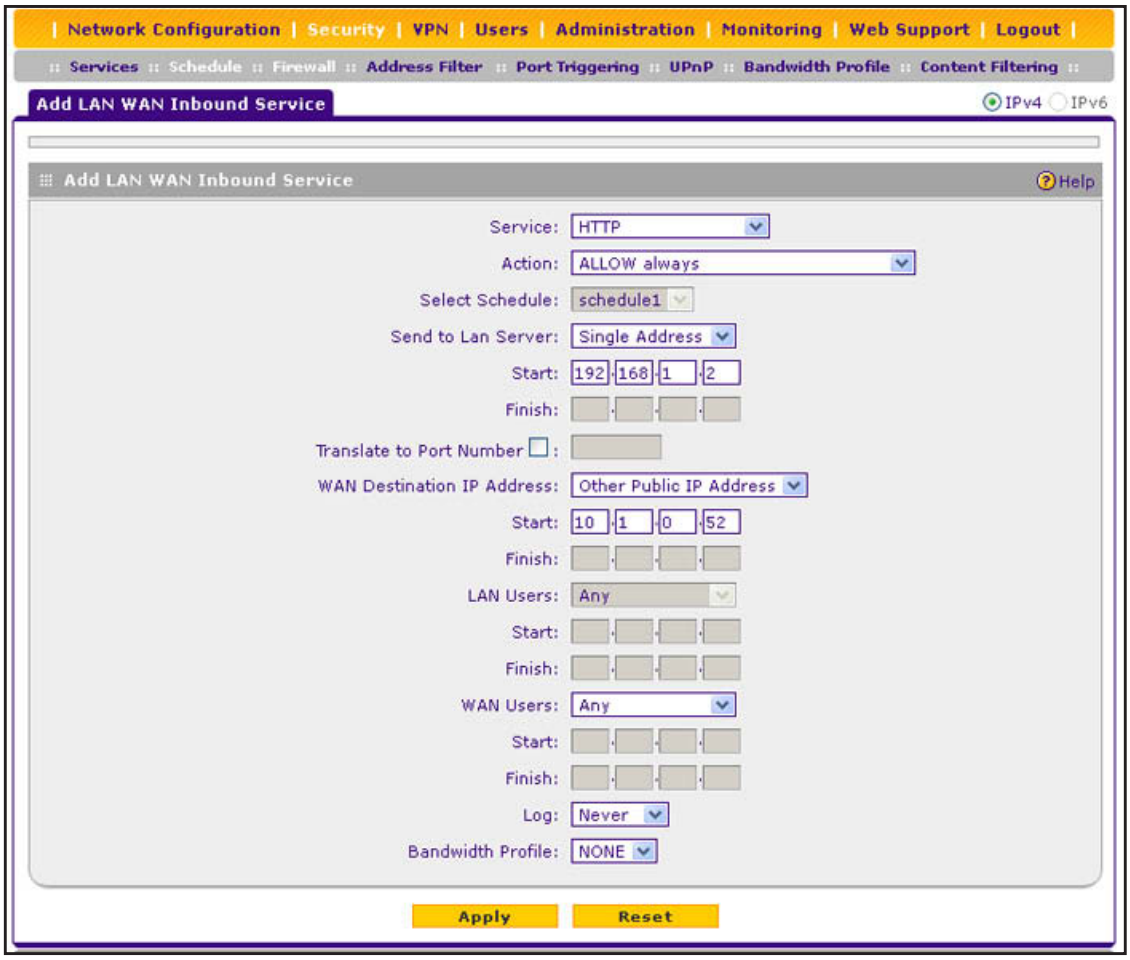

Figure 84.

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 computer (192.168.1.2 in this example).
7. In the WAN Destination IP Address fields, enter **10.1.0.52**.
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 7*. 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 wireless 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.

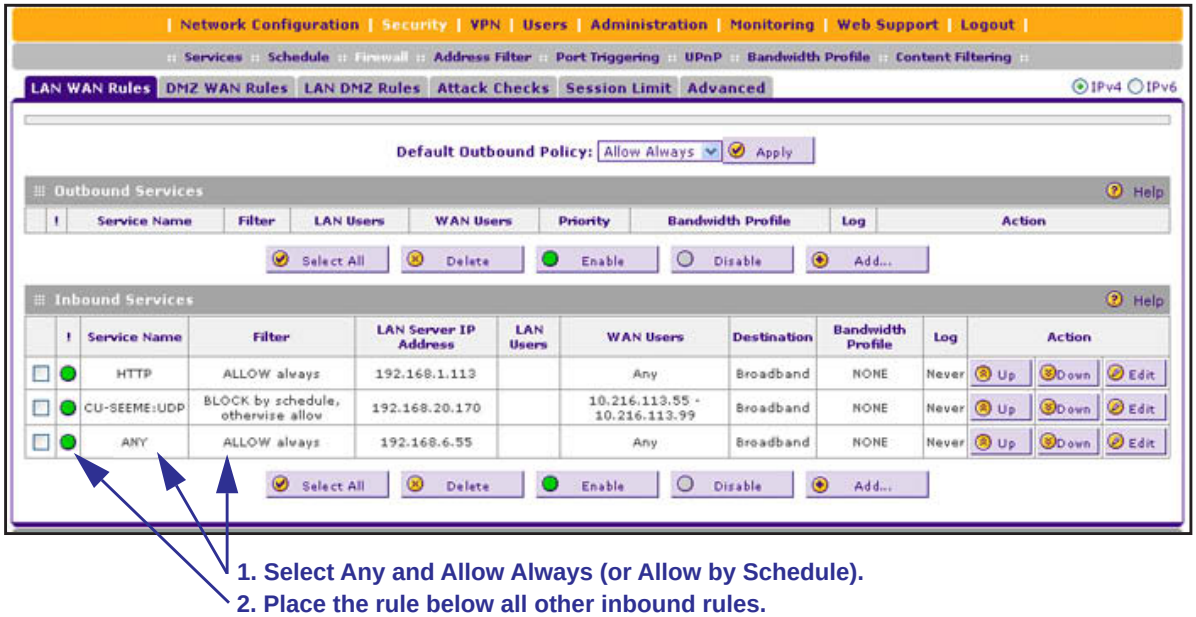

Figure 85.

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.

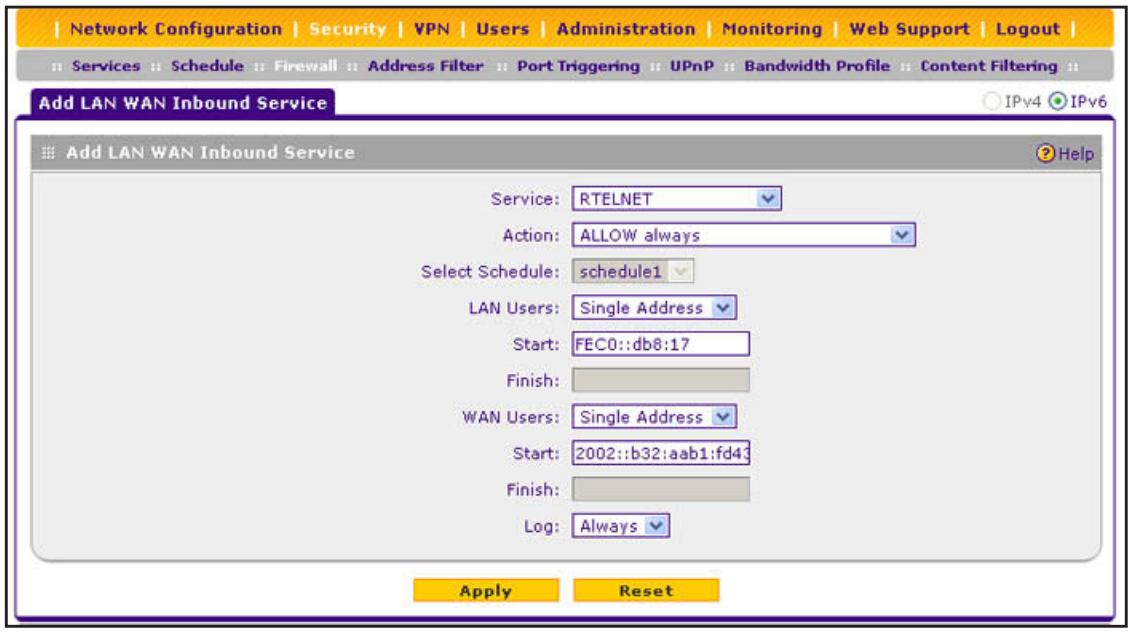

Figure 86.

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

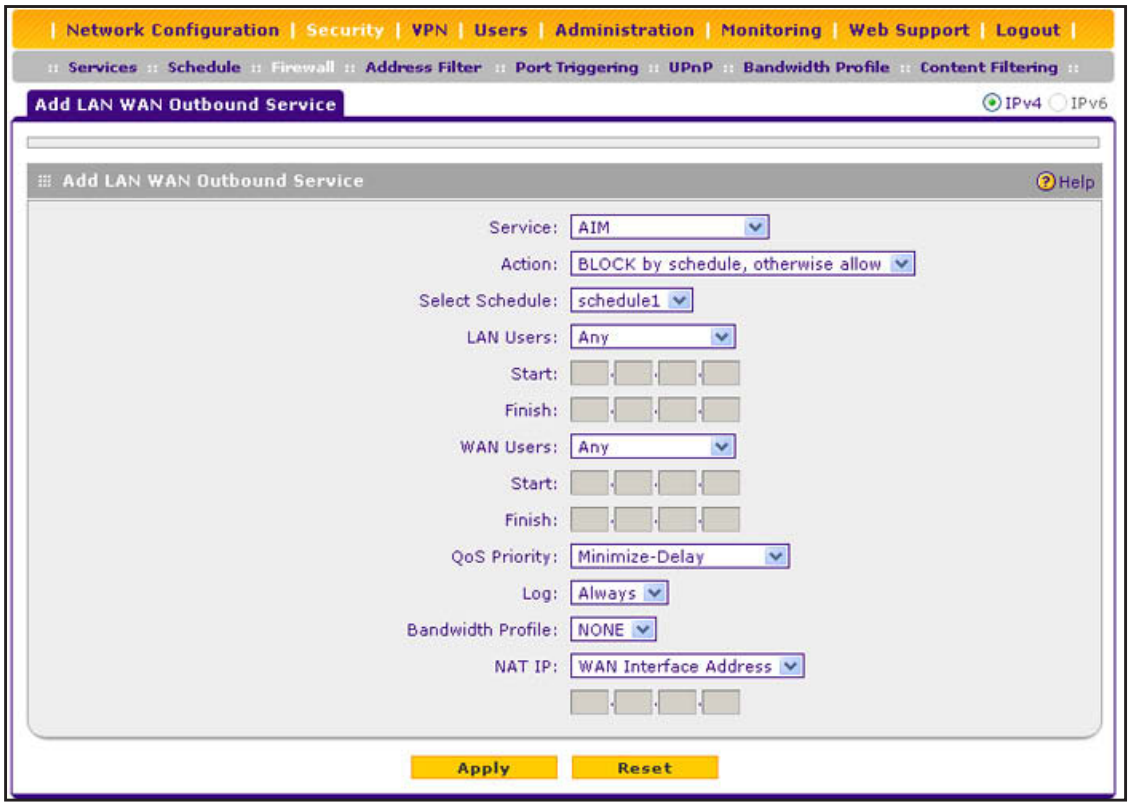

Figure 87.

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.

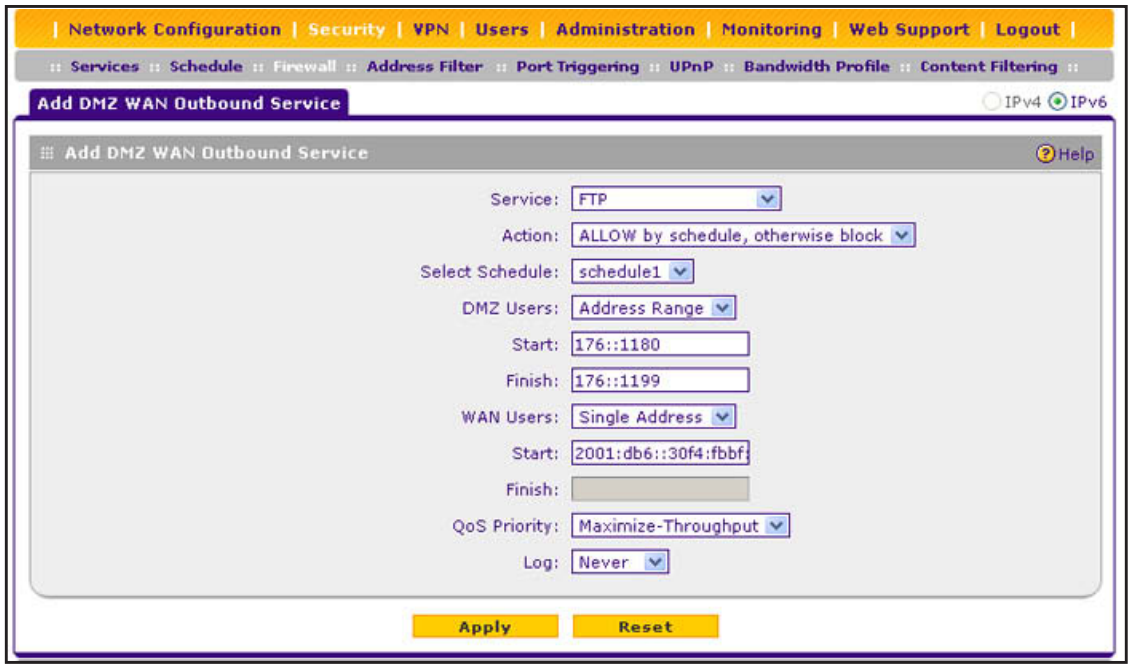

Figure 88.

Configure Other Firewall Features

- *Attack Checks*
- *Set Limits for IPv4 Sessions*
- *Manage the Application Level Gateway for SIP Sessions*

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

Attack Checks

The Attack Checks screen allows you to specify whether the wireless 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 168. 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:

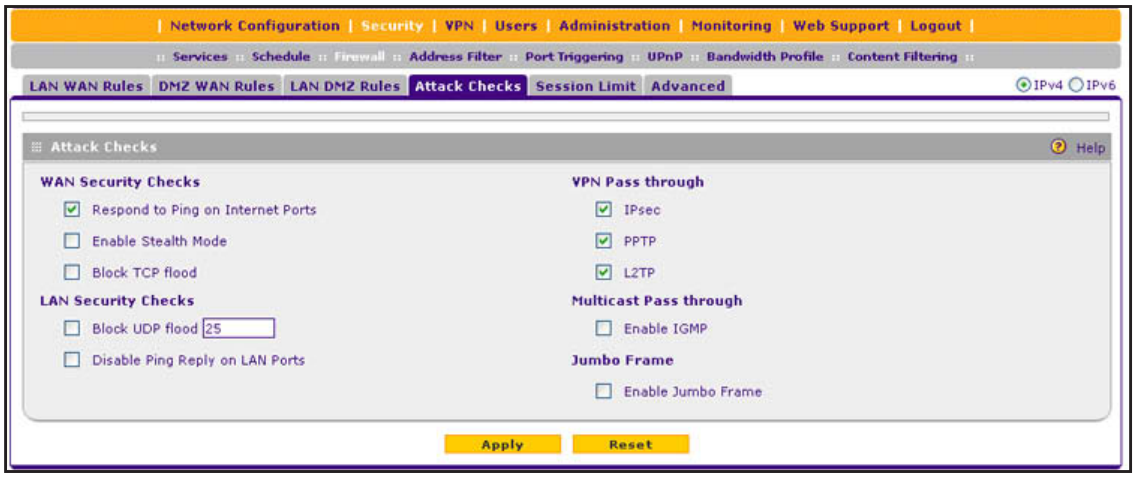

Figure 89.

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 wireless 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 wireless 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 wireless 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 wireless VPN firewall to drop all invalid TCP packets and to protect the wireless 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.

Table 35. Attack Checks screen settings for IPv4 (continued)

Setting	Description
LAN Security Checks	
Block UDP flood	Select the **Block UDP flood** check box to prevent the wireless 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 25 to 999. The default value is 25. The wireless VPN firewall drops UDP packets that exceed the specified number of connections per second. By default, the Block UDP flood check box is cleared so there is no restriction to the number of simultaneous, active UDP connections from a single device on the LAN. 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 wireless 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 wireless VPN firewall from responding to a ping on a LAN port.
VPN Pass through	
IPSec PPTP L2TP	When the wireless 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 wireless VPN firewall wants to connect to another VPN endpoint on the WAN side (placing the wireless VPN firewall between two VPN endpoints), encrypted packets are sent to the wireless VPN firewall. Because the wireless 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.

Table 35. Attack Checks screen settings for IPv4 (continued)

Setting	Description
Multicast Pass through	
Enable IGMP	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. Select the **Enable IGMP** check box to enable IP multicast pass-through. By default, IP multicast pass-through is disabled.
Jumbo Frames	
Enable Jumbo Frame	Jumbo frames allow multiple smaller packets to be combined into a single larger packet, reducing network overhead and increasing data transfer performance. Jumbo frames are supported on ports 1, 2, 3, and 4 only. Select the **Jumbo Frame** check box to enable jumbo frames. By default, jumbo frames are disabled. **Note:** Jumbo frames are not supported on Fast Ethernet interfaces.

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:

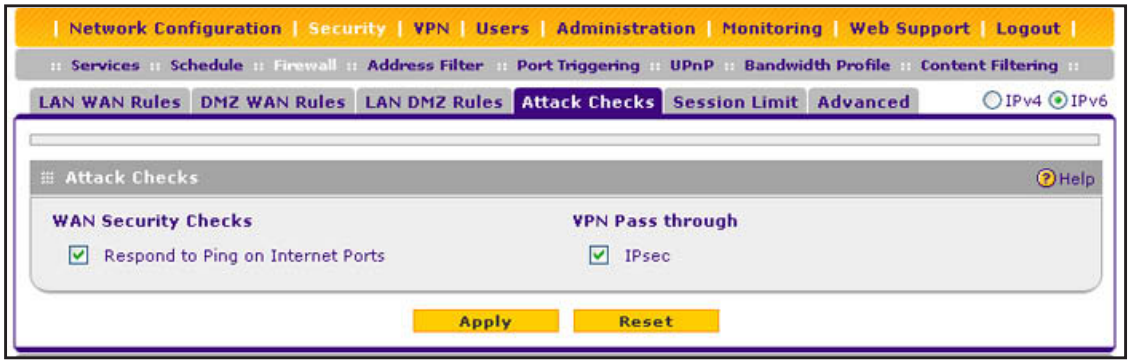

Figure 90.

3. Configure the following settings:
   - **Respond to Ping on Internet Ports**. Select the **Respond to Ping on Internet Ports** check box to enable the wireless 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 wireless 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 wireless 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:

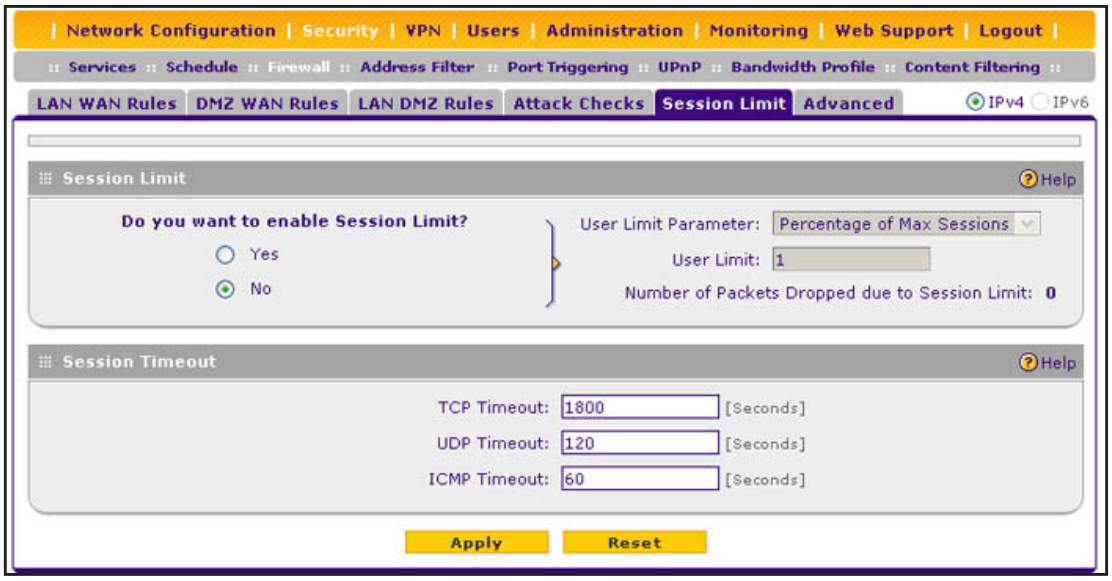

Figure 91.

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	
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 wireless VPN firewall. • **Number of Sessions**. An absolute number of maximum sessions.

Table 36. Session Limit screen settings (continued)

Setting	Description
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 wireless 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 should be considered 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 1800 seconds for TCP sessions, 120 seconds for UDP sessions, and 60 seconds for ICMP sessions.
UDP Timeout	
ICMP Timeout	

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

Manage the Application Level Gateway for SIP Sessions

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

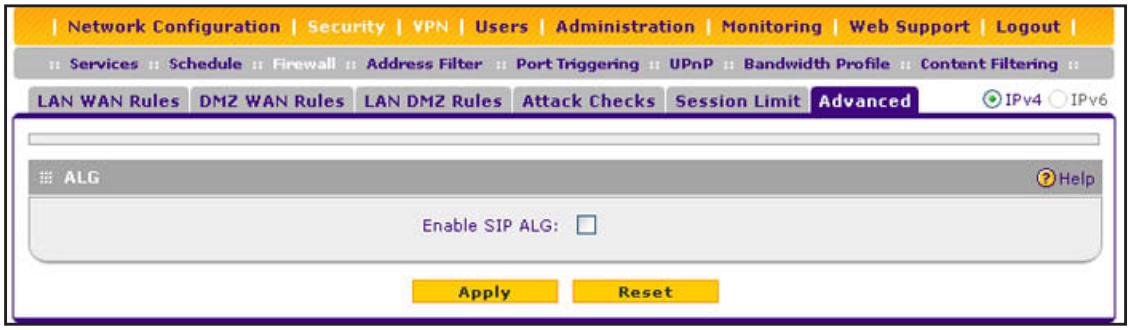

Figure 92.

2. Select the **Enable SIP ALG** check box.
3. Click **Apply** to save your settings.

Services, Bandwidth Profiles, and QoS Profiles

When you create inbound and outbound firewall rules, you use firewall objects such as services, QoS profiles, bandwidth profiles, and schedules to narrow down the firewall rules:

- **Services**. A service narrows down the firewall rule to an application and a port number. For information about adding services, see *Add Customized Services* on page 173.
- **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 176.
- **QoS profiles**. A Quality of Service (QoS) profile defines the relative priority of an IP packet for traffic that matches the firewall rule. For information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 178.

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 183.

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 wireless VPN firewall you can select service numbers in the range from 1 to 65535.

Although the wireless 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.)

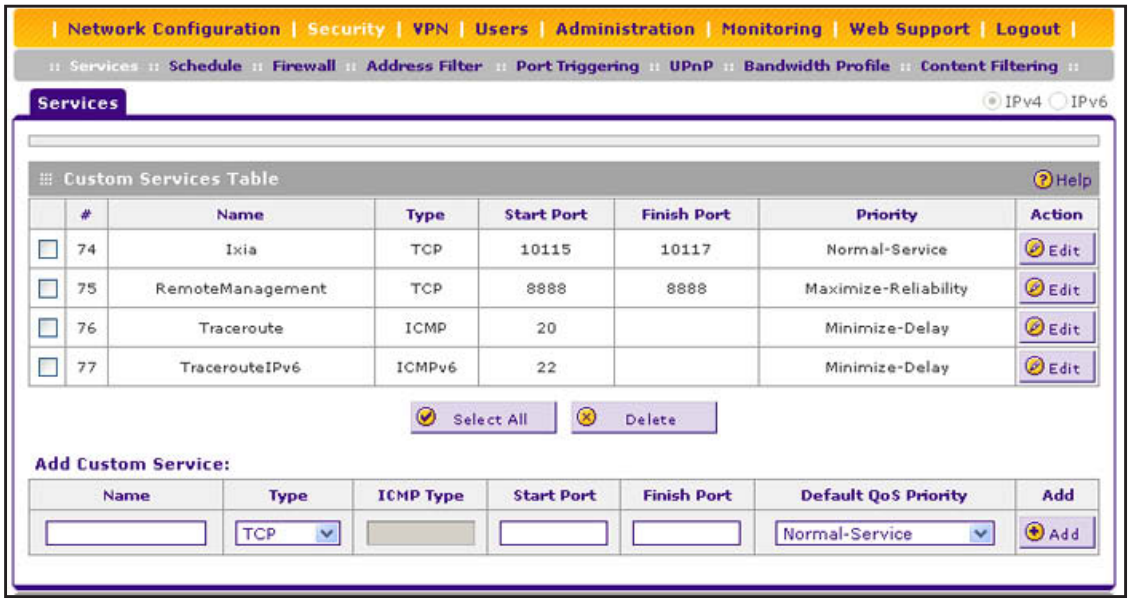

Figure 93.

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.

Table 37. Services screen settings (continued)

Setting	Description
Start Port	The first TCP or UDP port of a range that the service uses. **Note:** This field is enabled only when you select TCP or UDP from the Type drop-down list.
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.
Default QoS Priority	From the Default QoS Priority drop-down list, select the QoS profile that you want to assign to the service. For more information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 178.

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:

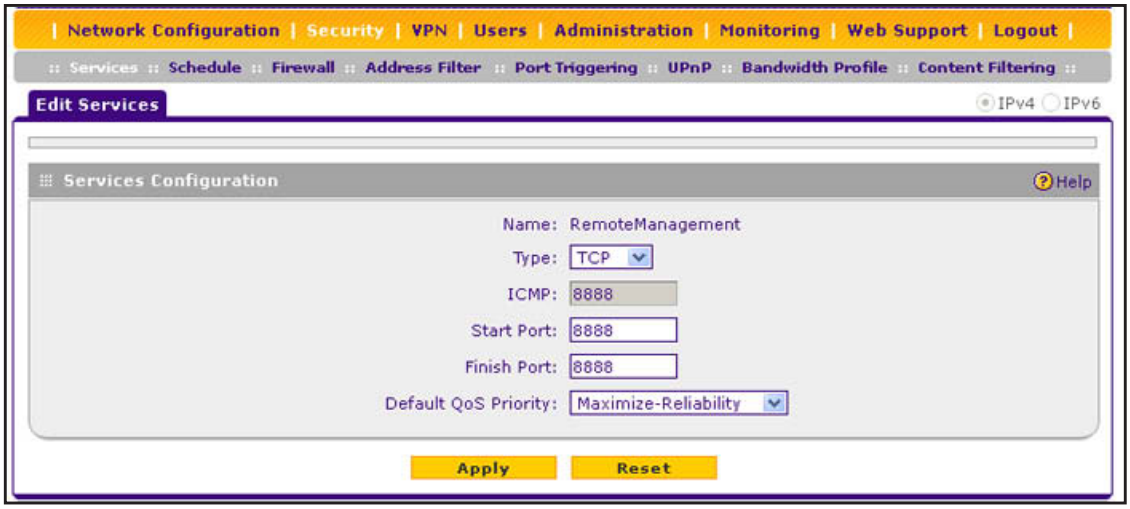

Figure 94.

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 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 66* on page 142)
- Add LAN WAN Inbound Services screen for IPv4 (see *Figure 68* on page 145)

➢ **To add and enable a bandwidth profile:**

1. Select **Security > Bandwidth Profiles**. The Bandwidth Profiles screen displays. (The following figure shows some examples.)

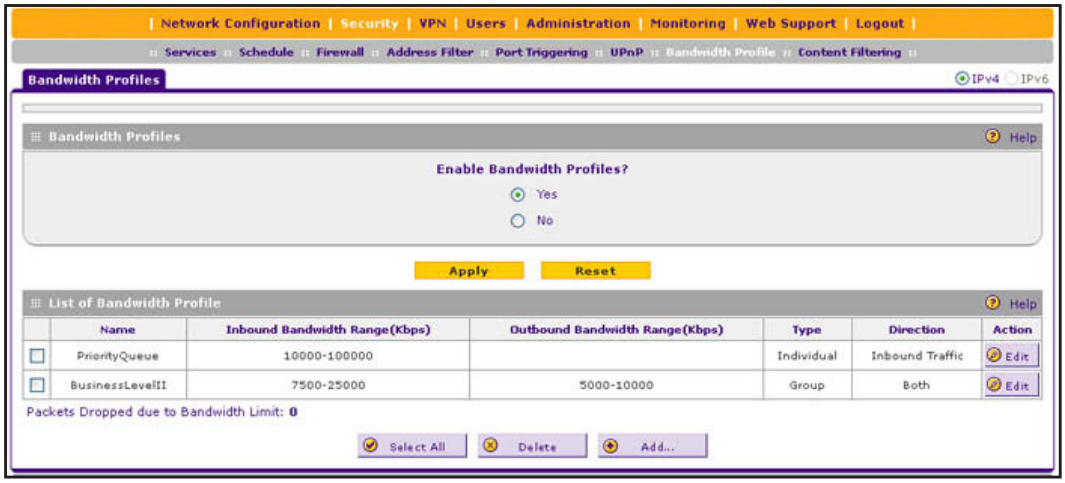

Figure 95.

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

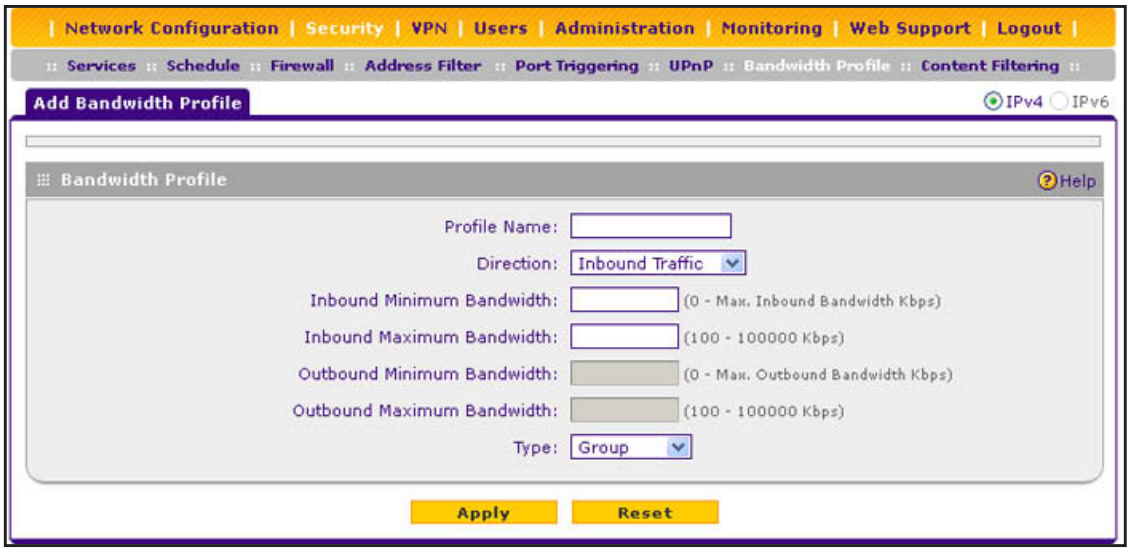

Figure 96.

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.
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.

Table 38. Add Bandwidth Profile screen settings (continued)

Setting	Description
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.

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.

Preconfigured Quality of Service Profiles

A Quality of Service (QoS) profile defines the relative priority of an IP packet when multiple connections are scheduled for simultaneous transmission on the wireless 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 wireless VPN firewall. Priorities are defined by the *Type of Service in the Internet Protocol Suite standards*, RFC 1349.

You can assign a QoS profile to a firewall rule or service on the following screens:

- Add LAN WAN Outbound Services screen for IPv4 (see *Figure 66* on page 142)
- Add LAN WAN Outbound Services screen for IPv6 (see *Figure 67* on page 143)
- Add DMZ WAN Outbound Services screen for IPv4 (see *Figure 72* on page 149)
- Add DMZ WAN Outbound Services screen for IPv6 (see *Figure 73* on page 150)
- Services screen (see *Figure 93* on page 174)

These are the default QoS profiles that are preconfigured and that 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 wireless 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 wireless 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.)

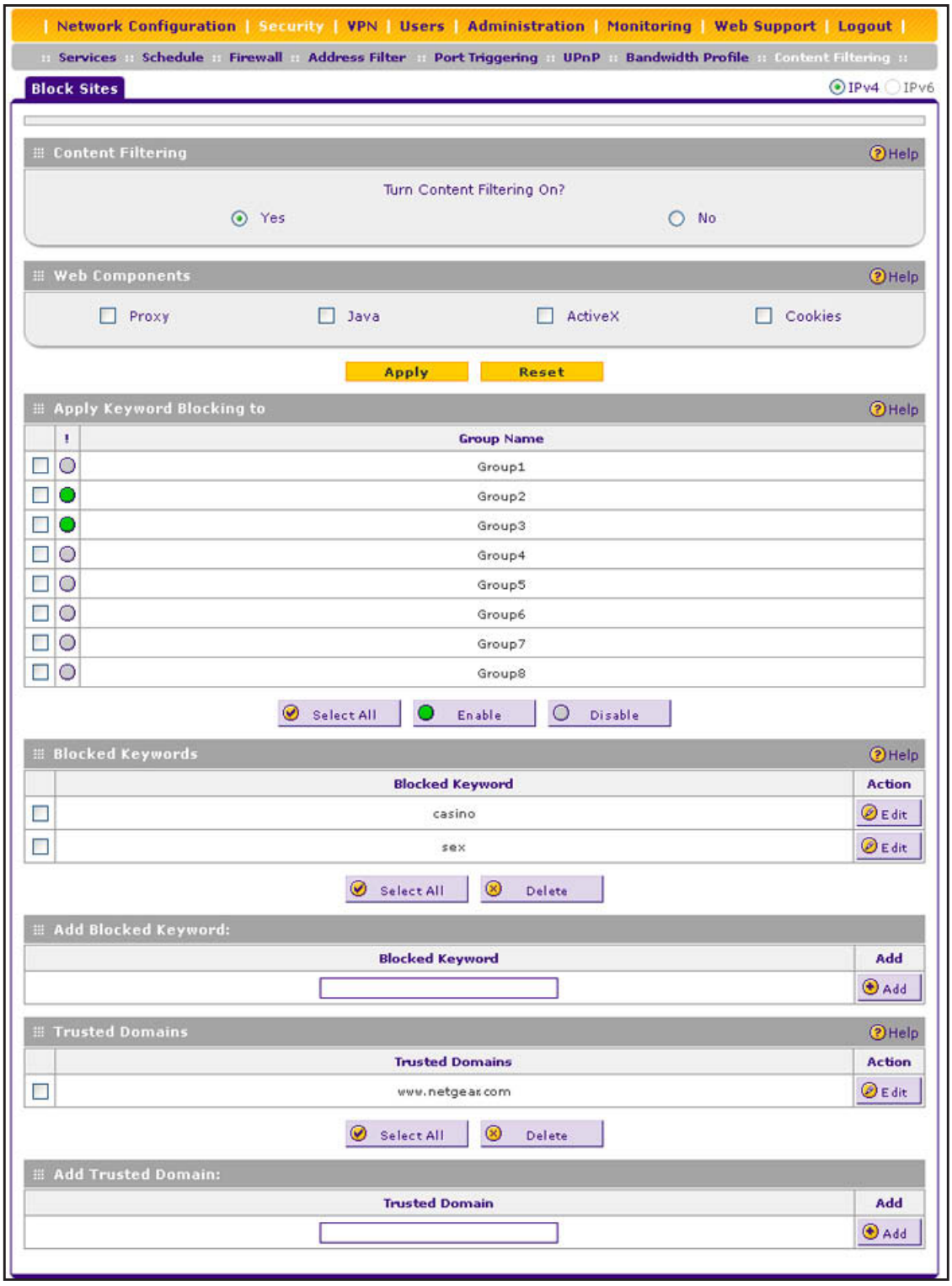

Figure 97.

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 179.
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 72), 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:

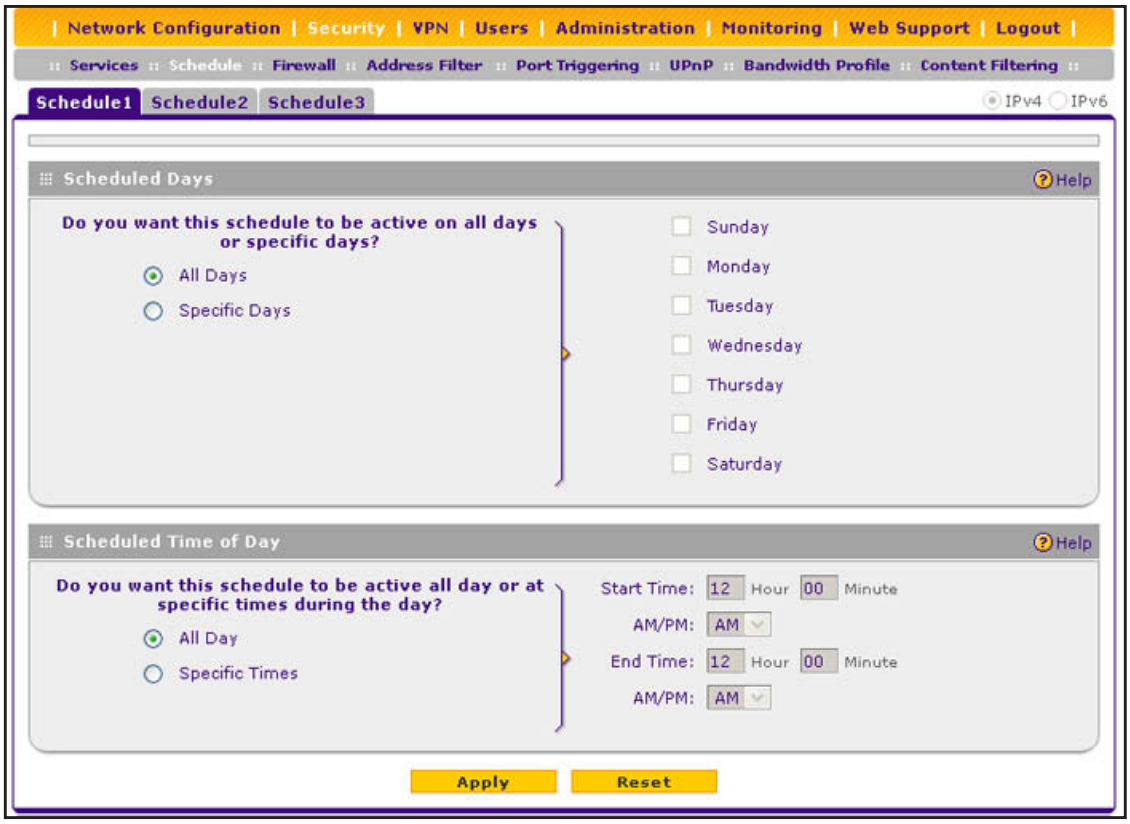

Figure 98.

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 132.

➢ **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.)

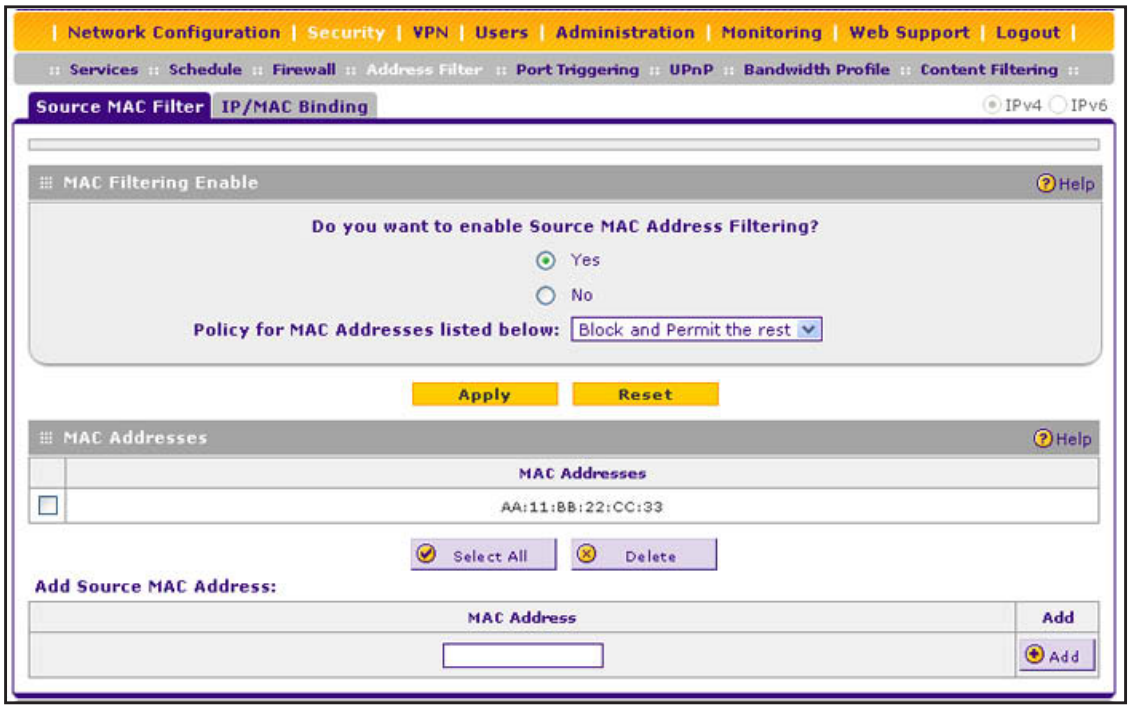

Figure 99.

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 (zero to nine) 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 wireless VPN firewall. If the wireless 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 wireless 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 69.

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 wireless 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.)

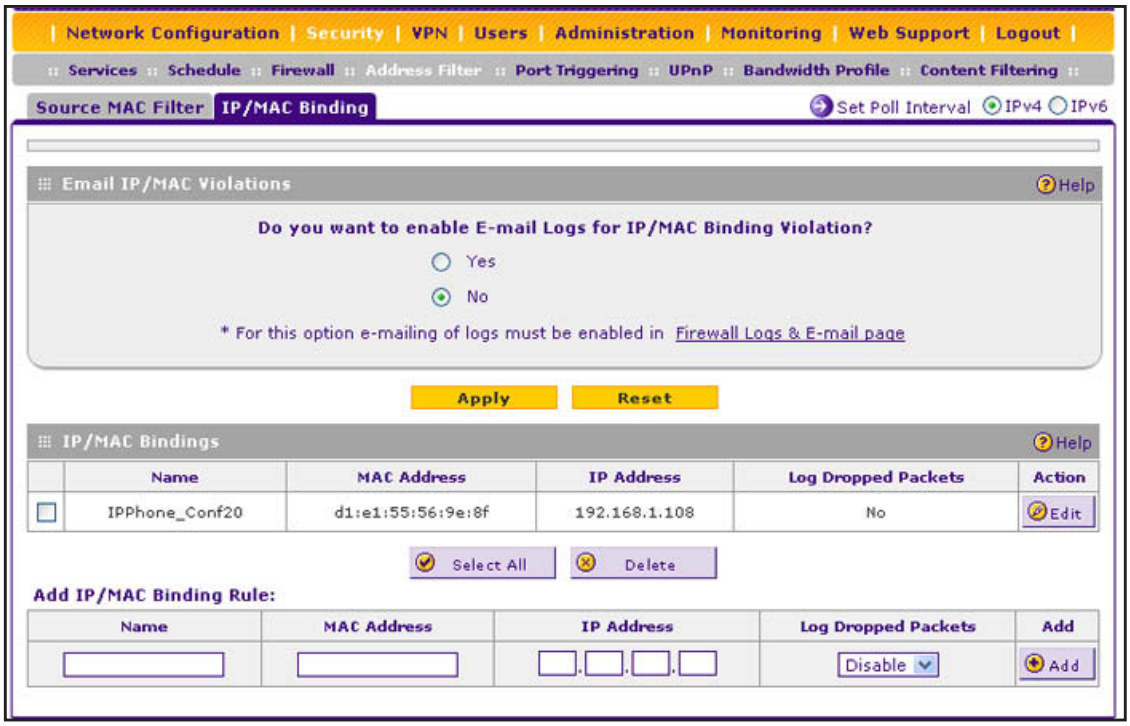

Figure 100.

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 352).
   - **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 39. 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:

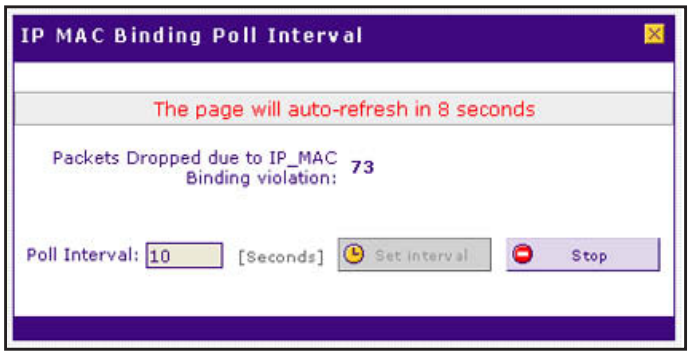

Figure 101.

  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.)

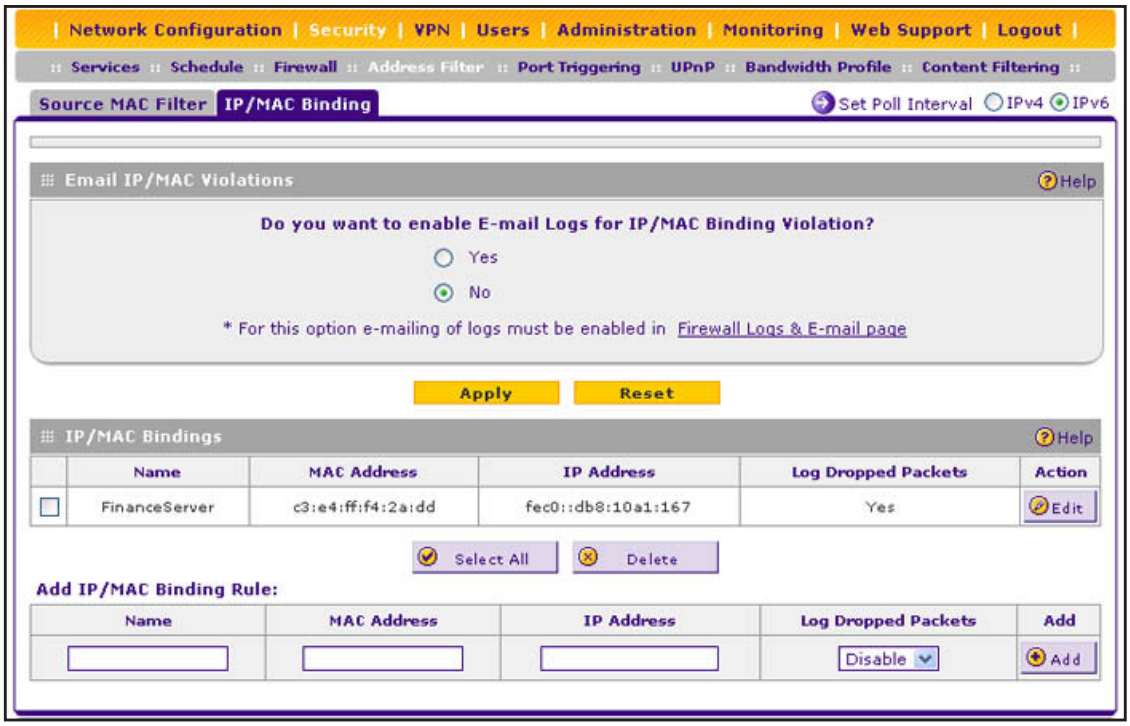

Figure 102.

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 352).
   - **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 40. 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.
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:

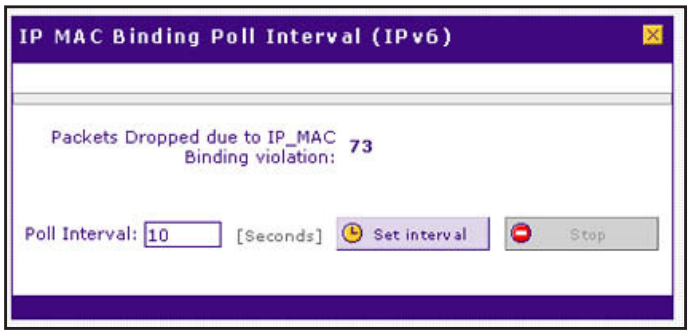

Figure 103.

  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 wireless 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 wireless VPN firewall.
4. The wireless 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 wireless VPN firewall can determine that the application has terminated.

Note: For additional ways of allowing inbound traffic, see *Inbound Rules (Port Forwarding)* on page 134.

➢ **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.)

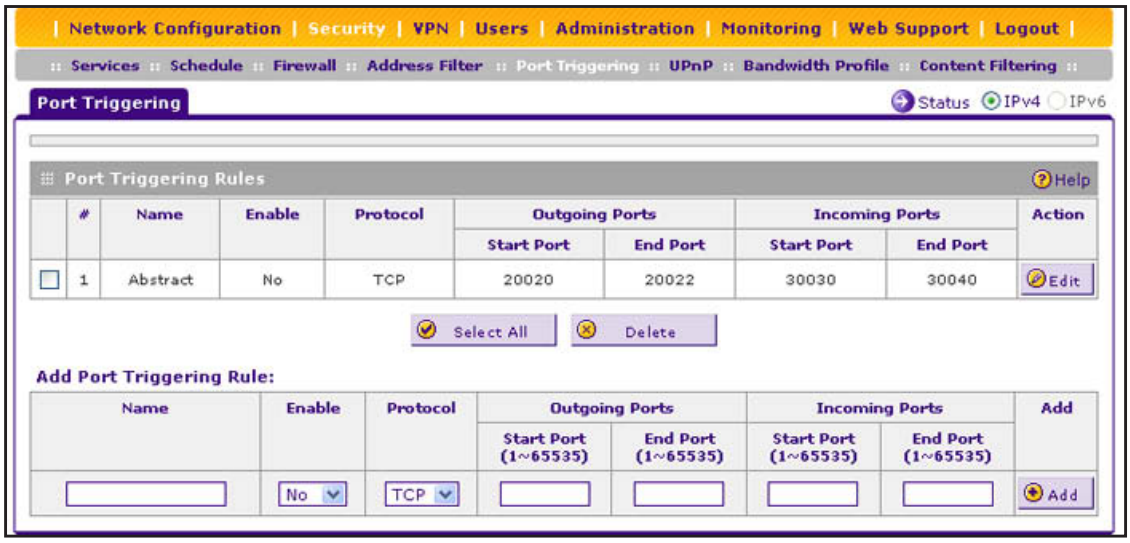

Figure 104.

2. In the Add Port Triggering Rule section, enter the settings as described in the following table:

Table 41. 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 (1–65535) of the range for triggering.
	End Port	The end port (1–65535) of the range for triggering.
Incoming Ports	Start Port	The start port (1–65535) of the range for responding.
	End Port	The end port (1–65535) 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.

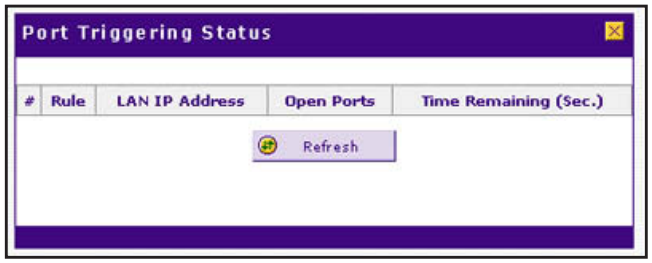

Figure 105.

Configure Universal Plug and Play

The Universal Plug and Play (UPnP) feature enables the wireless VPN firewall to automatically discover and configure devices when it searches the LAN and WAN. UPnP is supported for IPv4 devices only.

- **To configure UPnP:**

  1. Select **Security > UPnP**. The UPnP screen displays:

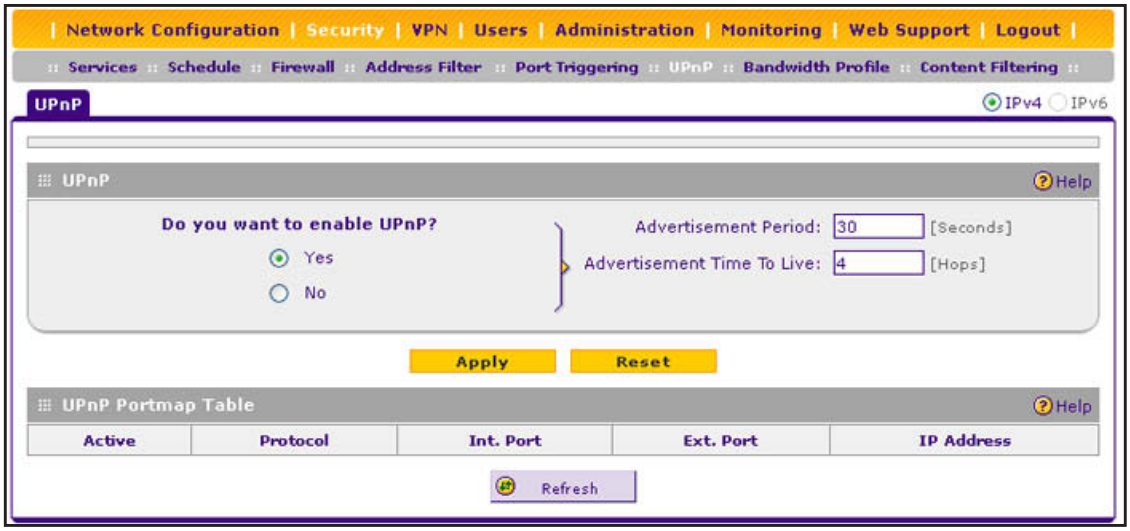

Figure 106.

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 wireless VPN firewall and that have been automatically detected by the wireless 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 wireless 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

6

This chapter describes how to use the IP security (IPSec) virtual private networking (VPN) features of the wireless VPN firewall to provide secure, encrypted communications between your local network and a remote network or computer. The chapter contains the following sections:

- *Use the IPSec VPN Wizard for Client and Gateway Configurations*
- *Test the Connection and View Connection and Status Information*
- *Manage IPSec VPN Policies*
- *Configure Extended Authentication (XAUTH)*
- *Assign IPv4 Addresses to Remote Users (Mode Config)*
- *Configure Keep-Alives and Dead Peer Detection*
- *Configure NetBIOS Bridging with IPSec VPN*
- *Configure the L2TP Server*

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 196
- *Create an IPv6 Gateway-to-Gateway VPN Tunnel with the Wizard* on page 200
- *Create an IPv4 Client-to-Gateway VPN Tunnel with the Wizard* on page 204

Note: Although the wireless 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

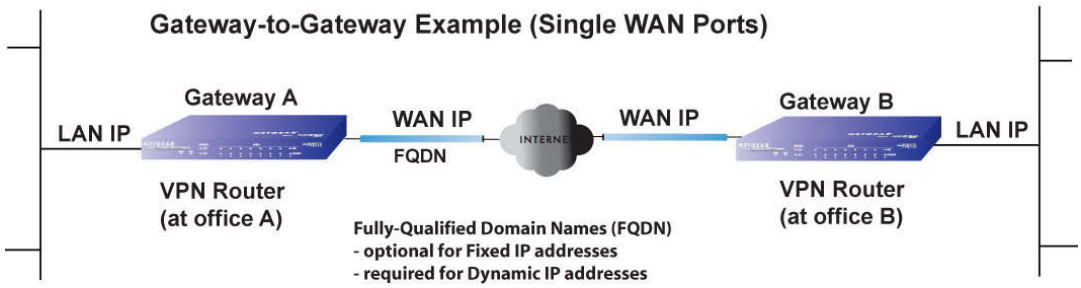

Figure 107.

➢ **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.)

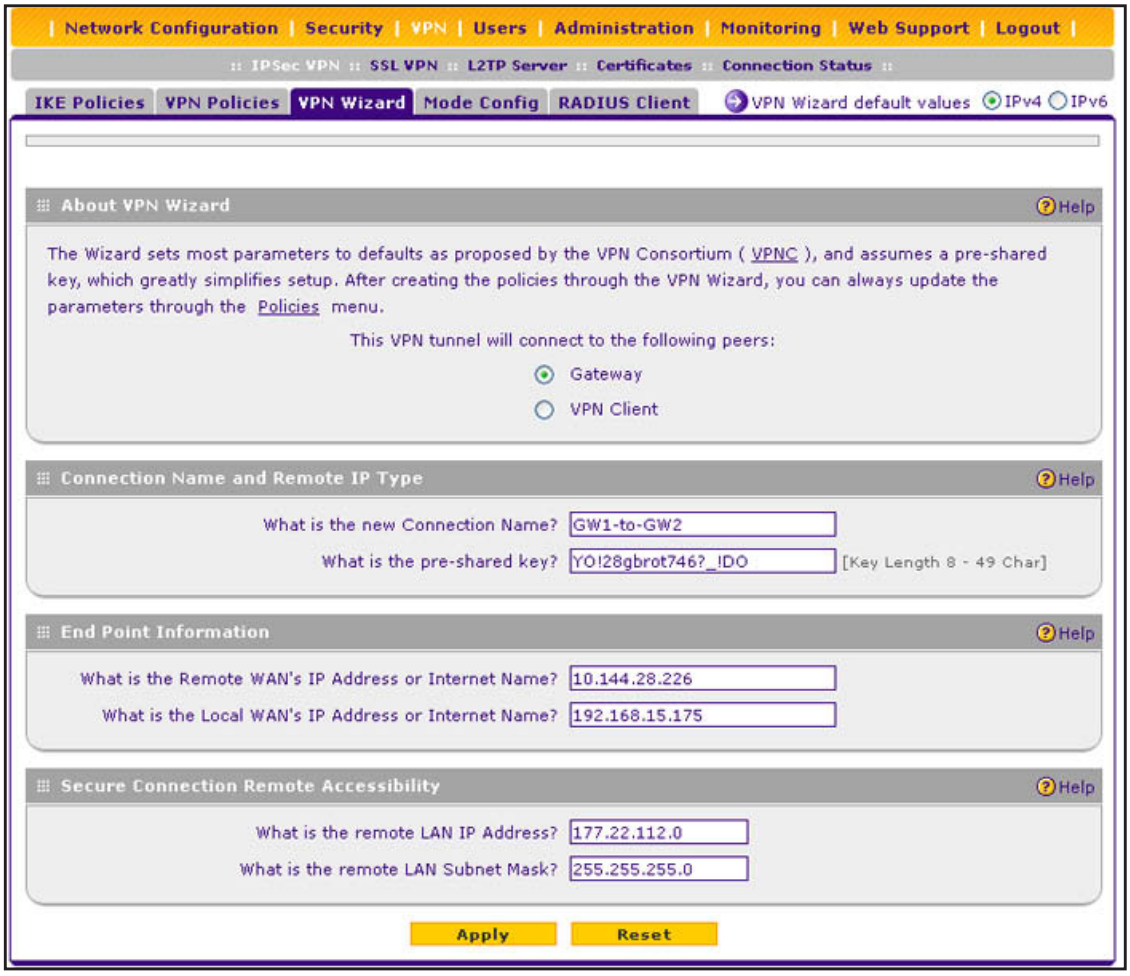

Figure 108.

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.

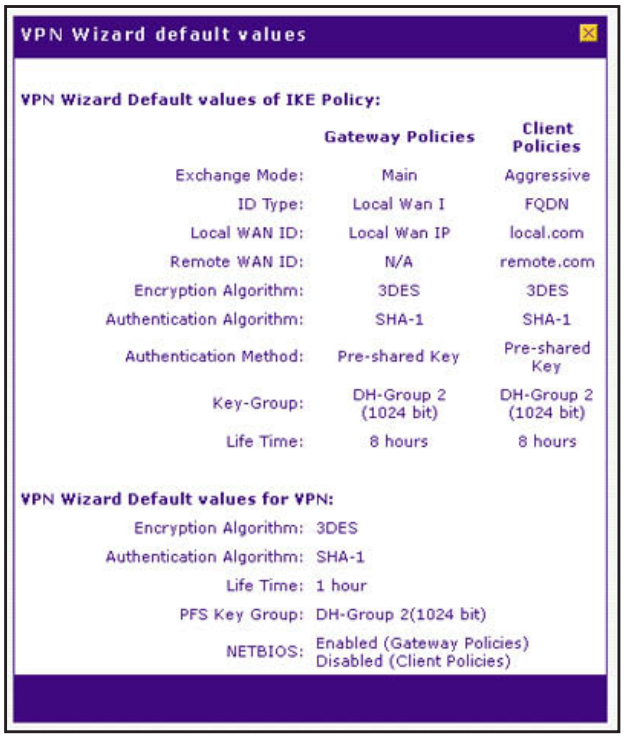

Figure 109.

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

Table 42. 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.
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 wireless VPN firewall's active WAN interface is automatically entered.

Table 42. IPSec VPN Wizard settings for an IPv4 gateway-to-gateway tunnel (continued)

Setting	Description
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 261.

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.

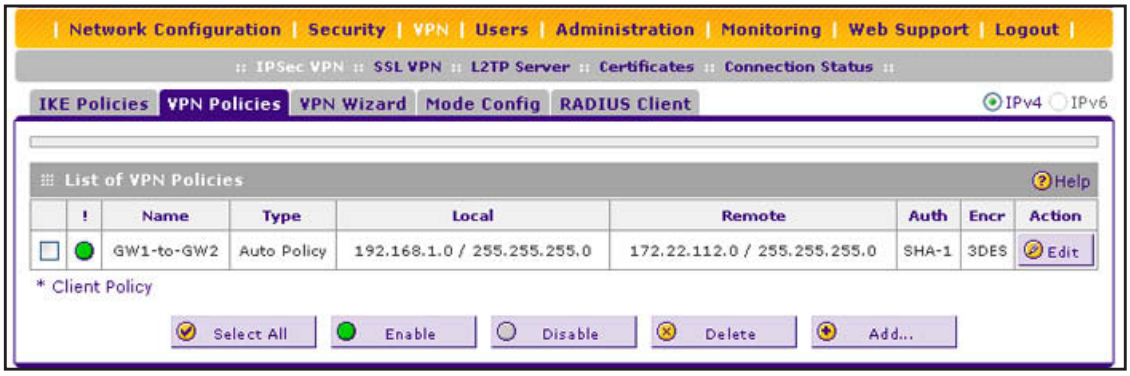

Figure 110.

4. Configure a VPN policy on the remote gateway that allows connection to the wireless 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:

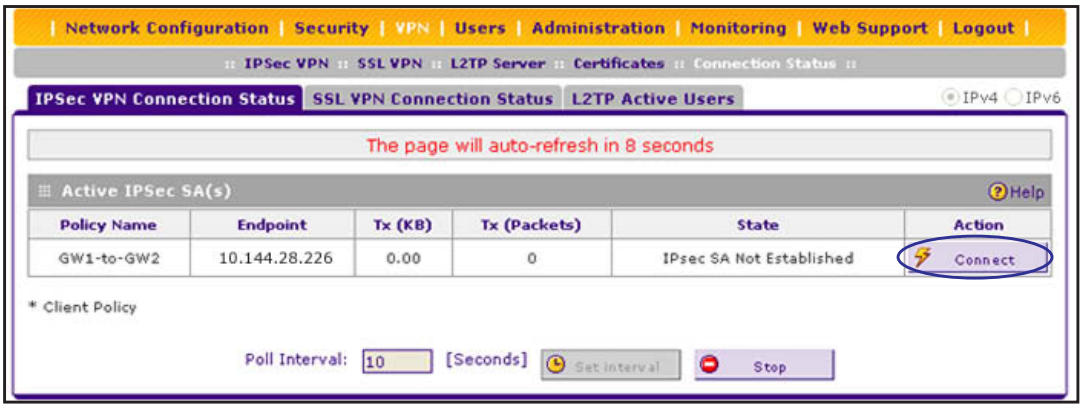

Figure 111.

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

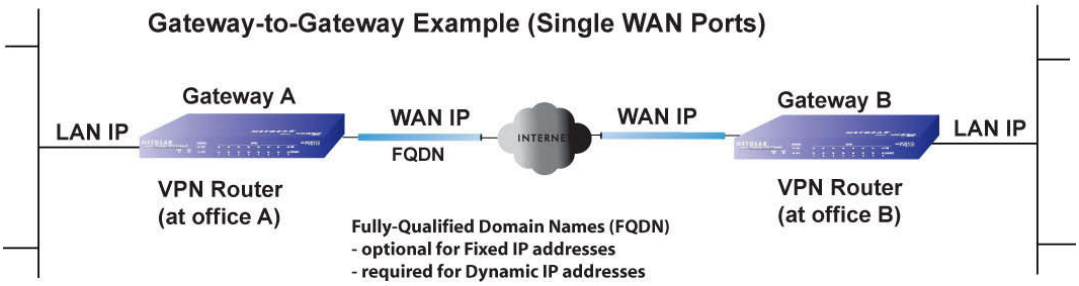

Figure 112.

➢ **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.)

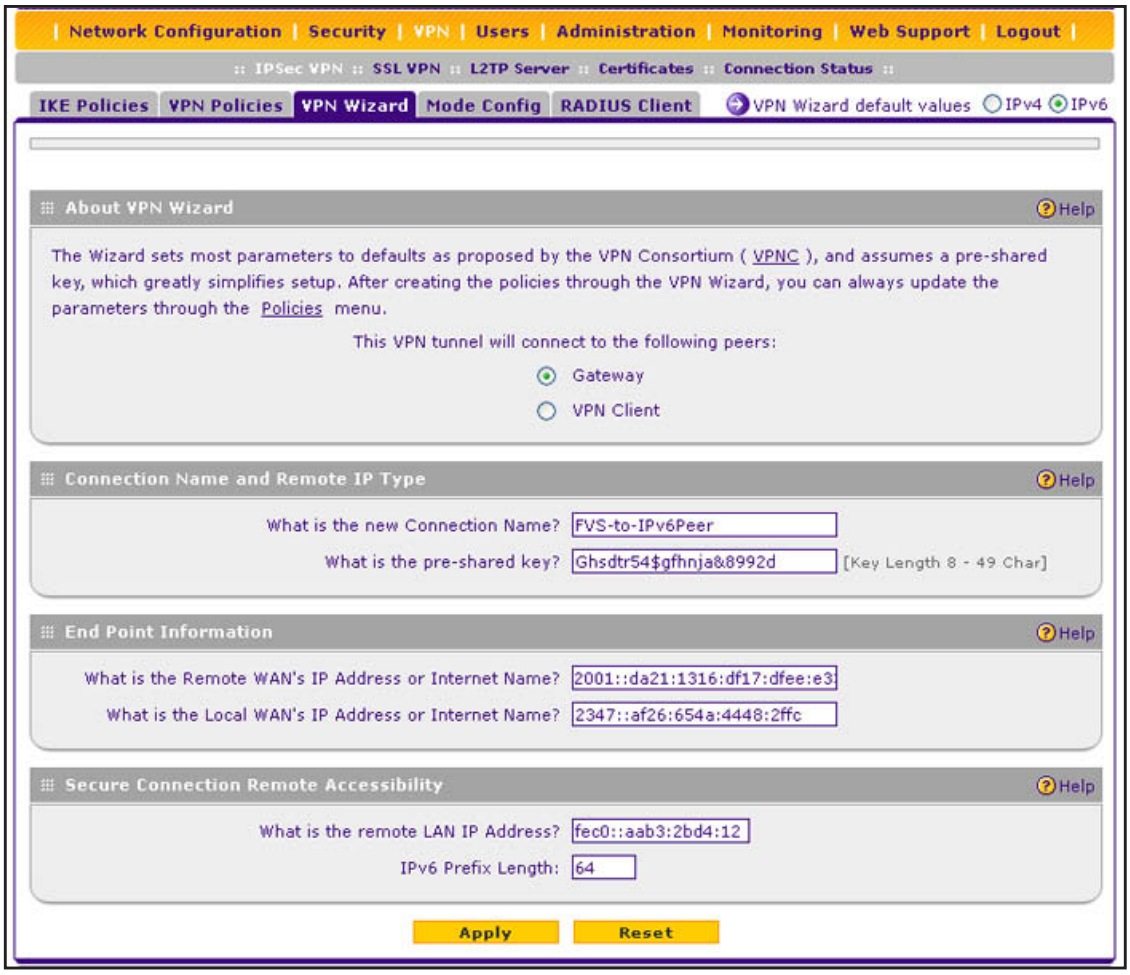

Figure 113.

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.

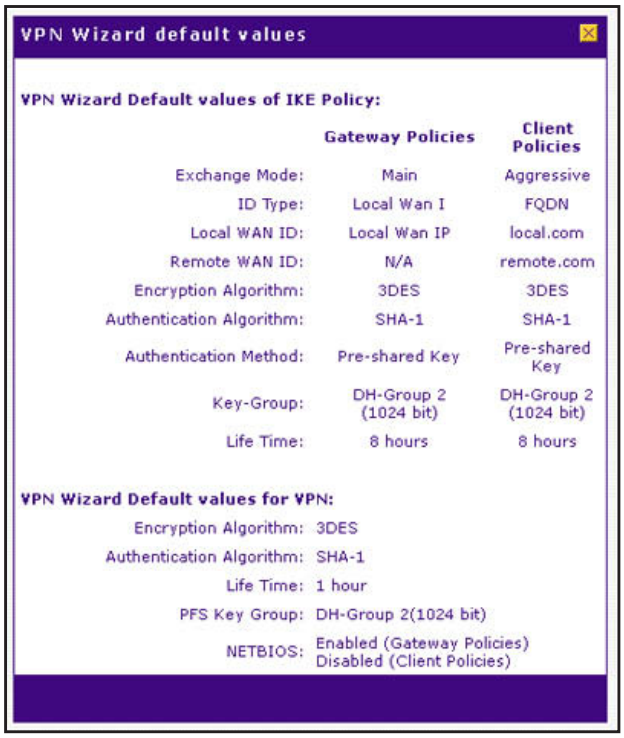

Figure 114.

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

Table 43. 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.
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 wireless VPN firewall's active WAN interface is automatically entered.

Table 43. IPSec VPN Wizard settings for an IPv6 gateway-to-gateway tunnel (continued)

Setting	Description
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 261.

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 115.

5. Configure a VPN policy on the remote gateway that allows connection to the wireless 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:

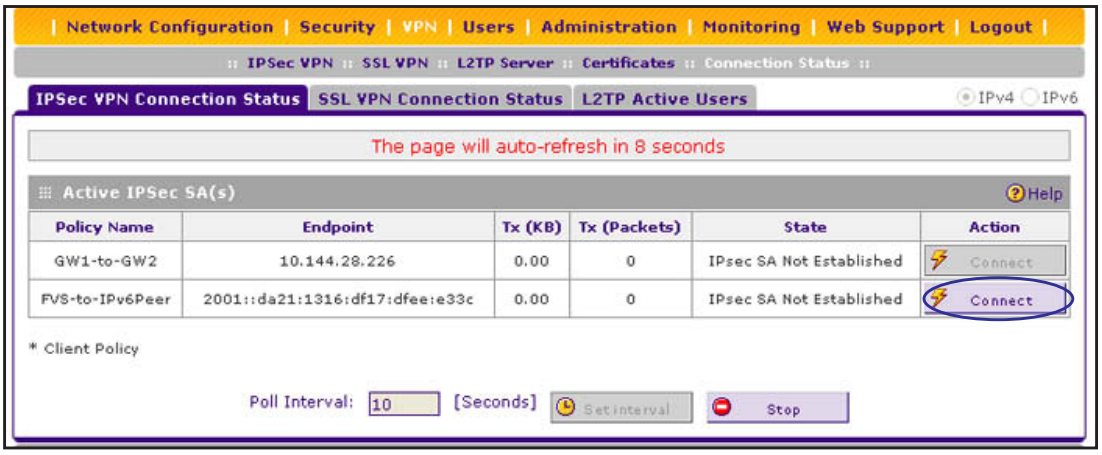

Figure 116.

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

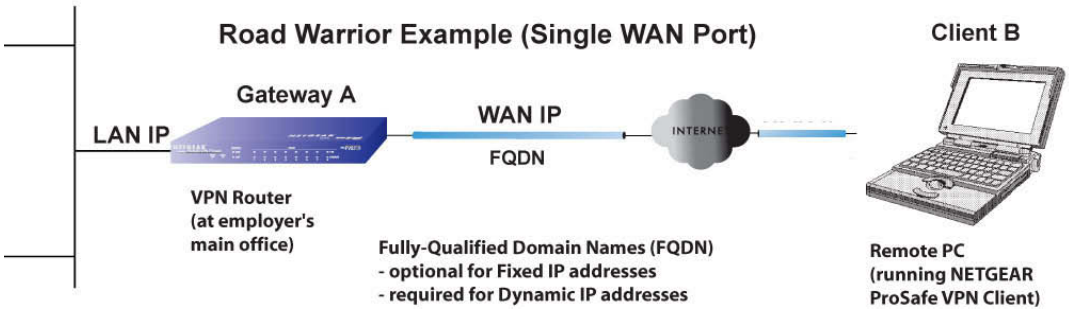

Figure 117.

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 205.
- *Use the NETGEAR VPN Client Wizard to Create a Secure Connection* on page 207 *or Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 212.

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.)

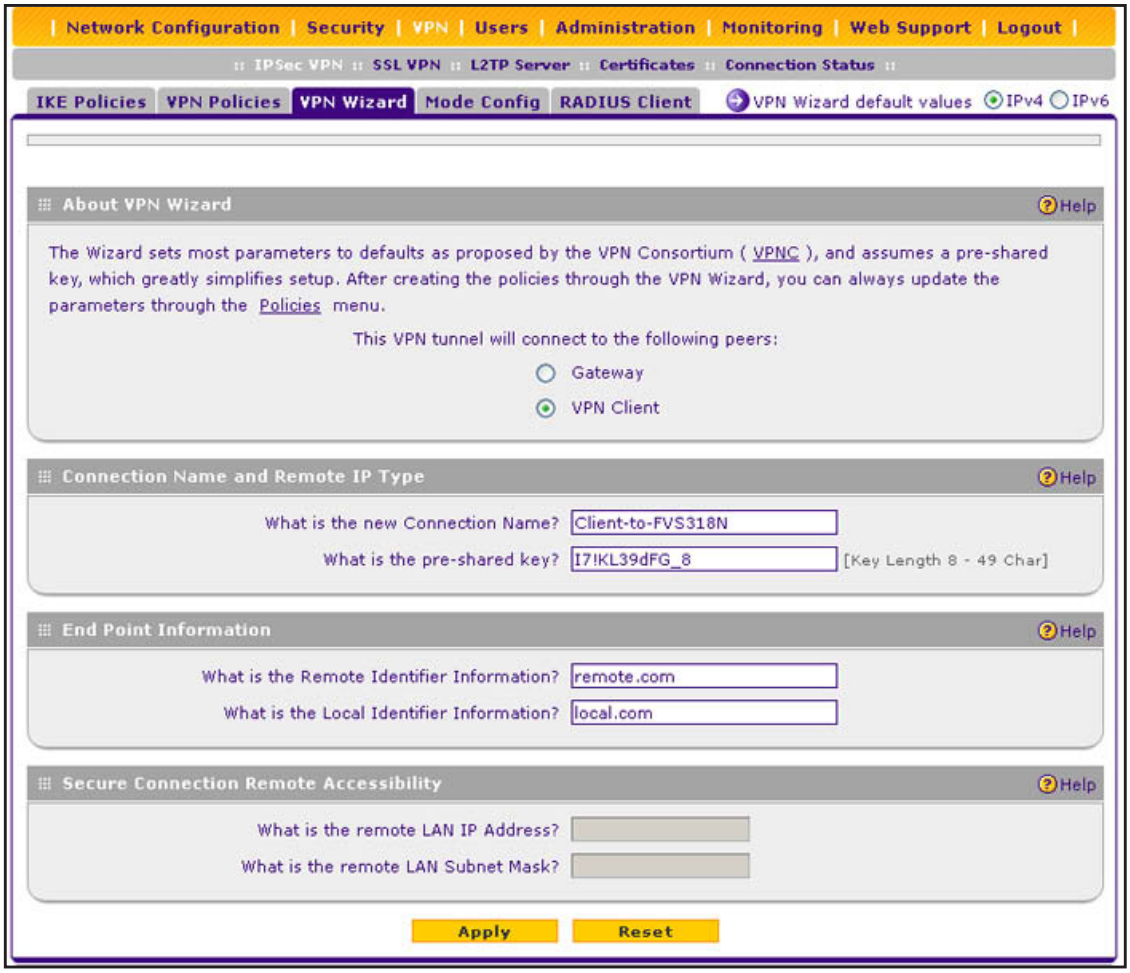

Figure 118.

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 109* on page 198), 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 44. 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.
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 wireless 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 wireless 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 wireless 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 wireless 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.

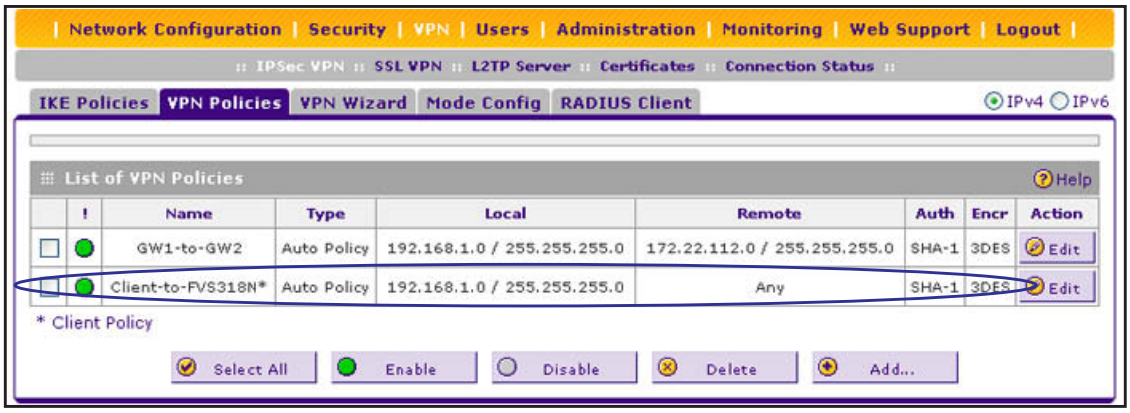

Figure 119.

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 45. 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 212) 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 wireless 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 wireless VPN firewall:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays:

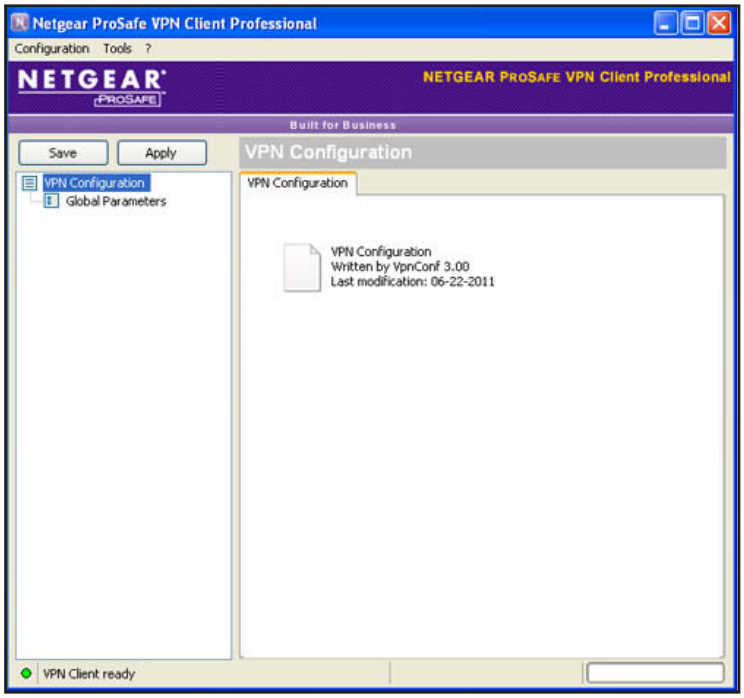

Figure 120.

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 121.

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:

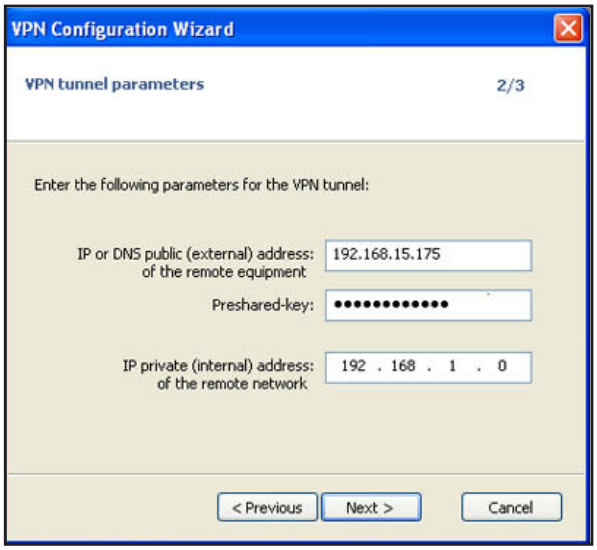

Figure 122.

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 wireless VPN firewall. For example, enter **192.168.15.175**.
   - **Preshared key**. Enter the pre-shared key that you already specified on the wireless VPN firewall. For example, enter **I7!KL39dFG_8**.
   - **IP private (internal) address of the remote network**. Enter the remote private IP address of the wireless 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:

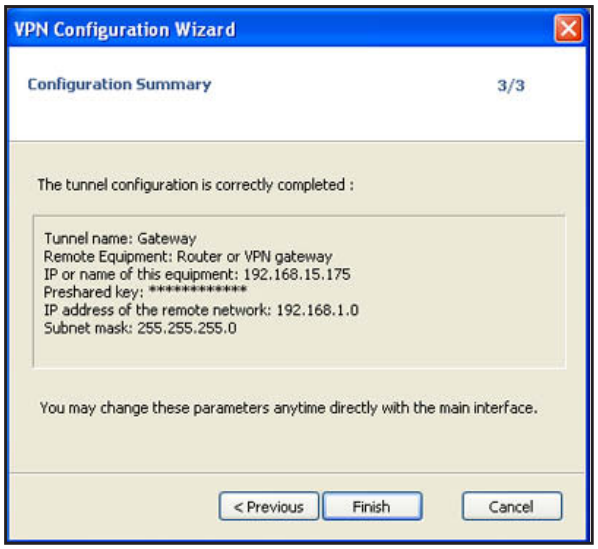

Figure 123.

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:

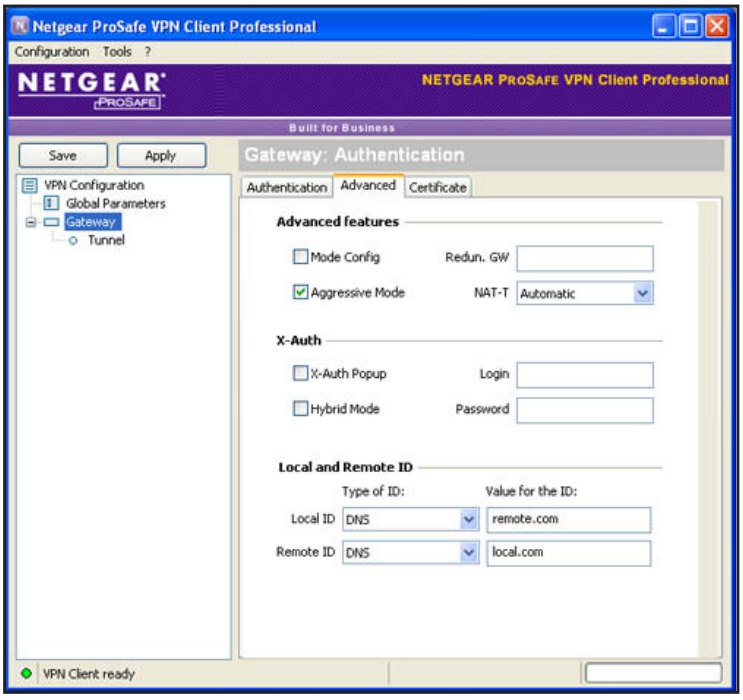

Figure 124.

c. Specify the settings that are described in the following table.

Table 46. 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 wireless VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and wireless 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 wireless 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 wireless 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 wireless 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 wireless VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the wireless VPN firewall. **Note:** The local ID on the wireless 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 wireless 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:

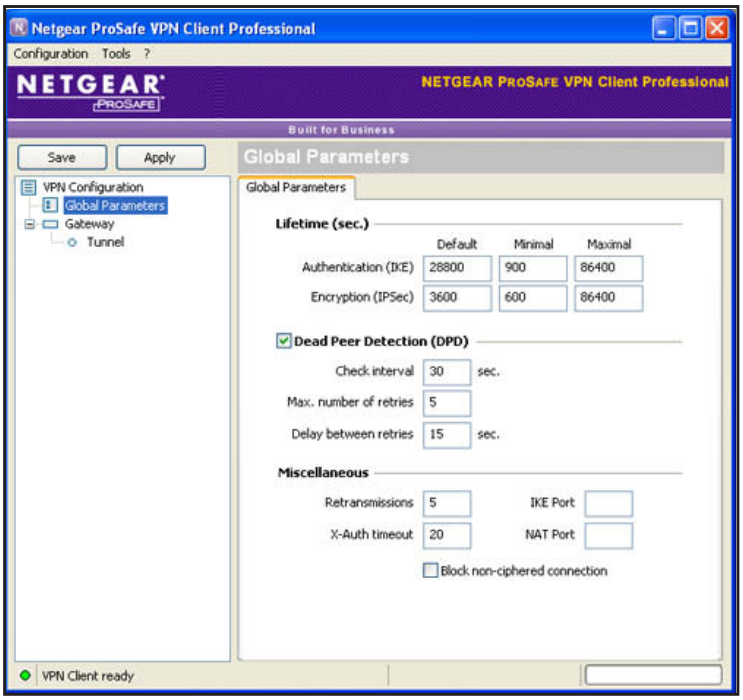

Figure 125.

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 wireless VPN firewall.
- **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the wireless 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 wireless 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:

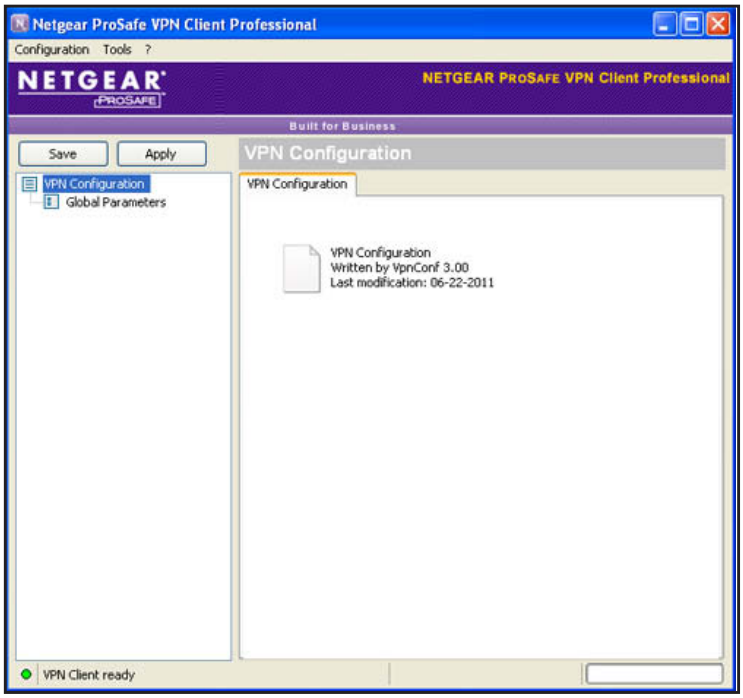

Figure 126.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.

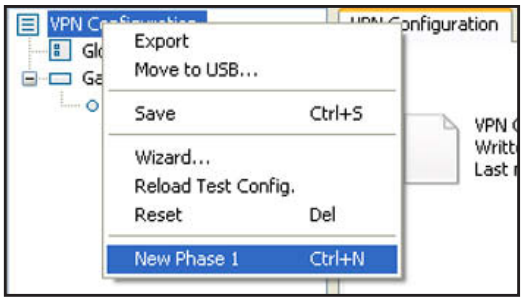

Figure 127.

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.

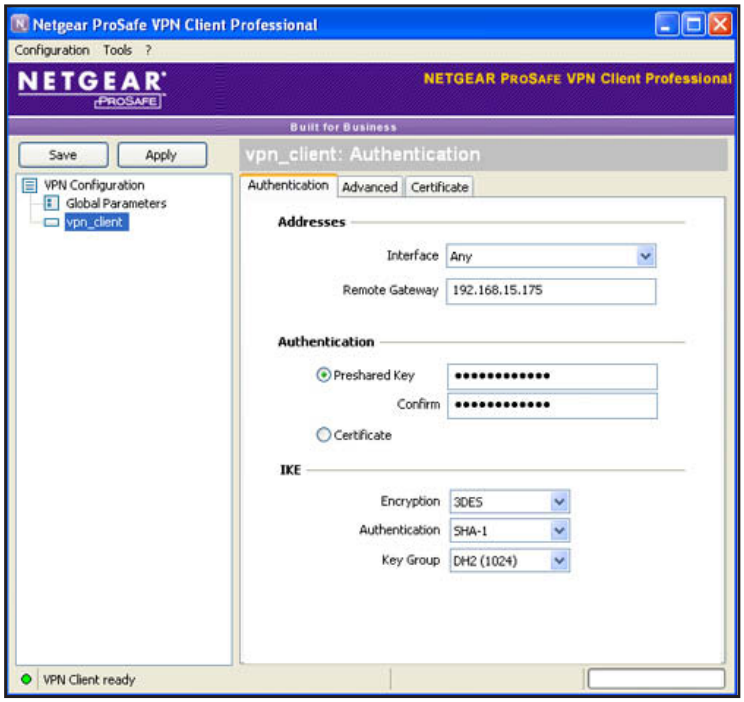

Figure 128.

4. Specify the settings that are described in the following table.

Table 47. 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 wireless 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 wireless 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 wireless 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:

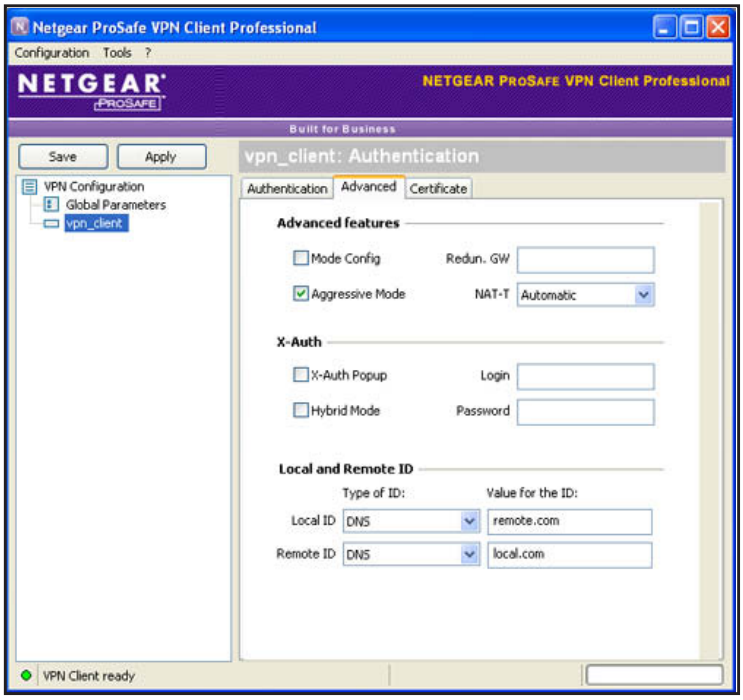

Figure 129.

7. 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 wireless VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and wireless 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 wireless 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 wireless 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 wireless VPN firewall and then enter client.com as the local ID on the VPN client.

Table 48. VPN client advanced authentication settings (continued)

Setting	Description
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the wireless VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the wireless VPN firewall. **Note:** The local ID on the wireless 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 wireless 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 wireless 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:

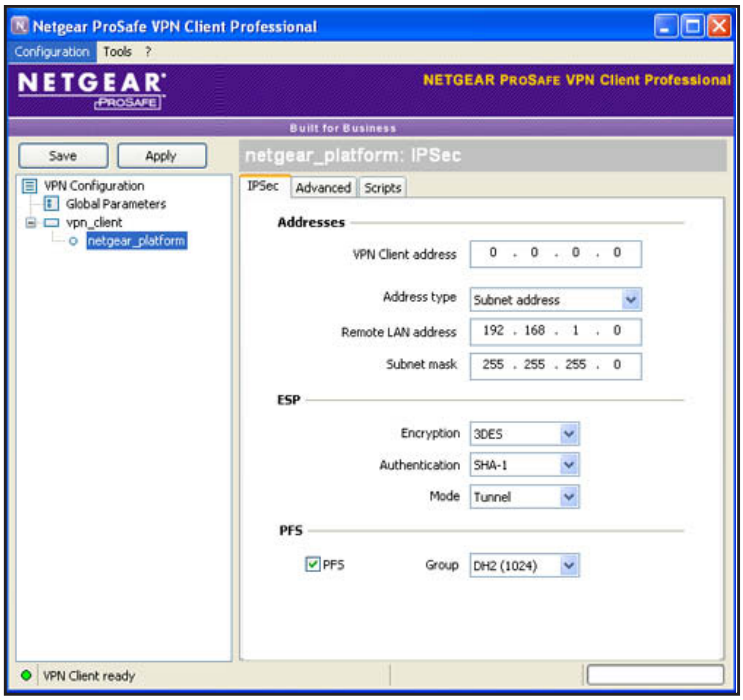

Figure 130.

3. Specify the settings that are described in the following table.

Table 49. 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 wireless 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 wireless 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:

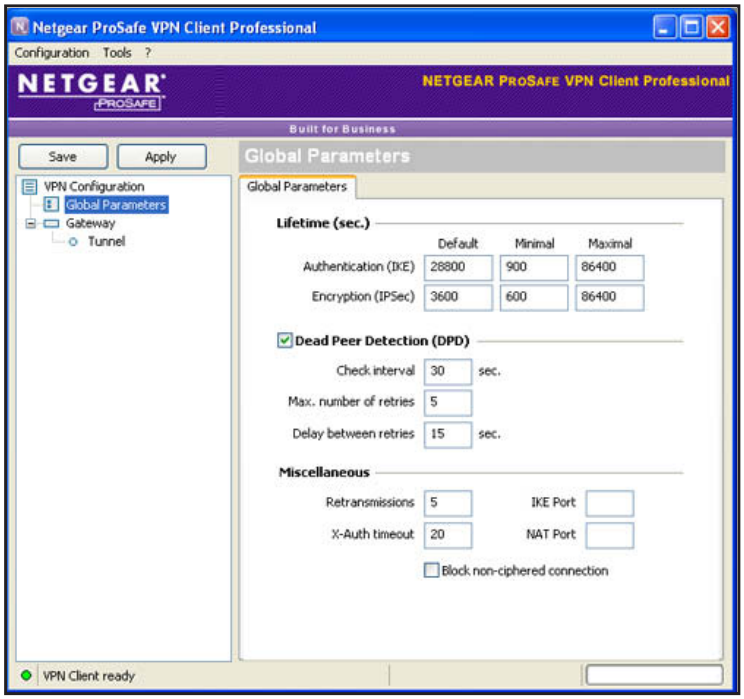

Figure 131.

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 wireless VPN firewall.
   - **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the wireless VPN firewall.
3. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The wireless VPN firewall configuration is now complete.

Test the Connection and View Connection and Status Information

Both the NETGEAR ProSafe VPN Client and the wireless 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**.

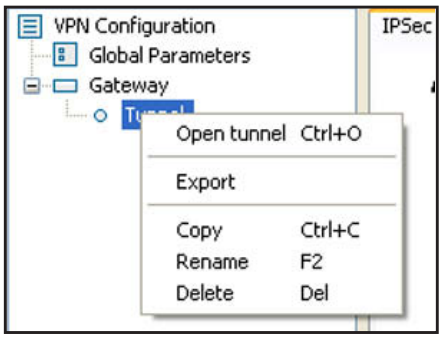

Figure 132.

- **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 133.

- **Use the system-tray icon**. Right-click the system tray icon, and select **Open tunnel 'Tunnel'**.

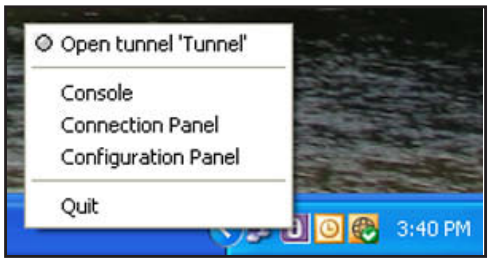

Figure 134.

Whichever way you choose to open the tunnel, when the tunnel opens successfully, the *Tunnel opened* message displays above the system tray:

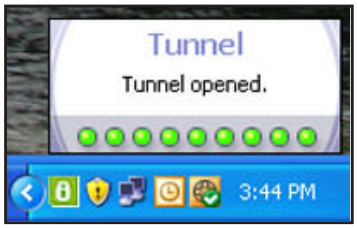

Figure 135.

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:

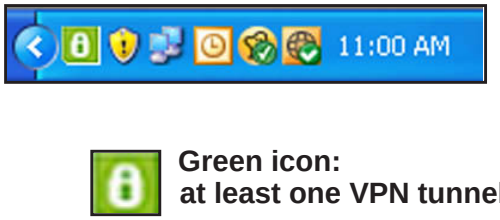

Figure 136.

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:

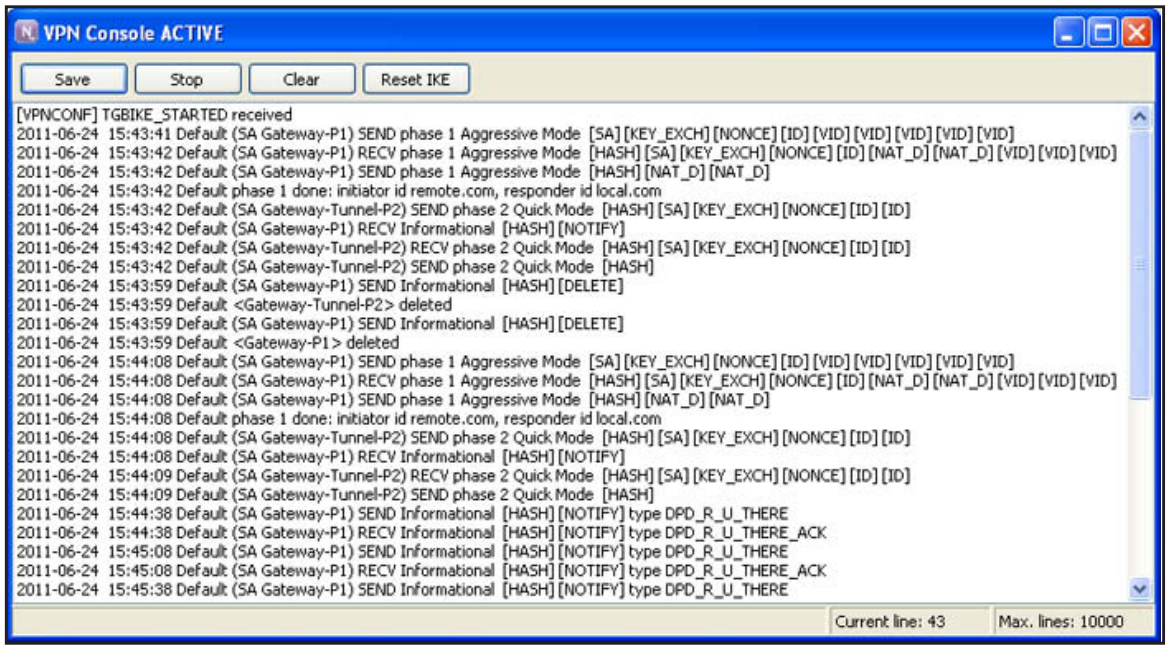

Figure 137.

View the Wireless 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.)

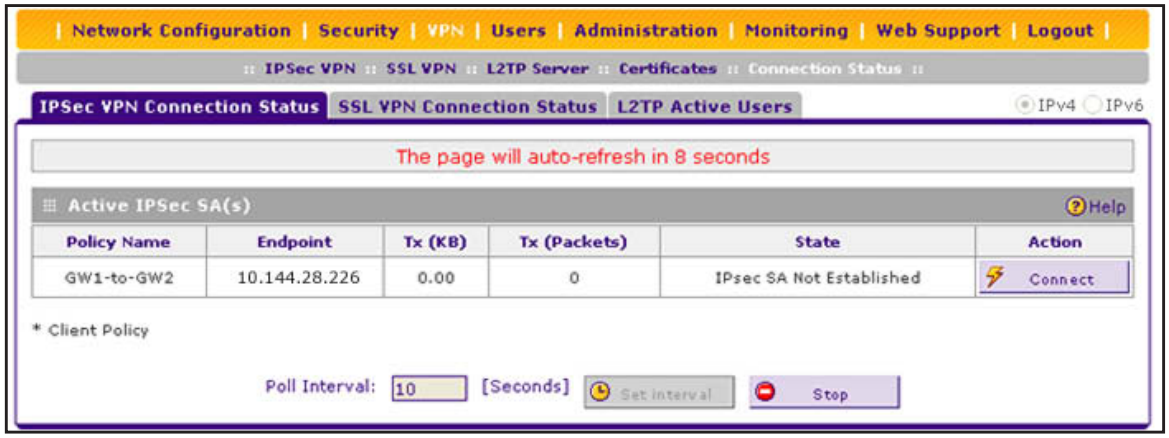

Figure 138.

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 50. 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 Wireless VPN Firewall IPSec VPN Log

➢ **To display the IPSec VPN log:**

Select **Monitoring > VPN Logs > IPSec VPN Logs.** The IPSec VPN Logs screen displays:

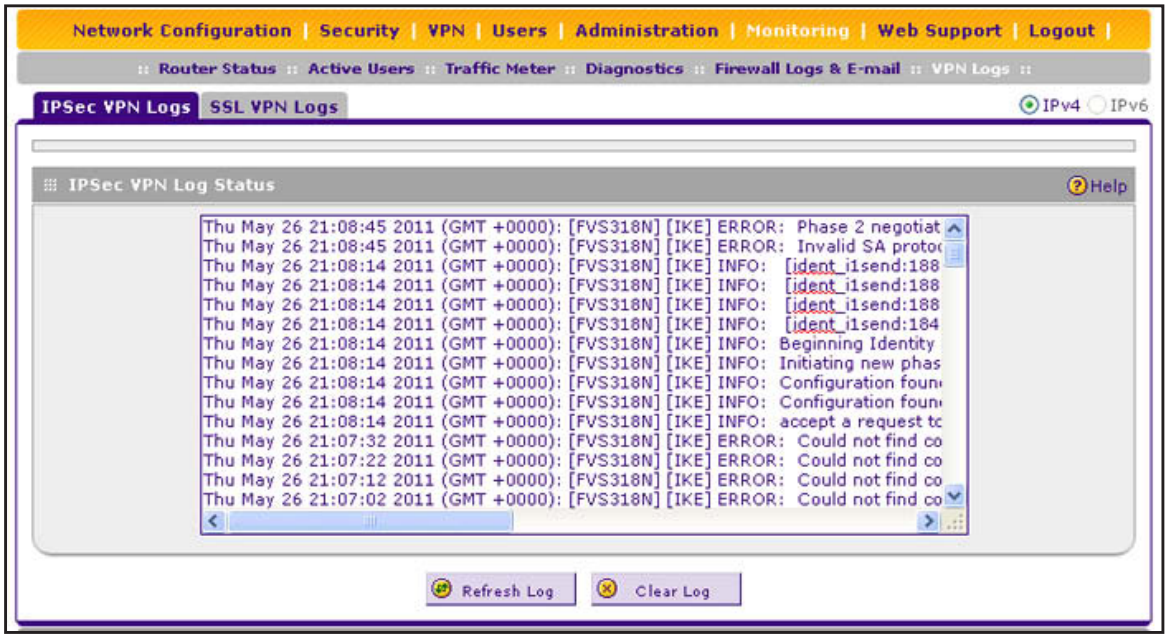

Figure 139.

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 143* on page 234) 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.

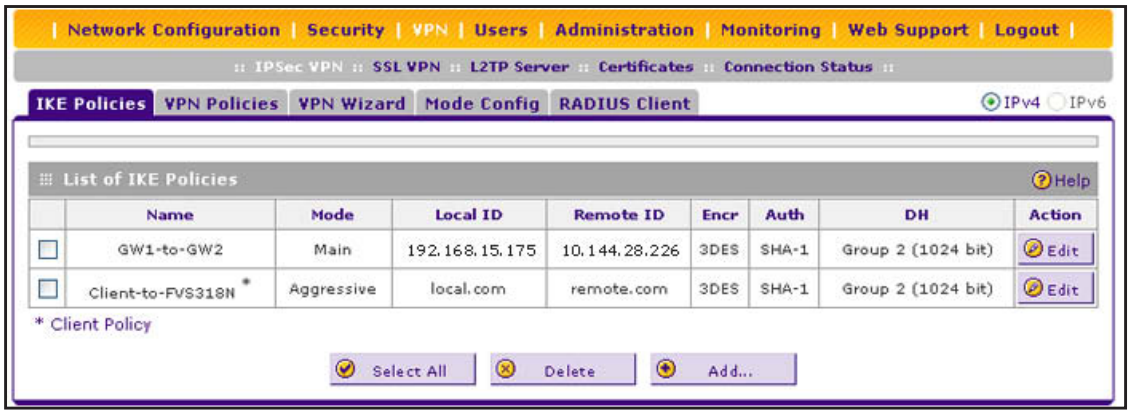

Figure 140.

Each policy contains the data that are described in the following table. These fields are described in more detail in *Table 52* on page 227.

Table 51. 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 wireless 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 225.

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 140* on page 224).
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).

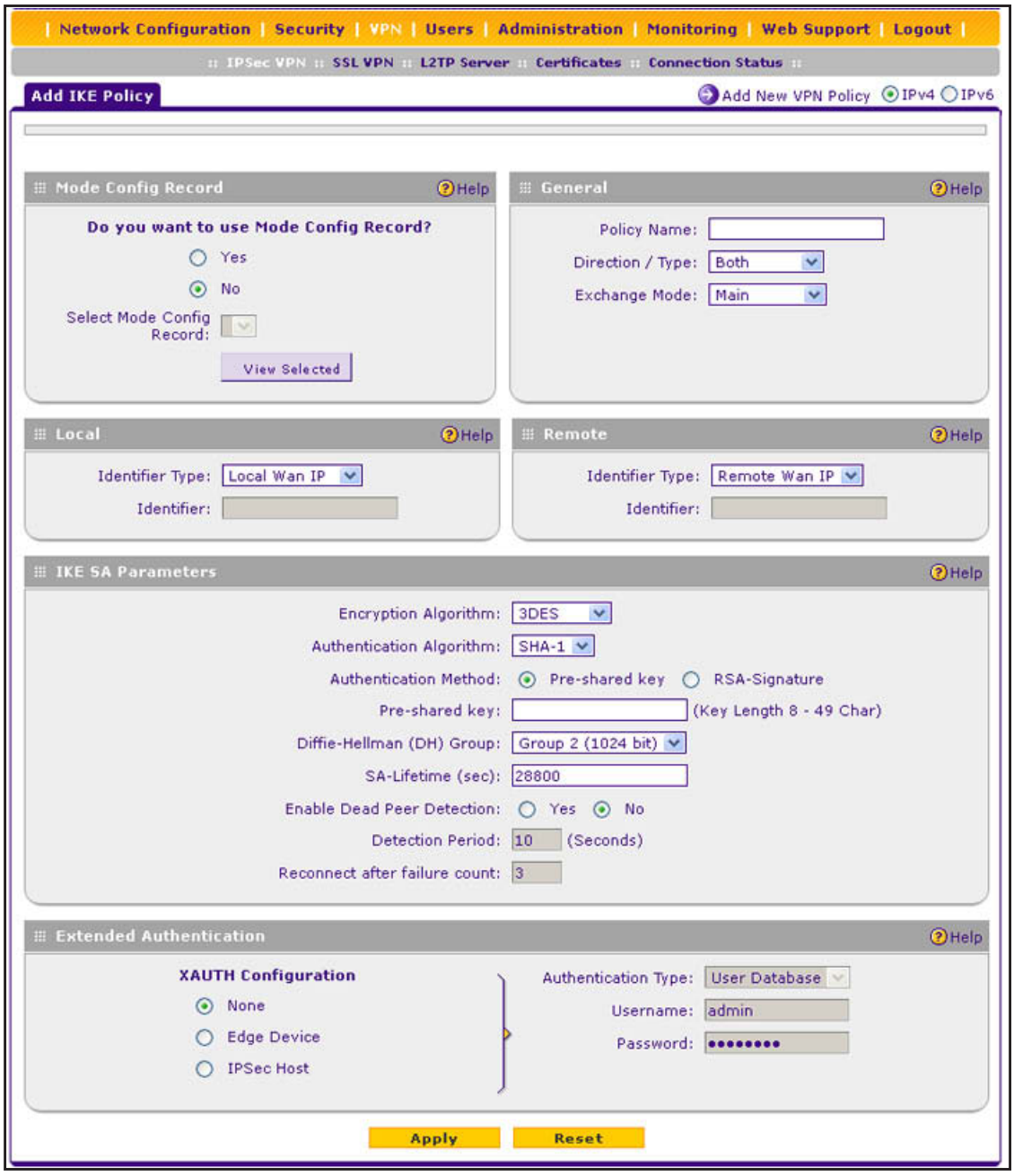
Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status ::
Add IKE Policy
Add New VPN Policy IPv4 IPv6
Mode Config Record
Help
Do you want to use Mode Config Record?
Yes
No
Select Mode Config Record:
View Selected
General
Help
Policy Name:
Direction / Type: Both
Exchange Mode: Main
Local
Help
Identifier Type: Local Wan IP
Identifier:
Remote
Help
Identifier Type: Remote Wan IP
Identifier:
IKE SA Parameters
Help
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: Pre-shared key RSA-Signature
Pre-shared key: (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800
Enable Dead Peer Detection: Yes No
Detection Period: 10 (Seconds)
Reconnect after failure count: 3
Extended Authentication
Help
XAUTH Configuration
None
Edge Device
IPSec Host
Authentication Type: User Database
Username: admin
Password: ••••••••
Apply
Reset

Figure 141.

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

Table 52. 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 244. 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 Wireless VPN Firewall* on page 245). **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 wireless VPN firewall: • **Initiator**. The wireless VPN firewall initiates the connection to the remote endpoint. • **Responder**. The wireless VPN firewall responds only to an IKE request from the remote endpoint. • **Both**. The wireless 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 wireless 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.	

Table 52. Add IKE Policy screen settings (continued)

Setting	Description	
Local		
Identifier	From the drop-down list, select one of the following ISAKMP identifiers to be used by the wireless VPN firewall, and specify the identifier in the Identifier field: • **Local Wan IP**. The WAN IP address of the wireless 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 wireless VPN firewall. • **User FQDN**. The email address for a local VPN client or the wireless VPN firewall. • **DER ASN1 DN**. A distinguished name (DN) that identifies the wireless 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 52. 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 wireless 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 319). 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 (eight hours).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 260.	Select a radio button to specify whether Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the wireless 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 wireless 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 wireless VPN firewall tears down the connection and then attempts to reconnect to the peer. The default is three failures.

Table 52. 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 240.	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 wireless 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 wireless VPN firewall functions as a VPN client of the remote gateway. In this configuration, the wireless 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 wireless VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 241). • **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 wireless VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client and Server Configuration* on page 241. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client and Server Configuration* on page 241.
	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 140* on page 224).
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 141* on page 226).

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 wireless 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 316). For gateways to use a CA to perform authentication, each VPN gateway needs to have a certificate from the CA. Each certificate contains 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.

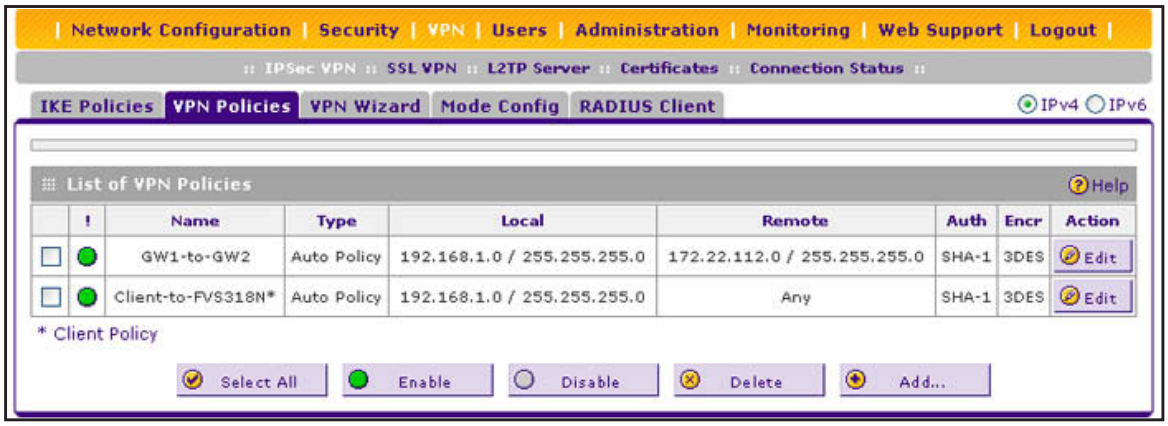

Figure 142.

Each policy contains the data that are described in the following table. These fields are described in more detail in *Table 54* on page 236.

Table 53. 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 142* on page 232).
  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 143* on page 234).
  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 144* on page 235).

Figure 143. Add New VPN Policy screen for IPv4

Figure 144. 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 54. 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.	
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.	
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 263. This feature is disabled by default.	
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 225.	
Enable Keepalive **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 260.	Select a radio button to specify if keep-alive is enabled: • **Yes**. This feature is enabled: Periodically, the wireless 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 wireless 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 wireless 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 wireless VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is three keep-alive requests.

Table 54. 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 wireless VPN firewall: • **Any**. All computers and devices on the network. You cannot select Any for both the wireless 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 three and eight 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 54. 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. • **None**. Key does not apply. • **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 three and eight 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 54. 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 142* on page 232).
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 143* on page 234; for IPv6 see *Figure 144* on page 235).
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 wireless 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 wireless 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 wireless 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 wireless 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 140* on page 224).
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 141* on page 226).

4. In the Extended Authentication section on the screen, complete the settings as described in the following table:

Table 55. 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 wireless 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 wireless VPN firewall functions as a VPN client of the remote gateway. In this configuration, the wireless 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 wireless VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 241). • **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 wireless VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client and Server Configuration* on page 241. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client and Server Configuration* on page 241.
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 306.

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:

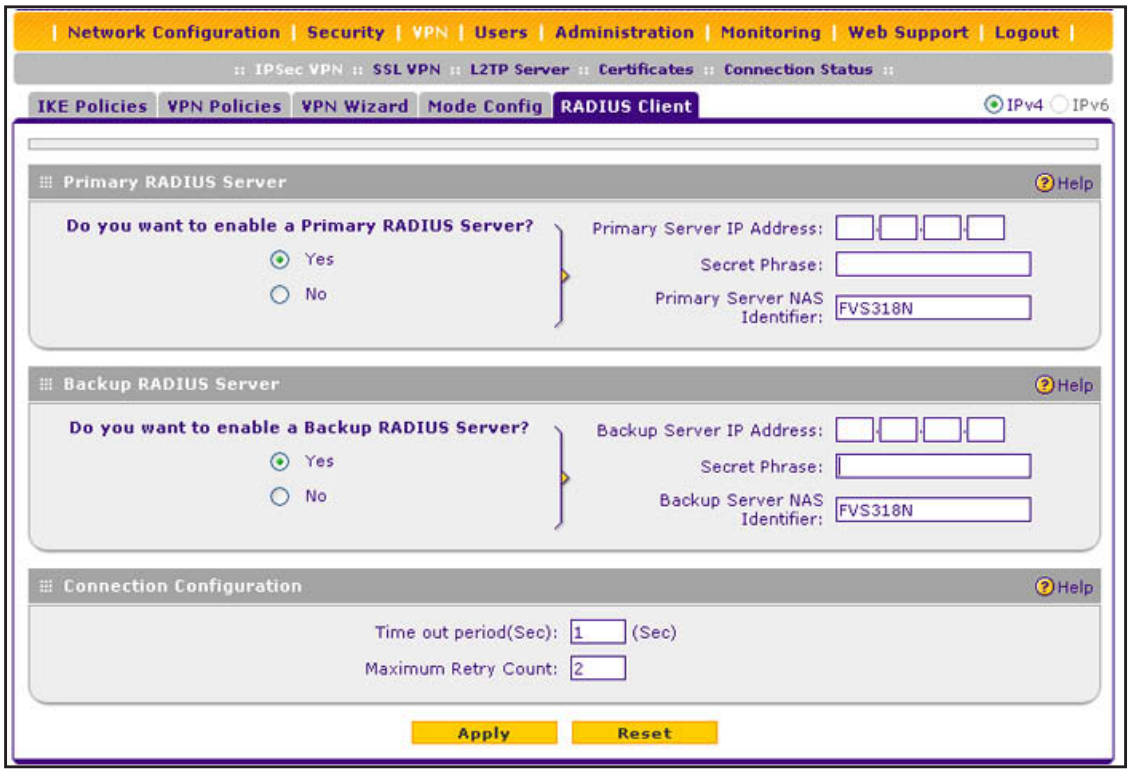

Figure 145.

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

Table 56. 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.	

Table 56. RADIUS Client screen settings (continued)

Setting	Description
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.
Primary Server NAS Identifier	The primary Network Access Server (NAS) identifier that needs to be present in a RADIUS request. **Note:** The wireless 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 wireless 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 wireless 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 wireless VPN firewall attempts to connect to a RADIUS server. The default setting is four 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 240).

Assign IPv4 Addresses to Remote Users (Mode Config)

To simplify the process of connecting remote VPN clients to the wireless 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 wireless 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 147* on page 246).

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 Wireless VPN Firewall* on page 245). 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 Wireless VPN Firewall

To configure Mode Config on the wireless 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 wireless VPN firewall:**

1. Select **VPN > IPSec VPN > Mode Config**. The Mode Config screen displays:

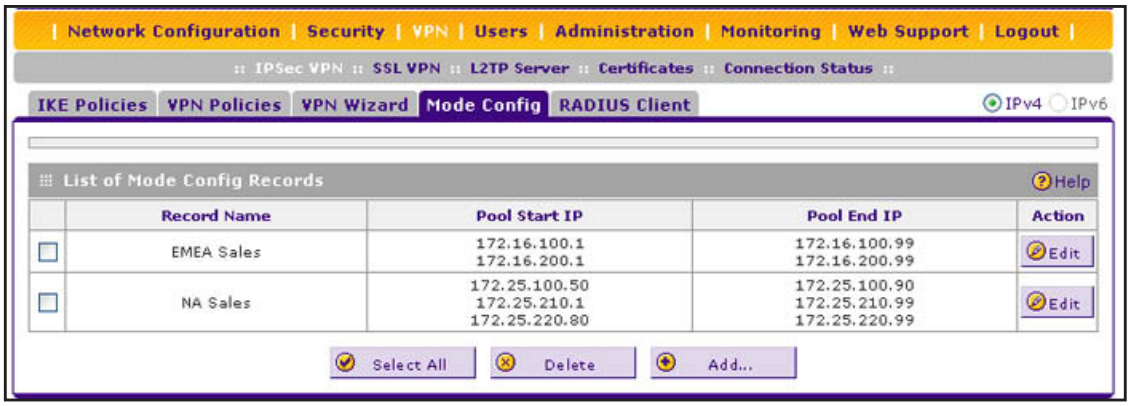

Figure 146.

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

- For EMEA Sales, a first pool (172.16.100.1 through 172.16.100.99) and second pool (172.16.200.1 through 172.16.200.99) are shown.
- For NA Sales, a first pool (172.25.100.50 through 172.25.100.99), a second pool (172.25.210.1 through 172.25.210.99), and a third pool (172.25.220.80 through 172.25.220.99) are shown.

2. Under the List of Mode Config Records table, click the **Add** table button. The Add Mode Config Record screen displays:

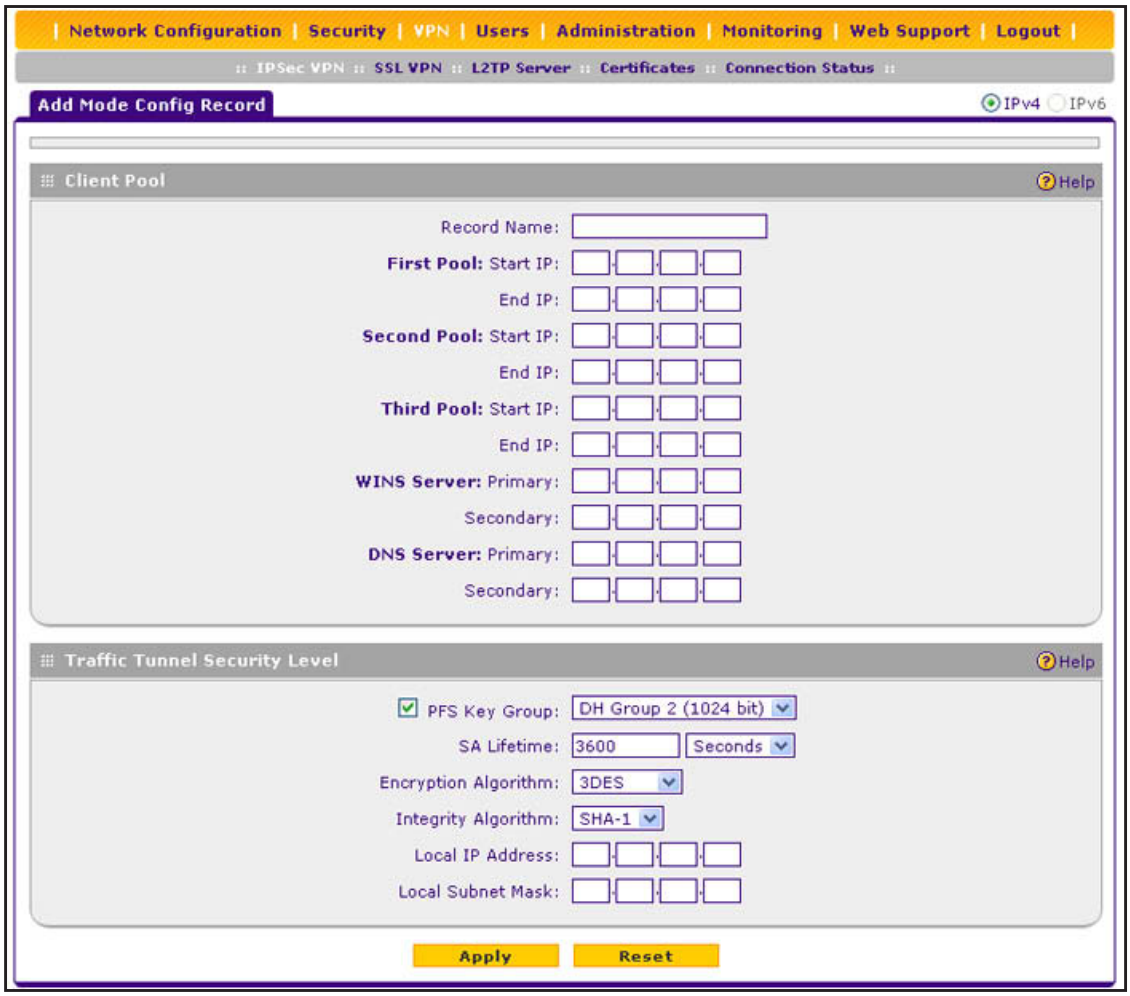

Figure 147.

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

Table 57. 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 wireless 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	

Table 57. Add Mode Config Record screen settings (continued)

Setting	Description
WINS Server	If there is a WINS server on the local network, enter its IP address in the Primary field. You can enter the IP address of a second WINS server in the Secondary field.
DNS Server	Enter the IP address of the DNS server that is used by remote VPN clients in the Primary field. You can enter the IP address of a second DNS server in the Secondary field.
Traffic Tunnel Security Level **Note:** Generally, the default settings work well for a Mode Config configuration.	
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and 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.
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 wireless 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 140* on page 224).
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.

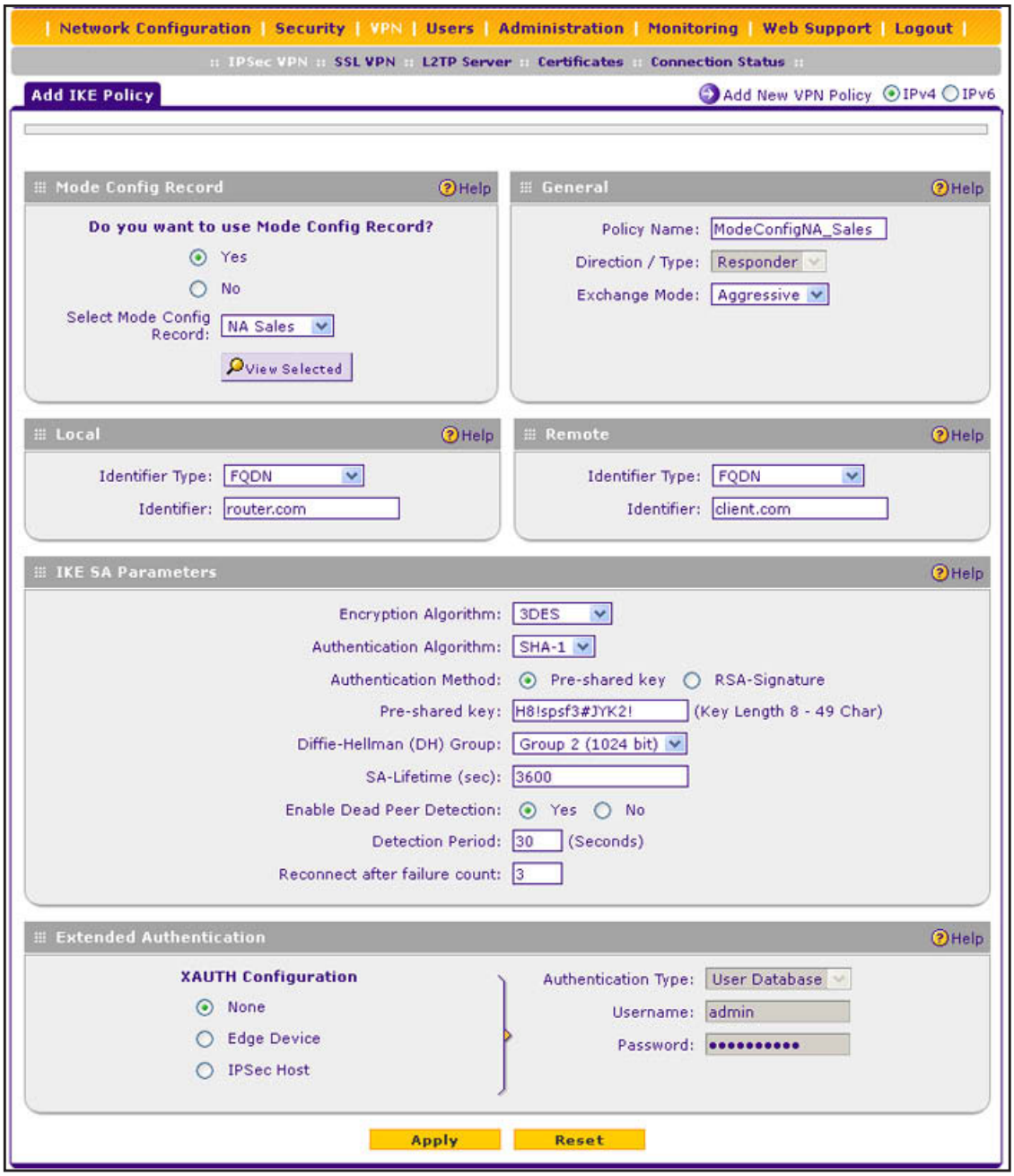

Figure 148.

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 52* on page 227 explains the general IKE policy settings.

Table 58. 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 248. This example uses NA Sales.
General		
Policy Name	A descriptive name of the IKE policy for identification and management purposes. This example uses ModeConfigNA_Sales. **Note:** The name is not supplied to the remote VPN endpoint.	
Direction / Type	Responder is automatically selected when you select the Mode Config record in the Mode Config Record section of the screen. This ensures that the wireless 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		
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the wireless VPN firewall (that is, the local endpoint) is defined by an FQDN.	
	Identifier	Enter an FQDN for the wireless 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 58. 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 eight 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 (eight hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (one hour).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 260.	Select a radio button to specify whether Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the wireless 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 wireless 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 wireless VPN firewall tears down the connection and then attempts to reconnect to the peer. The default setting is three failures.

Table 58. 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 240.	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 wireless 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 wireless VPN firewall functions as a VPN client of the remote gateway. In this configuration, the wireless 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 wireless VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 241). • **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 wireless VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client and Server Configuration* on page 241. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client and Server Configuration* on page 241.
	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 wireless 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 wireless 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:

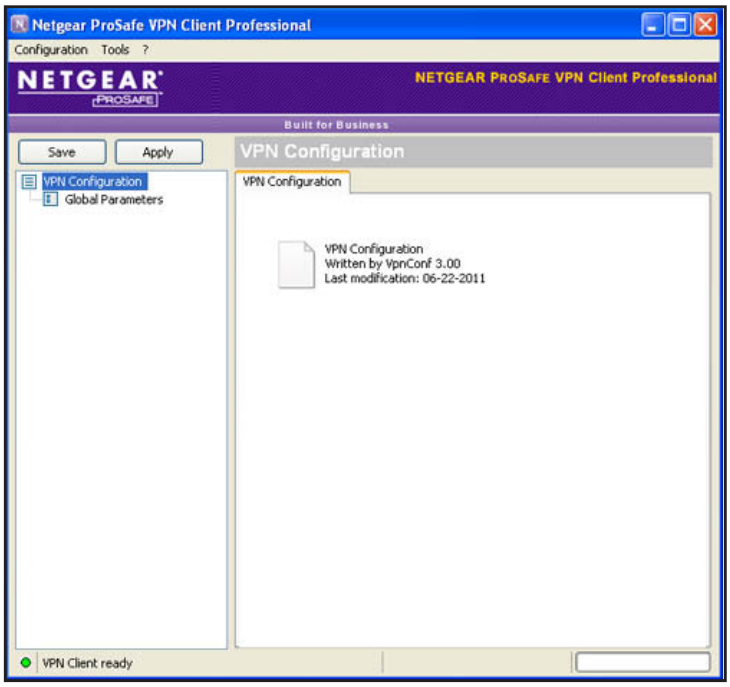

Figure 149.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.

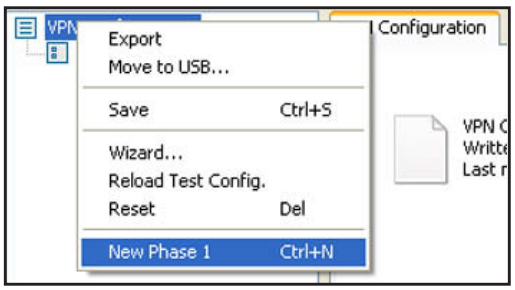

Figure 150.

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:

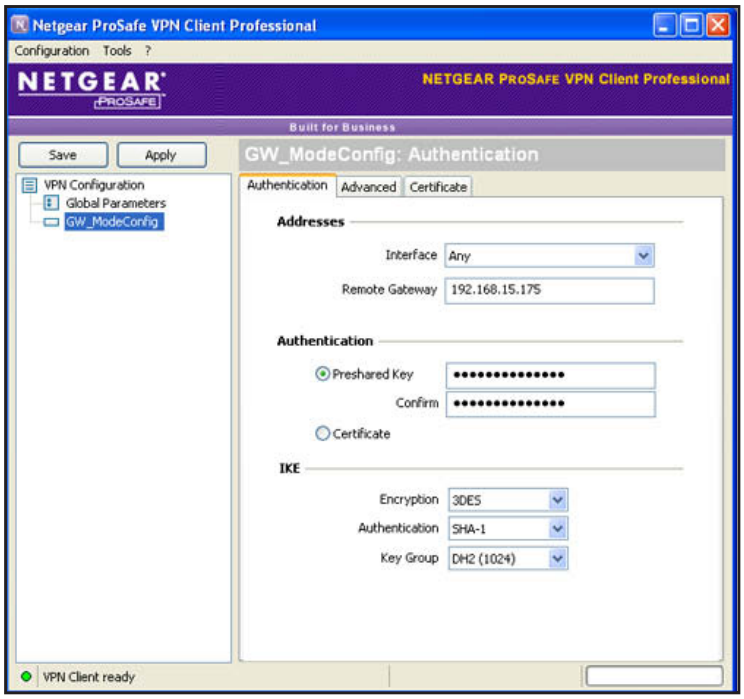

Figure 151.

4. Specify the settings that are described in the following table.

Table 59. 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 wireless 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 wireless VPN firewall. For example, enter **H8!spsf3#JYK2!**. Confirm the key in the Confirm field.

Table 59. 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 wireless 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:

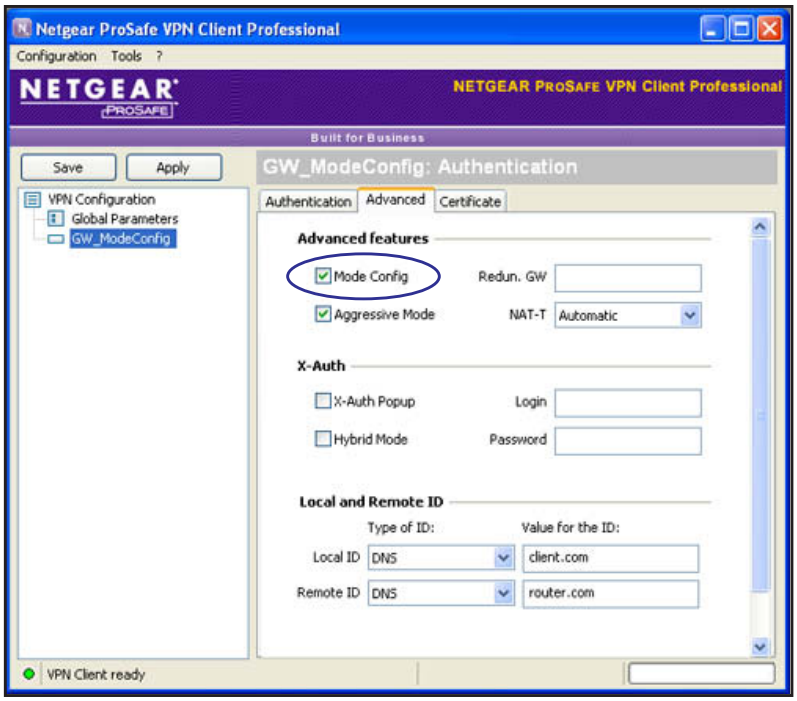

Figure 152.

7. Specify the settings that are described in the following table.

Table 60. 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 wireless VPN firewall.

Table 60. 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 wireless 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 wireless 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 wireless 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 wireless VPN firewall configuration. As the value of the ID, enter **router.com** as the remote ID for the wireless VPN firewall. **Note:** The local ID on the wireless 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 wireless 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:

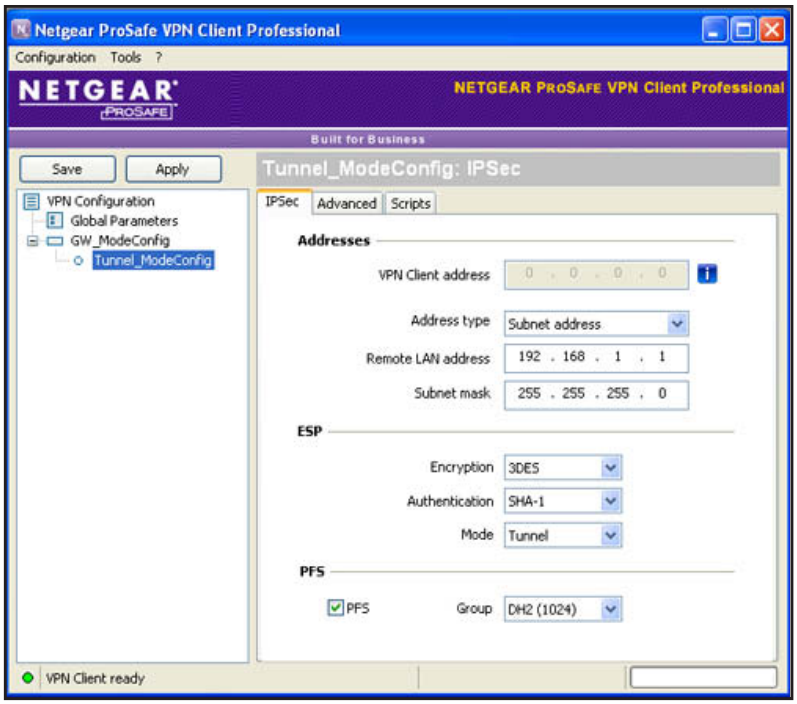

Figure 153.

3. Specify the settings that are described in the following table.

Table 61. 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 wireless VPN firewall displays in this field (see *Figure 158* on page 261).
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 wireless VPN firewall: • If you left the Local IP Address field blank, enter the wireless 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 wireless 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 wireless VPN firewall. If you left the Local Subnet Mask field blank, enter the wireless VPN firewall's default IP subnet mask.

Table 61. 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 wireless 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:

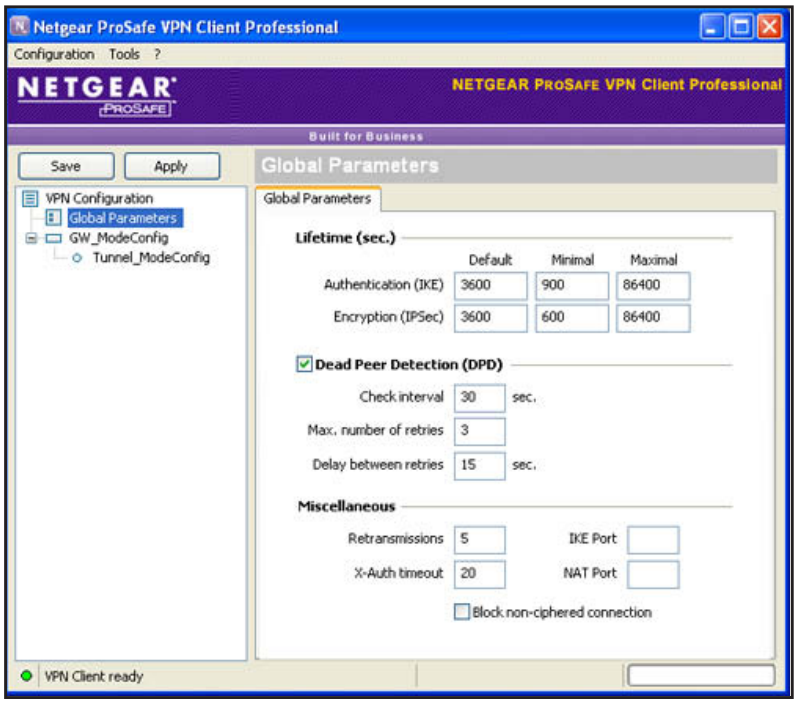

Figure 154.

2. Specify the following default lifetimes in seconds to match the configuration on the wireless VPN firewall:
   - **Authentication (IKE)**, **Default**. Enter **3600** seconds.

     Note: *The default setting is 28800 seconds (eight hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (one 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 wireless 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 wireless VPN firewall:**

1. Right-click the system tray icon, and select **Open tunnel 'Tunnel_ModeConfig'**.

Figure 155.

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.

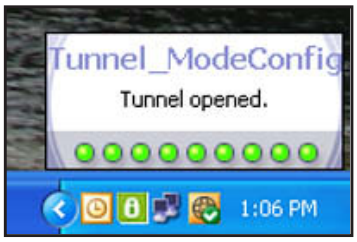

Figure 156.

2. Verify that the wireless 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.)

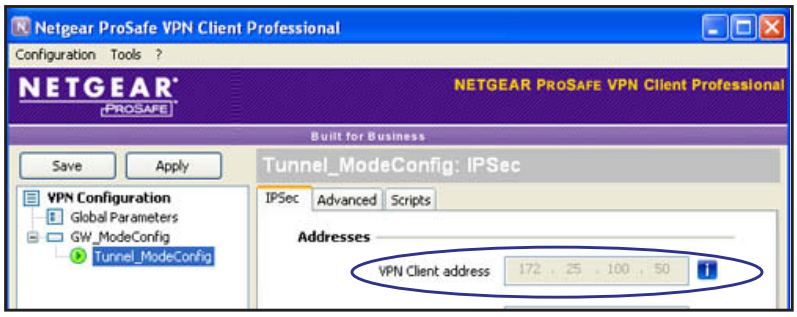

Figure 157.

3. From the client computer, ping a computer on the wireless 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 146* on page 245), 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 147* on page 246).
2. Modify the settings as described in *Table 57* on page 246.
3. Click **Apply** to save your settings.

➢ **To delete one or more Mode Config records:**

1. On the Mode Config screen (see *Figure 146* on page 245), 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 142* on page 232).
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.)

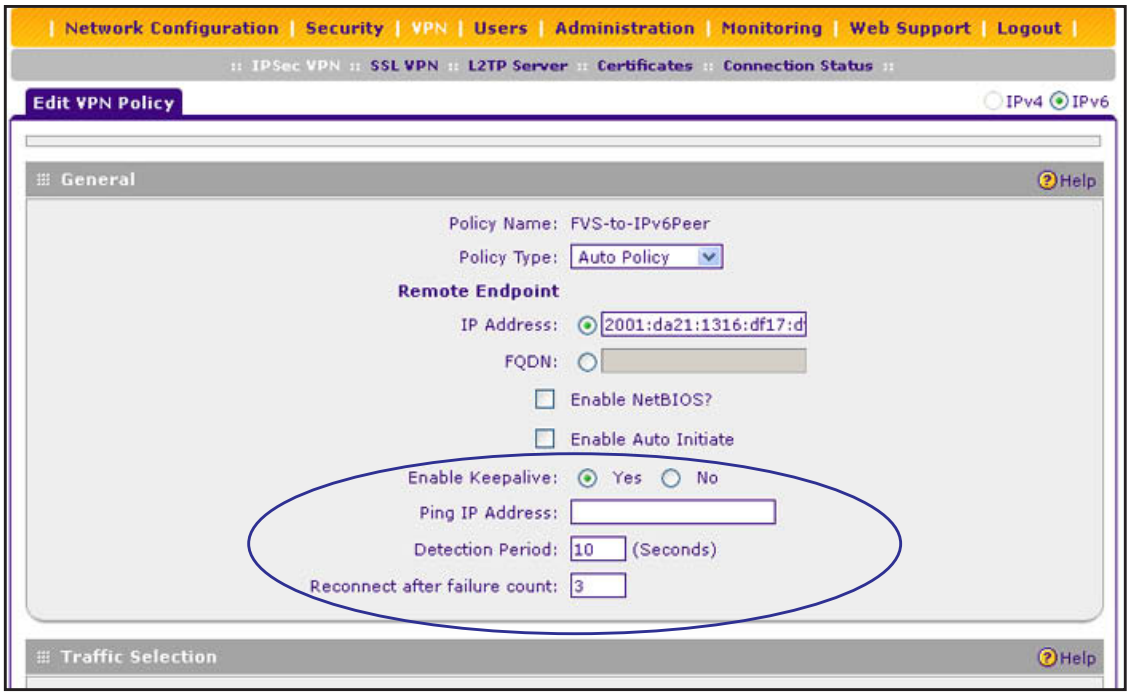

Figure 158.

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

Table 62. Keep-alive settings

Setting	Description	
General		
Enable Keepalive	Select the **Yes** radio button to enable the keep-alive feature. Periodically, the wireless 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 wireless VPN firewall sends in the Reconnect after failure count field.	
	Ping IP Address	The IP address that the wireless 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 wireless VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is three keep-alive requests.

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

Configure Dead Peer Detection

The Dead Peer Detection (DPD) feature lets the wireless 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 140* on page 224).
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).

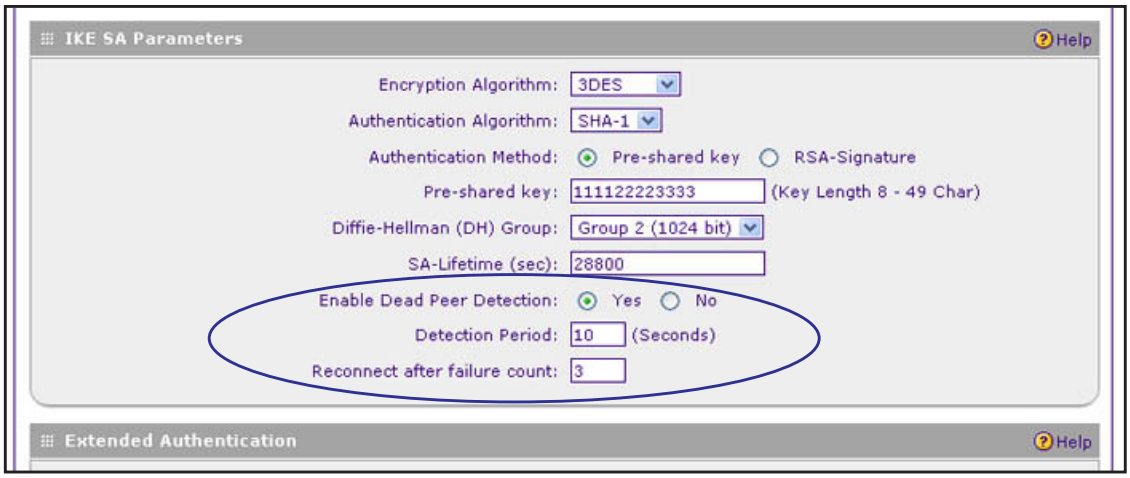

Figure 159.

4. In the IKE SA Parameters section of the screen, locate the DPD fields, and complete the settings as described the following table:

Table 63. Dead Peer Detection settings

Setting	Description	
IKE SA Parameters		
Enable Dead Peer Detection	Select the **Yes** radio button to enable DPD. When the wireless 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 wireless 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 wireless VPN firewall tears down the connection and then attempts to reconnect to the peer. The default setting is three 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 wireless 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 142* on page 232).
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.)

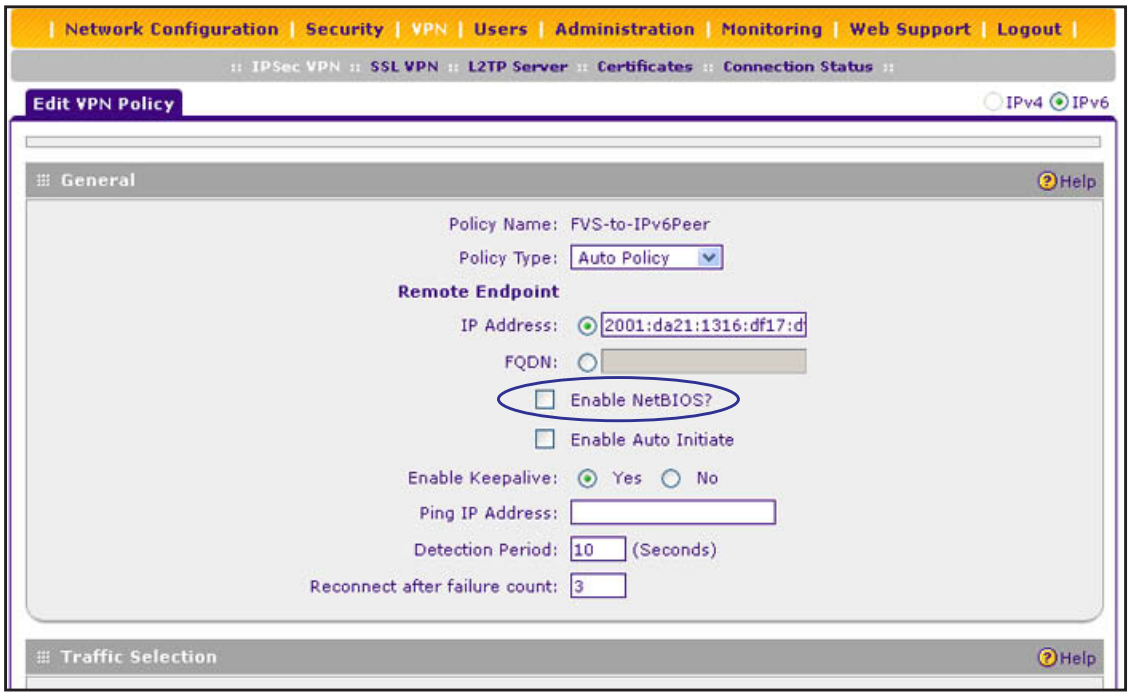

Figure 160.

4. Select the **Enable NetBIOS?** check box.
5. Click **Apply** to save your settings.

Configure the L2TP Server

As an alternate solution to IPSec VPN tunnels, you can configure a Layer 2 Tunneling Protocol (L2TP) server on the wireless 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 wireless 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 wireless 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 wireless 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 306.

➢ **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.)

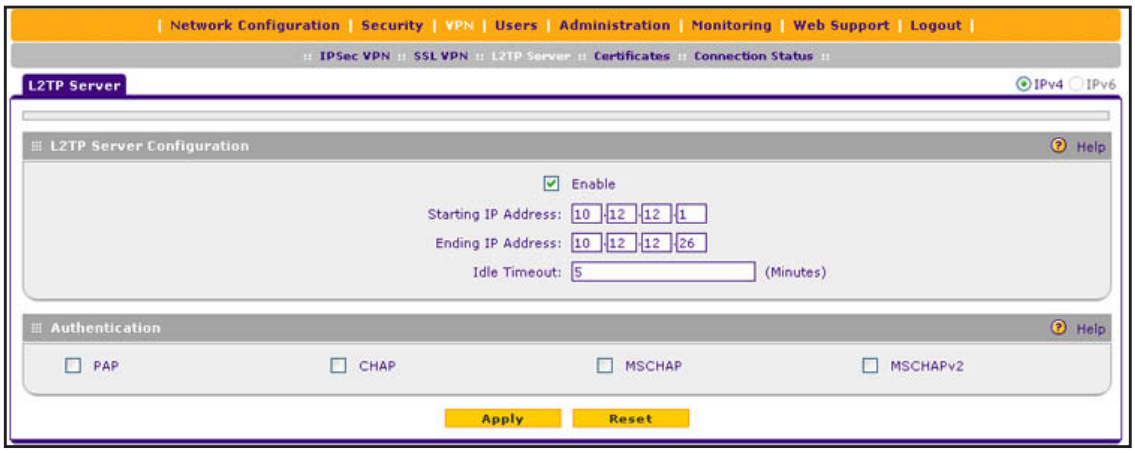

Figure 161.

2. To enable the L2TP server, select the **Enable** check box.
3. Enter the settings as described in the following table:

Table 64. L2TP Server screen settings

Setting	Description
L2TP Server Configuration	
Starting IP Address	The first IP address of the pool. This address is used for distribution to the wireless 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 10 minutes.

Table 64. L2TP Server screen settings (continued)

Setting	Description
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).	

4. 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:

Figure 162.

The List of L2TP Active Users table lists each active connection with the information that is described in the following table.

Table 65. L2TP Active Users screen information

Item	Description
Username	The name of the L2TP user that you have defined (see *Configure User Accounts* on page 306).
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 wireless VPN firewall.
Action	Click the **Disconnect** table button to terminate the L2TP connection.

7. Virtual Private Networking Using SSL Connections

The wireless 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 wireless 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 wireless 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 wireless VPN firewall's SSL VPN portal can provide two levels of SSL service to the remote user:

- **SSL VPN tunnel**. The wireless 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 wireless 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 wireless VPN firewall, and a virtual network interface is created on the user's computer. The wireless 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 269).

   When remote users log in to the wireless 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 274).)

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

      When remote users log in to the wireless 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 274).

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 wireless 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 277).

For the SSL VPN tunnel option, the wireless 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 281).

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 284).

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 298). 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 wireless 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 wireless 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*.

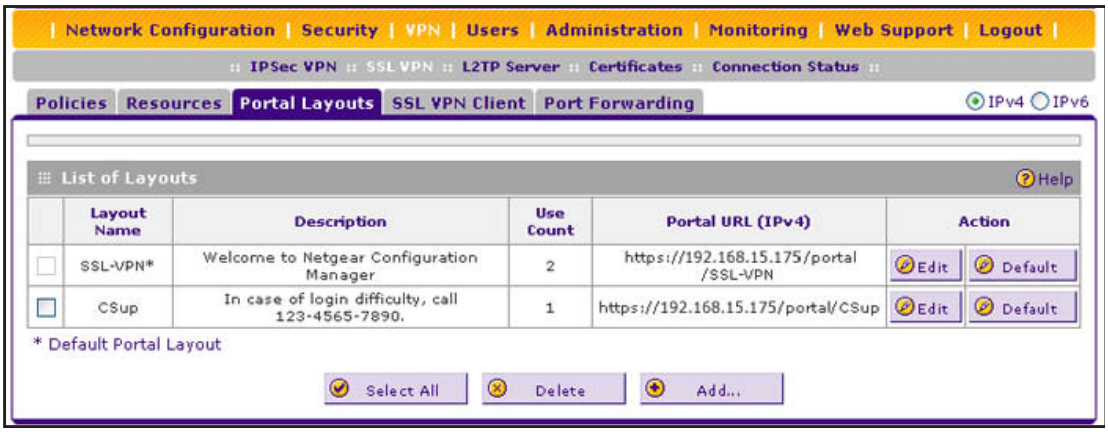

Figure 163. Portal Layouts screen for IPv4

- **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.)

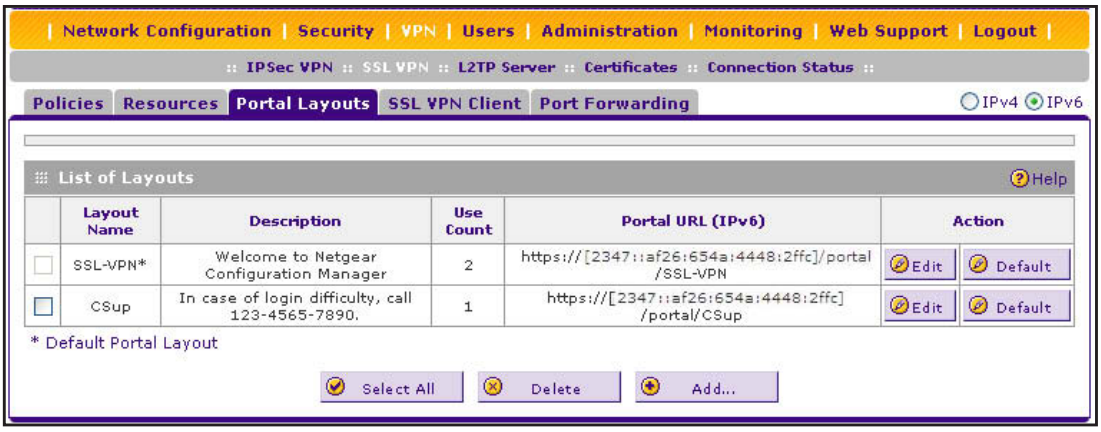

Figure 164. Portal Layouts screen for IPv6

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 176* on page 292).
- **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 wireless VPN firewall (see *Configure the IPv4 Internet Connection and WAN Settings* on page 27). 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 wireless VPN firewall (see *Configure the IPv6 Internet Connection and WAN Settings* on page 38). 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.)

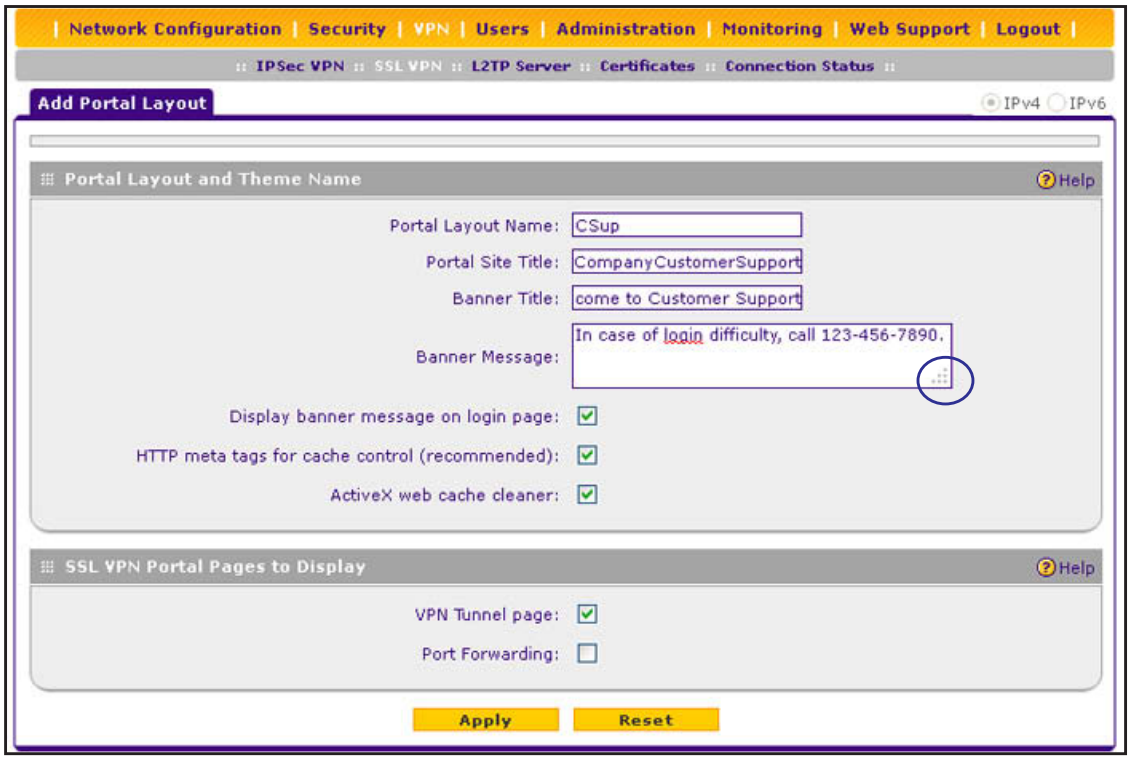

Figure 165.

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

Table 66. 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*.

Table 66. Add Portal Layout screen settings (continued)

Setting	Description
Banner Title	The banner title of a banner message that users see before they log in to the portal, for example, *Welcome to Customer Support*. **Note:** For an example, see *Figure 176* on page 292. 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 176* on page 292. 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 176* on page 292.
HTTP meta tags for cache control (recommended)	Select this check box to apply cache control directives for the HTTP meta tags to this portal layout. Cache control directives include: <meta http-equiv=”pragma” content=”no-cache”> <meta http-equiv=”cache-control” content=”no-cache”> <meta http-equiv=”cache-control” content=”must-revalidate”> **Note:** NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user’s web browser cache.
ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to delete all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. The ActiveX web cache control is ignored by web browsers that do not support ActiveX.
SSL VPN Portal Pages to Display	
VPN Tunnel page	To provide full network connectivity, select this check box.
Port Forwarding	To 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 290.

➢ **To edit a portal layout:**

1. On the Portal Layouts screen (for IPv4, see *Figure 163* on page 270; for IPv6, see *Figure 164* on page 271), 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 163* on page 270; for IPv6, see *Figure 164* on page 271), 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 wireless 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 298.

Configure Applications for Port Forwarding

- *Add Servers and Port Numbers*
- *Add a New Host Name*

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 wireless VPN firewall.

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.)

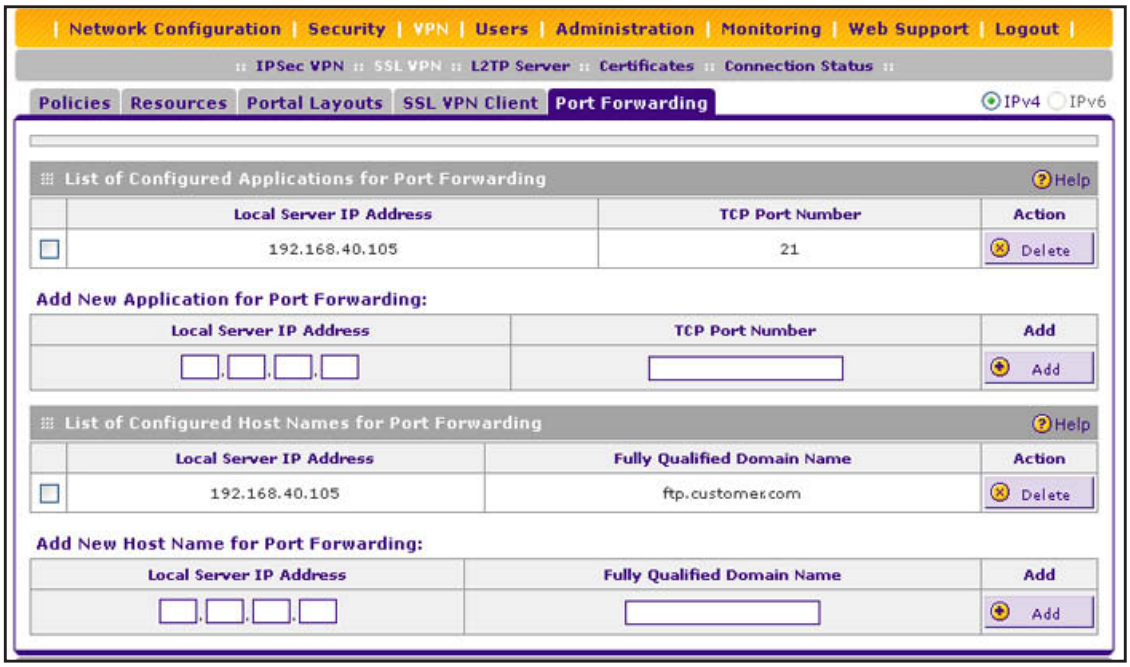

Figure 166.

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 67. 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

Table 67. Port forwarding applications/TCP port numbers (continued)

TCP Application	Port Number
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 166* on page 275).
2. In the Add New Host Name for Port Forwarding section of the screen, specify information in the following fields:
   - **Local Server IP Address**. The IP address of an internal server or host computer that you want to name.
   - **Fully Qualified Domain Name**. The full server name.

Note: If the server or host computer that you want to name does not display in the List of Configured Applications for Port Forwarding table, you need to add it before you can rename it.

3. Click the **Add** table button. The new application entry is added to the List of Configured Host Names for Port Forwarding table.

➢ **To delete a name from the List of Configured Host Names for Port Forwarding table:**

1. Select the check box to the left of the name that you want to delete.
2. Click the **Delete** table button in the Action column.

Configure the SSL VPN Client

The SSL VPN client on the wireless 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 wireless 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*.

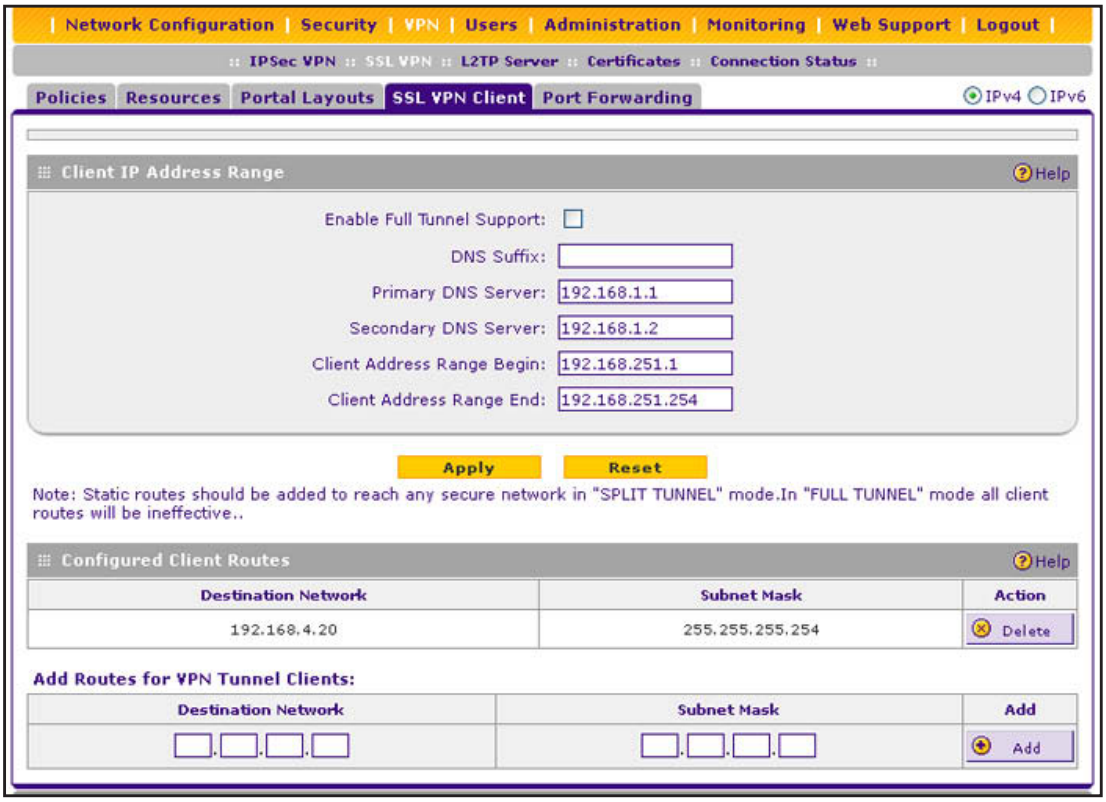

Figure 167. SSL VPN Client screen for IPv4

- **IPv6**. Select the **IPv6** radio button. The SSL VPN Client screen displays the IPv6 settings (the following screen shows some examples).

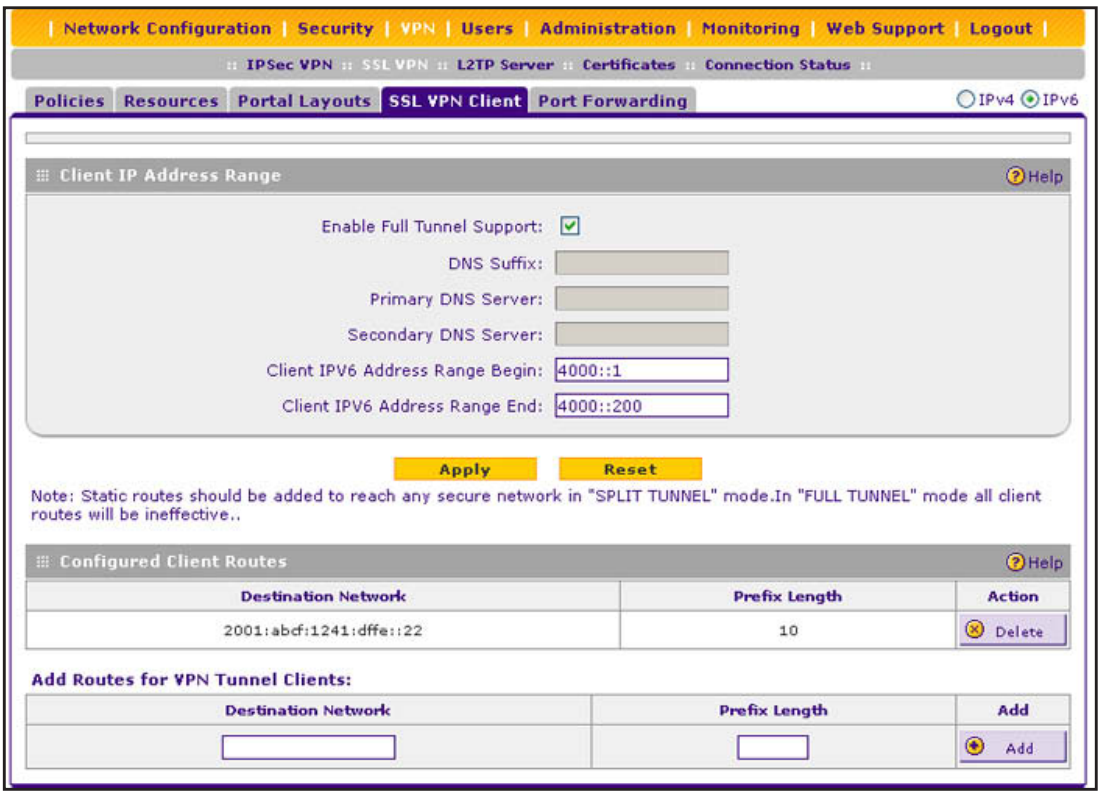

Figure 168. SSL VPN Client screen for IPv6

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

Table 68. 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 280). **Note:** When full-tunnel support is enabled, client routes are not operable.
DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the SSL VPN client after a VPN tunnel has been established.

Table 68. SSL VPN Client screen settings for IPv4 and IPv6 (continued)

Setting	Description	
Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.	
IPv4 screen only	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.
	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 wireless 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 167* on page 278).
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 168* on page 279).

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 192.168.4.20.
   - **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 294). 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

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 282) 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.)

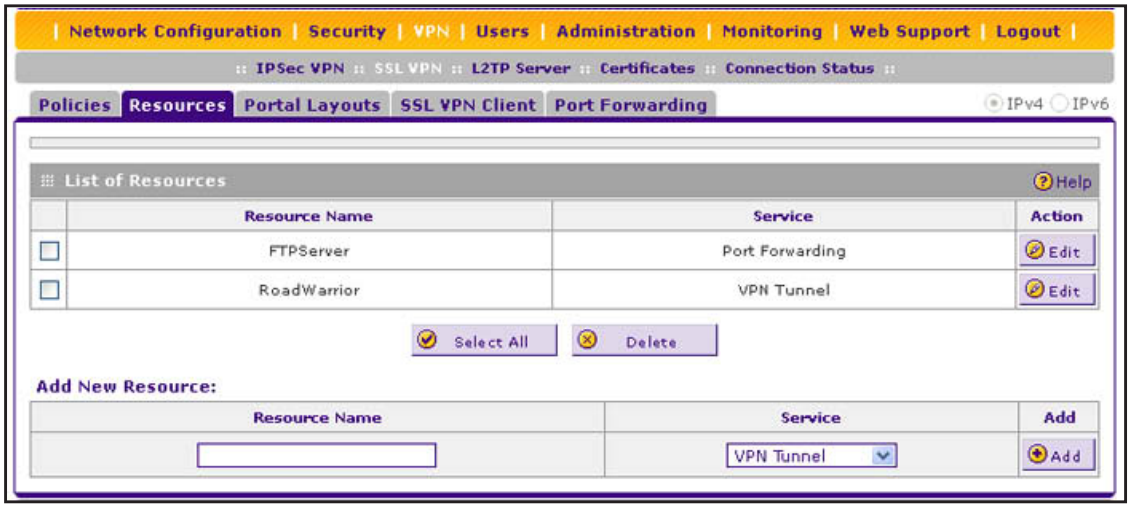

Figure 169.

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. This screen is identical to the screen for IPv4 (see the next figure, which shows some examples).

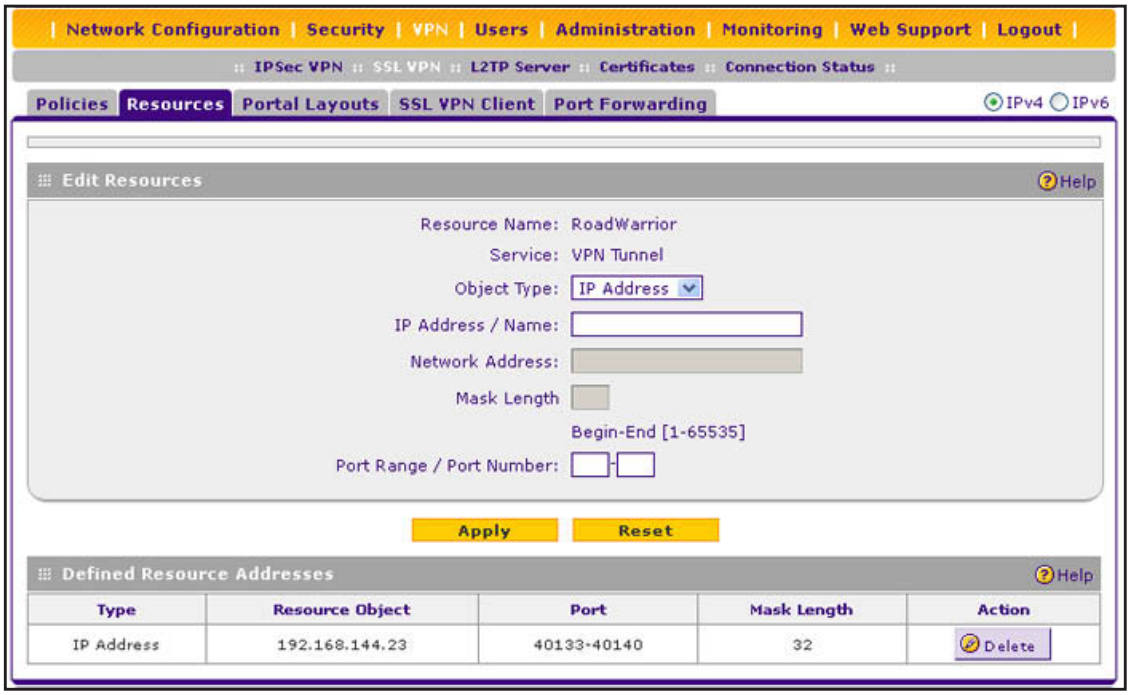

Figure 170.

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

Table 69. 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.

Table 69. Resources screen settings to edit a resource (continued)

Setting	Description	
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):
	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 wireless 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 wireless 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.)

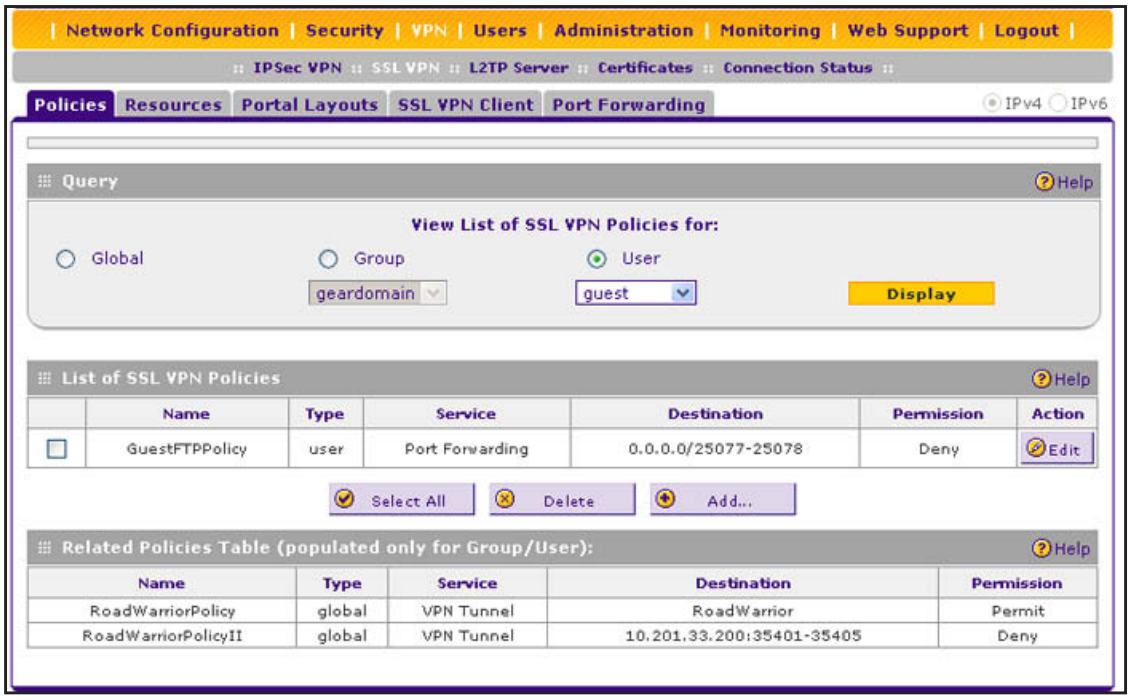

Figure 171.

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*.

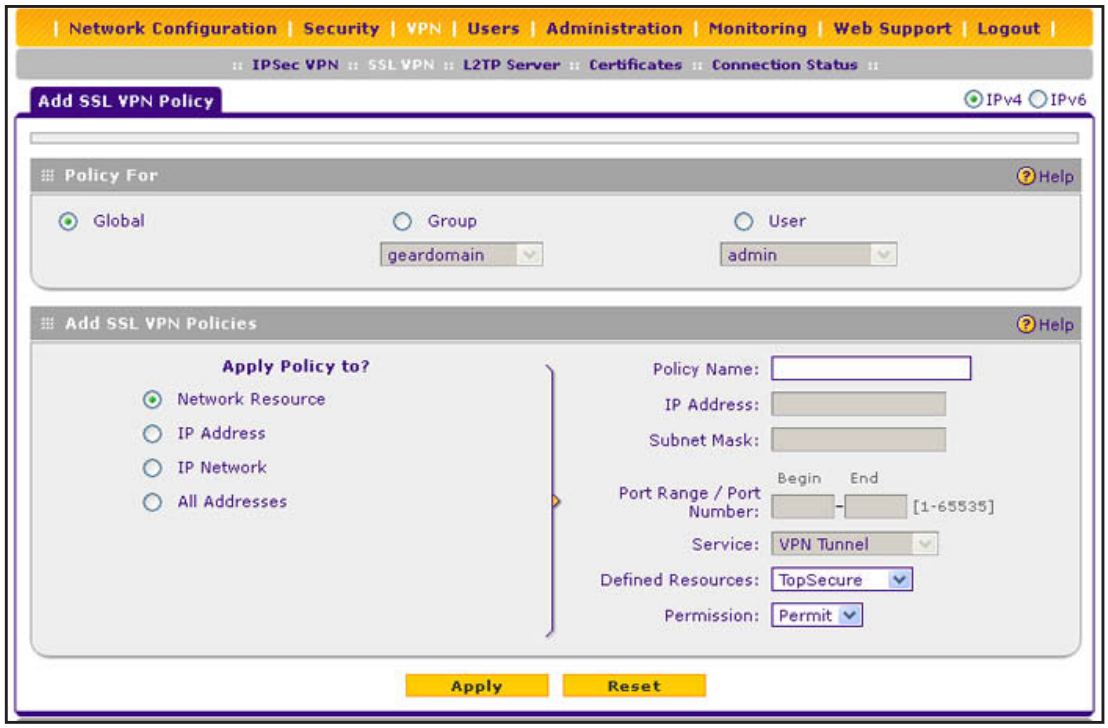

Figure 172. Add SSL VPN Policy screen for IPv4

- **IPv6**. Select the **IPv6** radio button. The Add SSL VPN Policy screen displays the IPv6 settings:

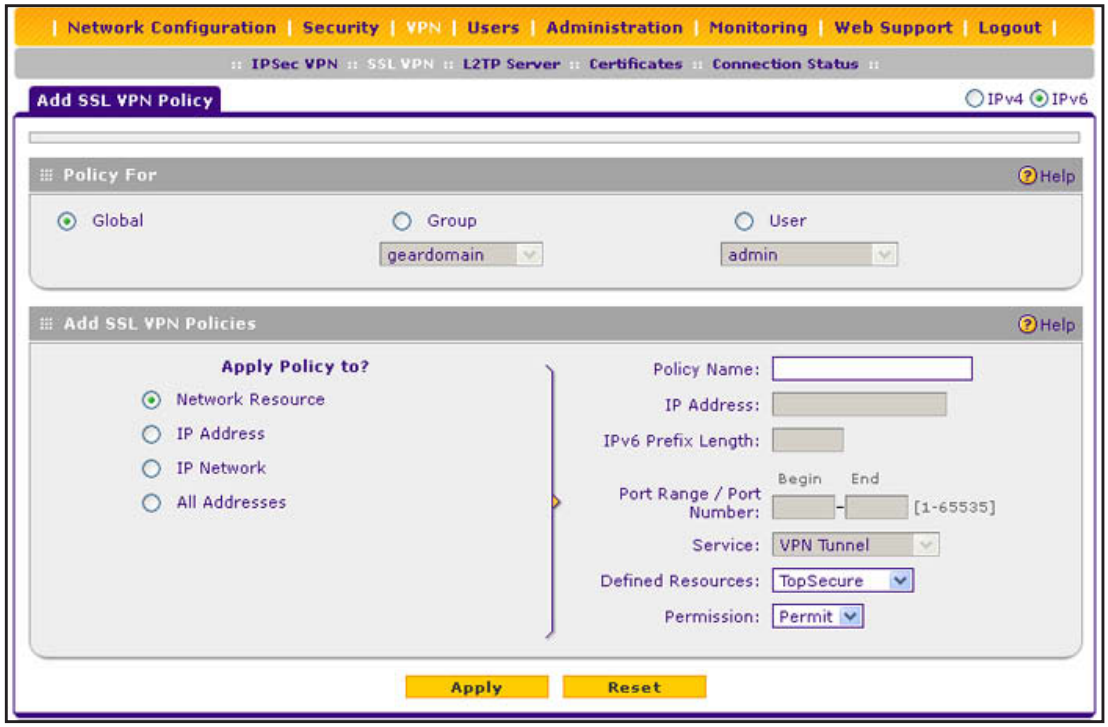

Figure 173. Add SSL VPN Policy screen for IPv6

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

Table 70. 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 303. • **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 306.			
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 281). • **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.		
	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 281).
		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.

Table 70. Add SSL VPN Policy screen settings (continued)

Setting	Description			
Apply Policy to? (continued)	IP Address (continued)	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.	
		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 333). 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 171* on page 286), 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 171* on page 286), 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 (

).

When you click the **User Portal** link, the SSL VPN default portal opens (see *Figure 177* on page 293). This user portal is not the same as the new SSL portal login screen that you defined in *Create the Portal Layout* on page 269.

- **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*.

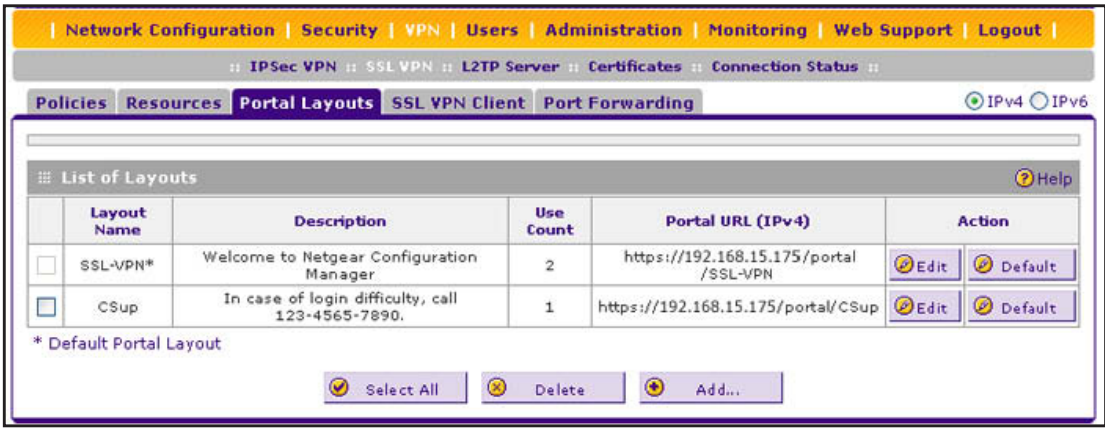

Figure 174. Portal Layouts screen for IPv4

- **IPv6**. Select the **IPv6** radio button. The Portal Layouts screen displays the IPv6 settings.

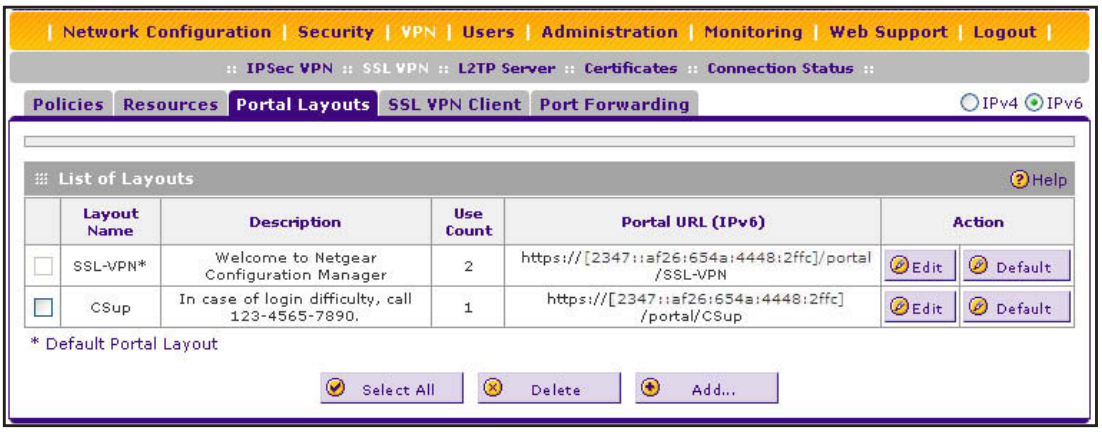

Figure 175. Portal Layouts screen for IPv6

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 CSup layout that was defined in *Create the Portal Layout* on page 269.)

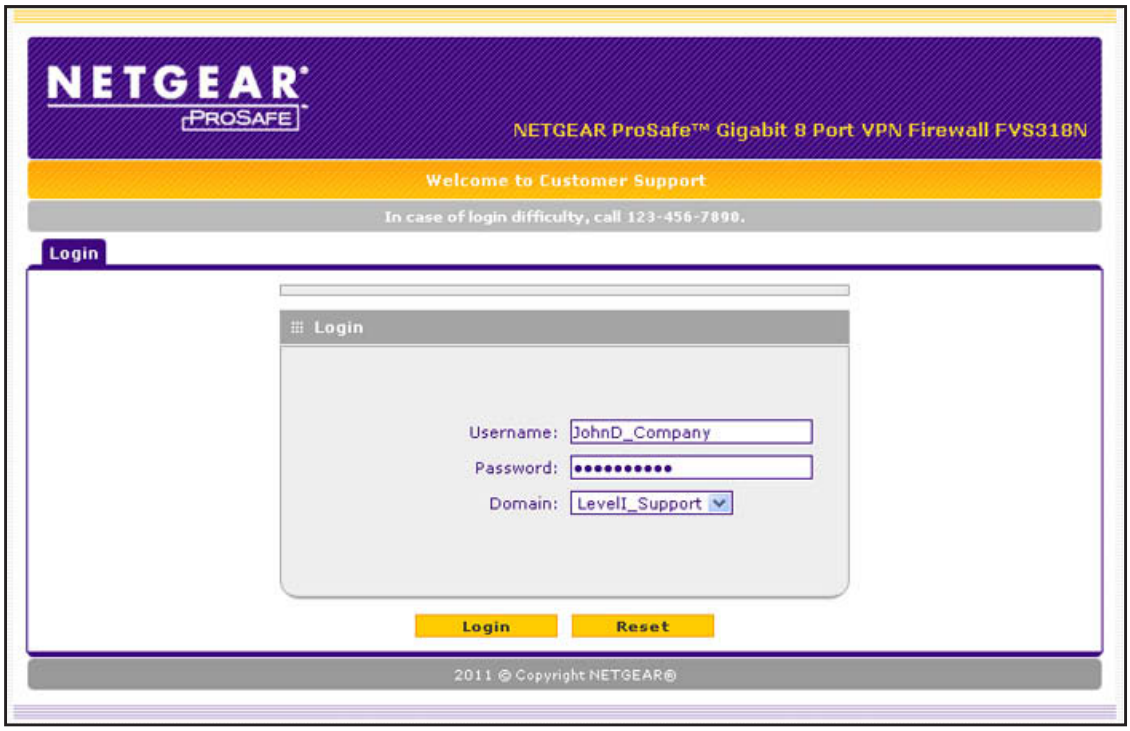

Figure 176.

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 274.
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 269):
   - *Figure 177* on page 293 shows the User Portal screen with the VPN Tunnel icon and both a VPN Tunnel and a Port Forwarding menu option.
   - *Figure 178* on page 293 show the User Portal screen with the Port Forwarding icon and a Port Forwarding menu option only. The VPN Tunnel menu option is not displayed.

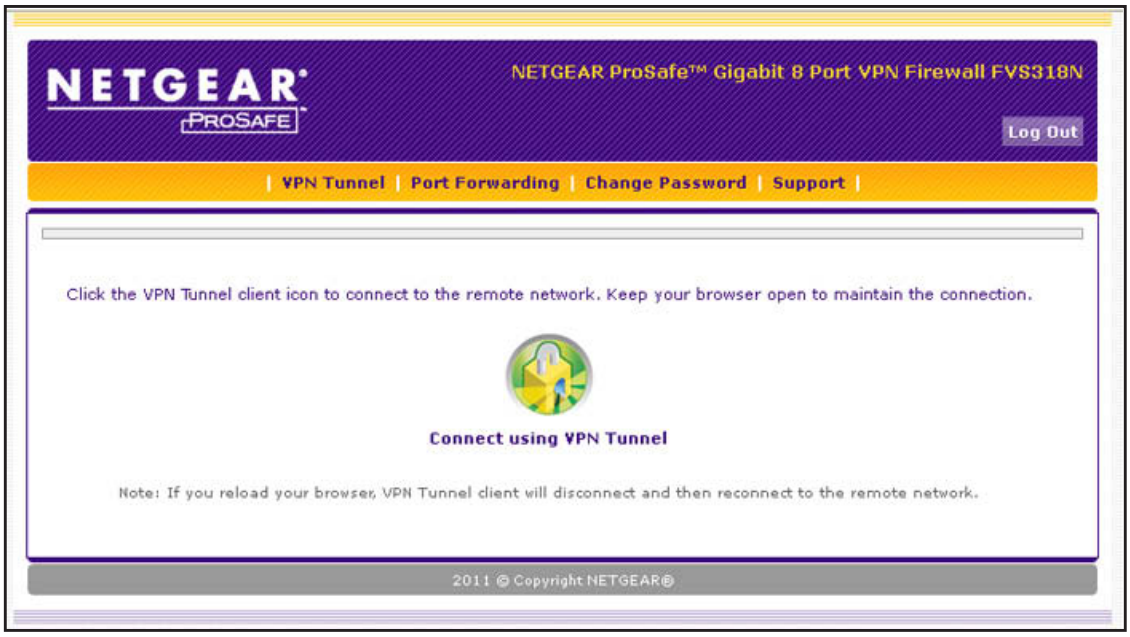

Figure 177.

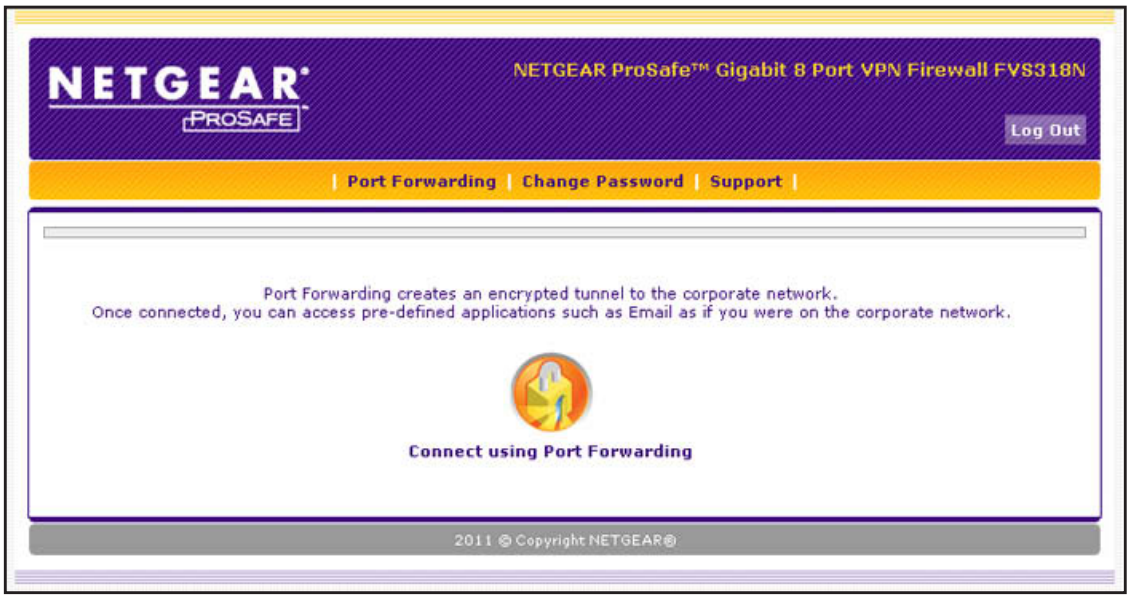

Figure 178.

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 274.

- **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 179.

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:

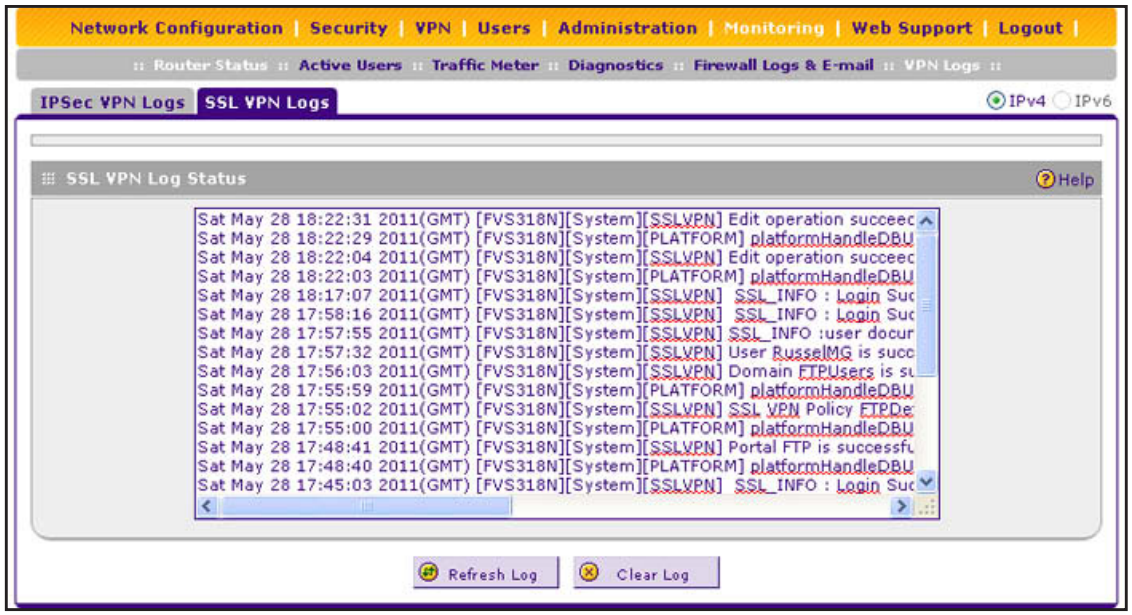
Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
IPv4
IPv6
SSL VPN Log Status
Help
Sat May 28 18:22:31 2011(GMT) [FVS318N][System][SSLVPN] Edit operation succeec
Sat May 28 18:22:29 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 18:22:04 2011(GMT) [FVS318N][System][SSLVPN] Edit operation succeec
Sat May 28 18:22:03 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 18:17:07 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Sat May 28 17:58:16 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Sat May 28 17:57:55 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO :user docur
Sat May 28 17:57:32 2011(GMT) [FVS318N][System][SSLVPN] User RusselMG is succ
Sat May 28 17:56:03 2011(GMT) [FVS318N][System][SSLVPN] Domain FTPUsers is su
Sat May 28 17:55:59 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:55:02 2011(GMT) [FVS318N][System][SSLVPN] SSL VPN Policy FTPDe
Sat May 28 17:55:00 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:48:41 2011(GMT) [FVS318N][System][SSLVPN] Portal FTP is successfu
Sat May 28 17:48:40 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:45:03 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Refresh Log
Clear Log

Figure 180.

Manage Users, Authentication, and VPN Certificates

8

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

- *The Wireless VPN Firewall's Authentication Process and Options*
- *Configure Authentication Domains, Groups, and Users*
- *Manage Digital Certificates for VPN Connections*

The Wireless 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 68.

You need to create name and password accounts for all users who need to be able to connect to the wireless 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 wireless VPN firewall need to be authenticated before being allowed to access the wireless 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 and L2TP 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 wireless VPN firewall supports.

Table 71. 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 71. 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 B, 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 wireless 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 wireless VPN firewall's default domain—geardomain—and, as an example, other domains in the List of Domains table.)

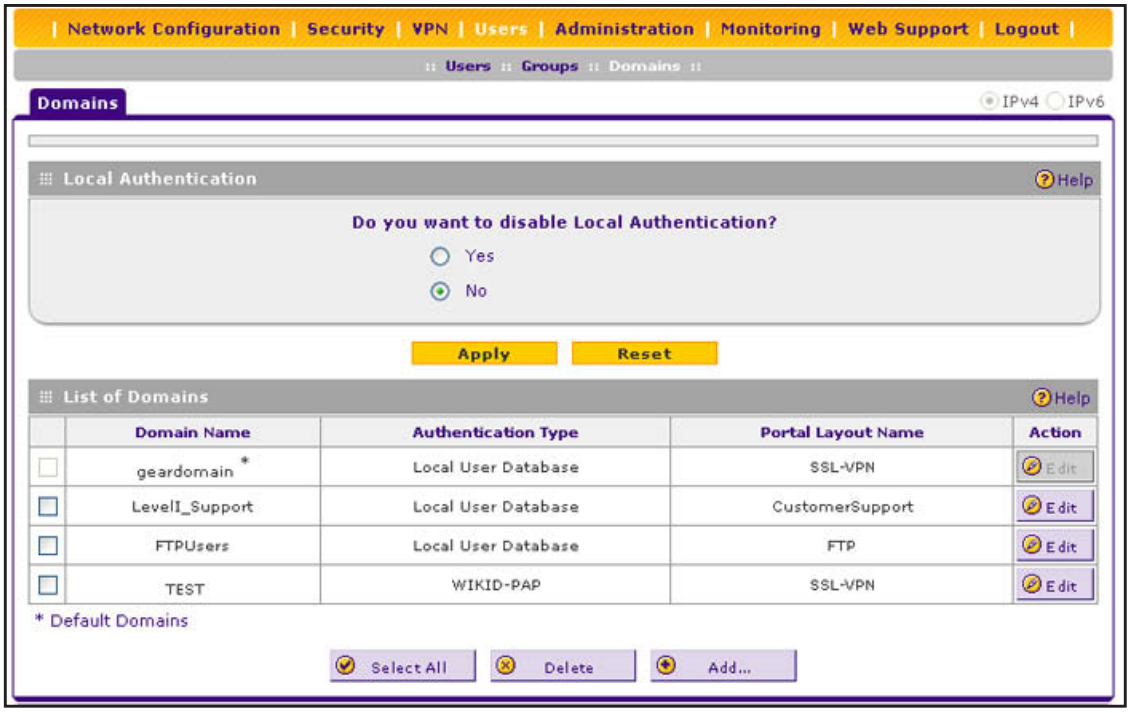

Figure 181.

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:

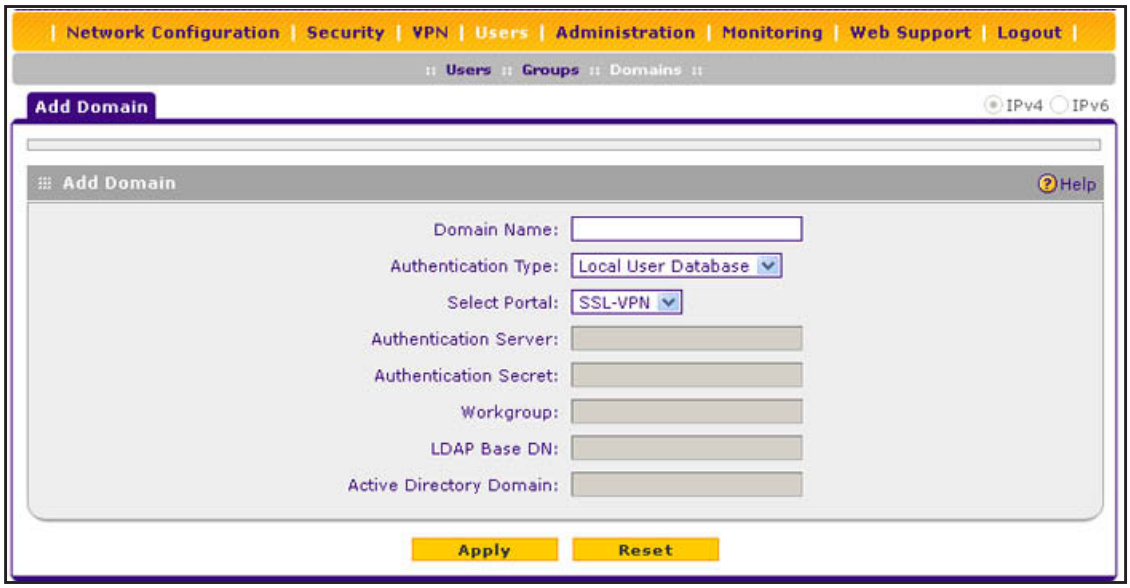

Figure 182.

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

Table 72. Add Domain screen settings

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the drop-down list, select the authentication method that the wireless VPN firewall applies: • **Local User Database (default)**. Users are authenticated locally on the wireless 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

Table 72. 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 241).	• **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 • **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 wireless 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 181* on page 299), 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 wireless 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 181* on page 299).
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 wireless 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 and L2TP 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 68.

Create Groups

➢ **To create a VPN group:**

1. Select **Users > Groups**. The Groups screen displays. (The following figure shows the wireless VPN firewall's default group—geardomain—and, as an example, several other groups in the List of Groups table.)

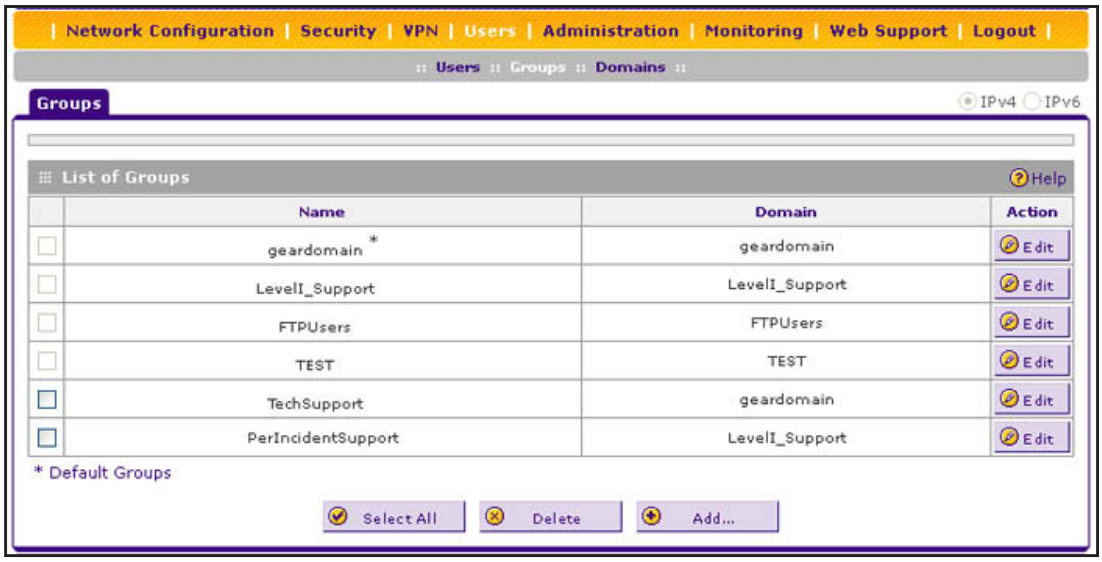

Figure 183.

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:

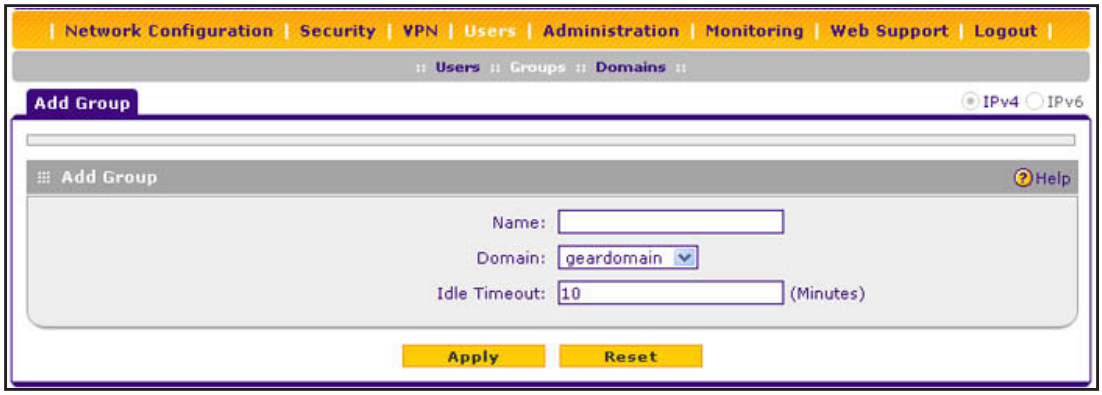

Figure 184.

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

Table 73. 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 298.
Idle Timeout	The period after which an idle user is automatically logged out of the wireless 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 183* on page 304).
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 and L2TP 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 wireless VPN firewall configuration (that is, read-write access).
- **Guest user**. A user who can only view the wireless 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 239).
- **L2TP user**. A user who can connect over an L2TP connection to an L2TP client that is located behind the wireless VPN firewall.

➢ **To create a user account:**

1. Select **Users > Users**. The Users screen displays. (The following figure shows the wireless VPN firewall's default users—admin and guest—and, as an example, several other users in the List of Users table.)

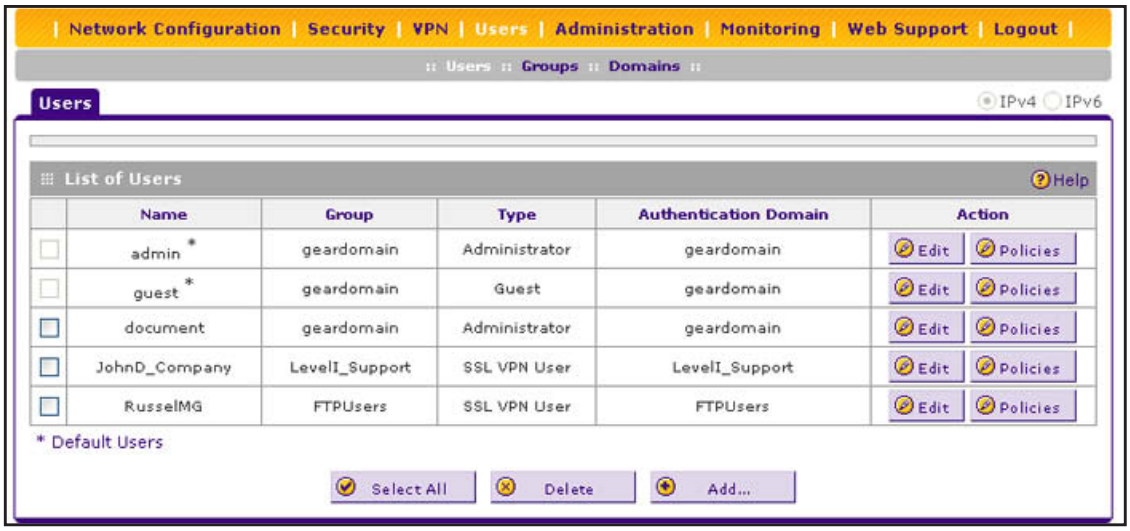

Figure 185.

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 wireless 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:

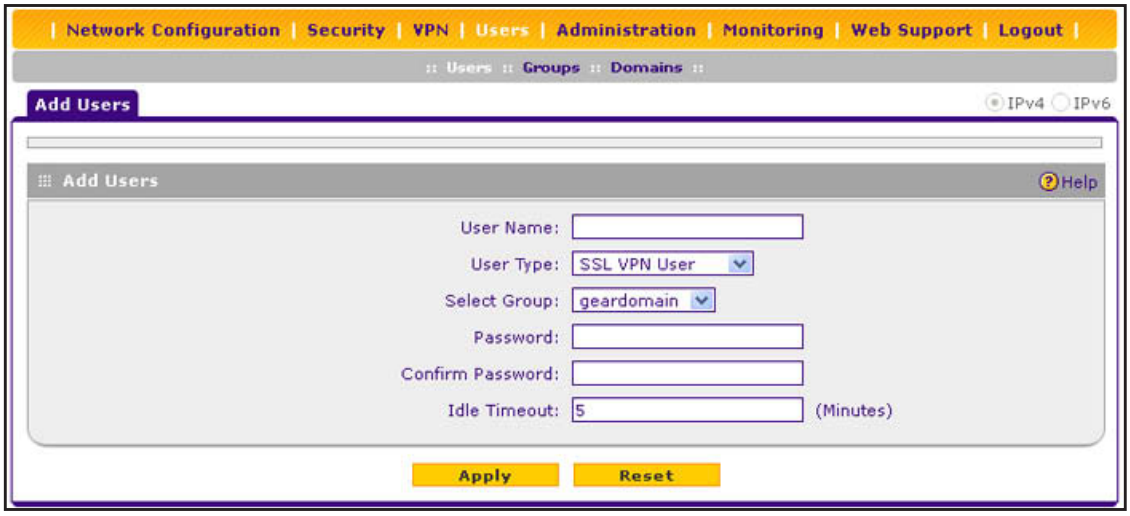

Figure 186.

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

Table 74. 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: • **Administrator**. A user who has full access and the capacity to change the wireless VPN firewall configuration (that is, read/write access). • **SSL VPN User**. A user who can log in only to the SSL VPN portal. • **Guest User**. A user who can only view the wireless 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 239). • **L2TP User**. A user who can connect over an L2TP connection to an L2TP client that is located behind the wireless 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 303. **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 wireless 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 five 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 wireless 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 185* on page 307).
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:

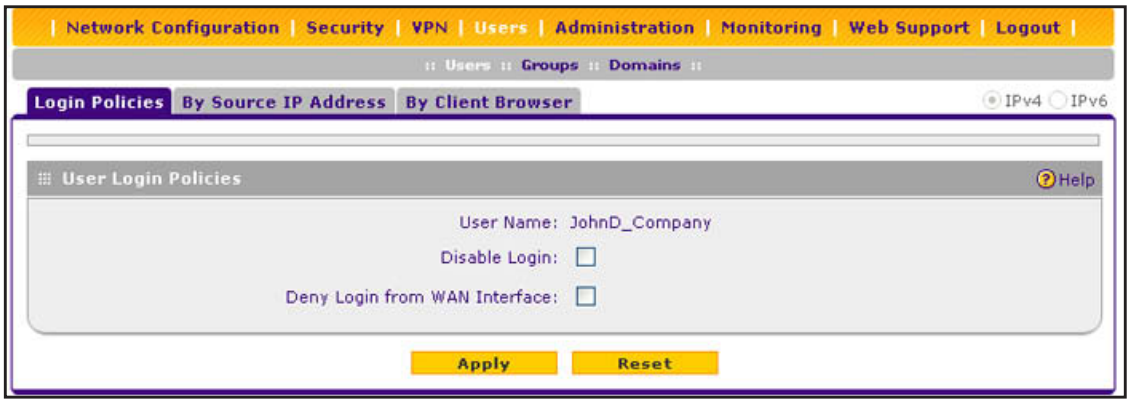

Figure 187.

3. Make the following optional selections:
   - To prohibit the user from logging in to the wireless 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 185* on page 307).
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.)

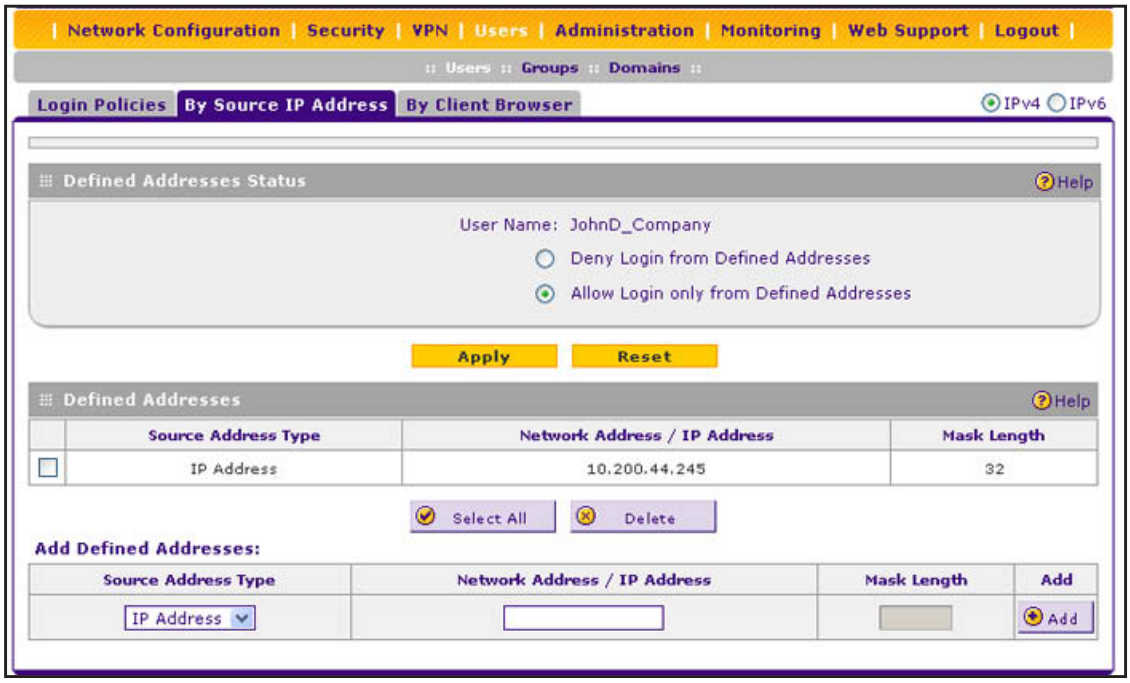

Figure 188.

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 75. 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 185* on page 307).
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.)

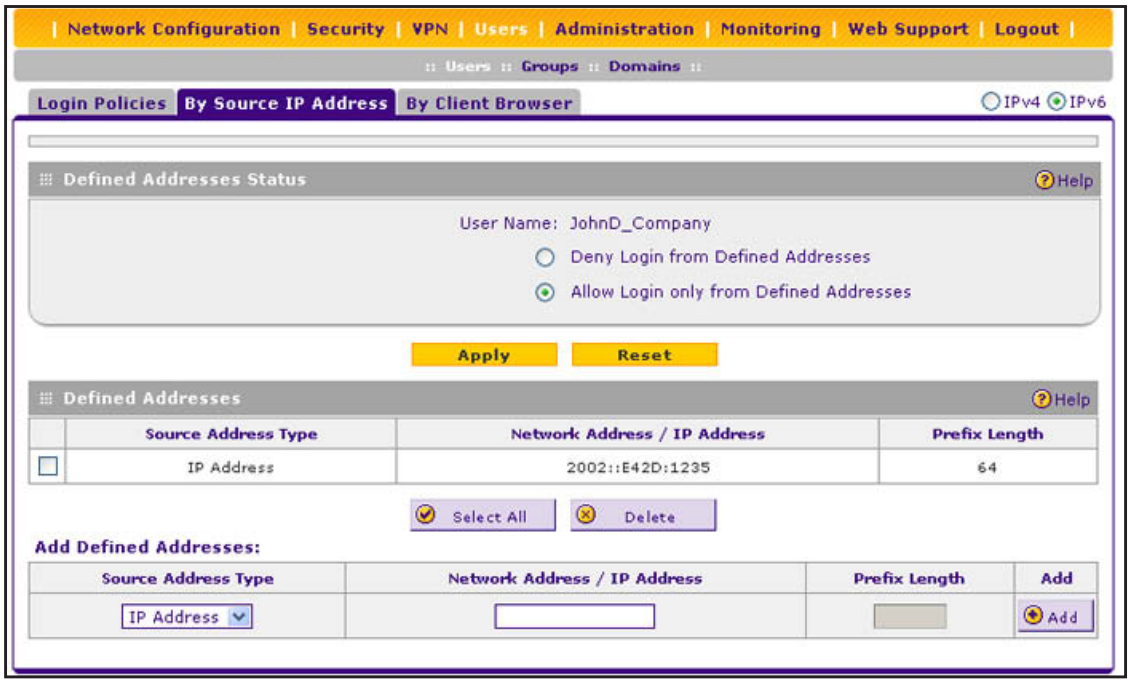

Figure 189.

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 76. 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 185* on page 307).
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.)

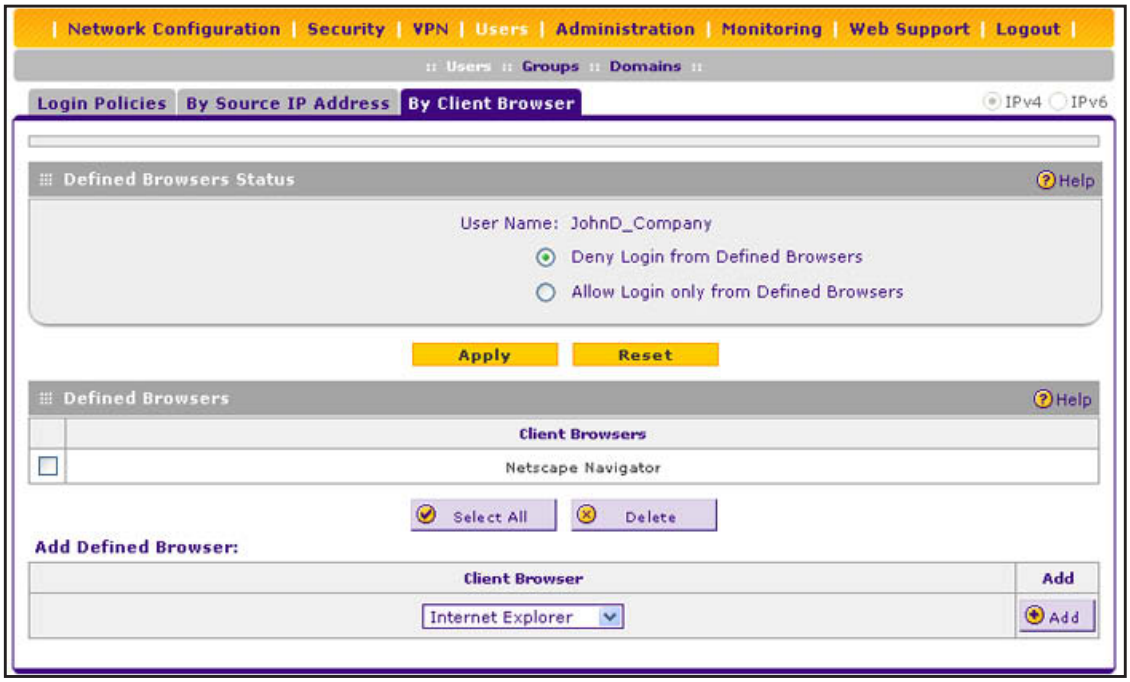

Figure 190.

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 five minutes, respectively.

➢ **To modify user settings, including passwords:**

1. Select **Users > Users**. The Users screen displays (see *Figure 185* on page 307).
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:

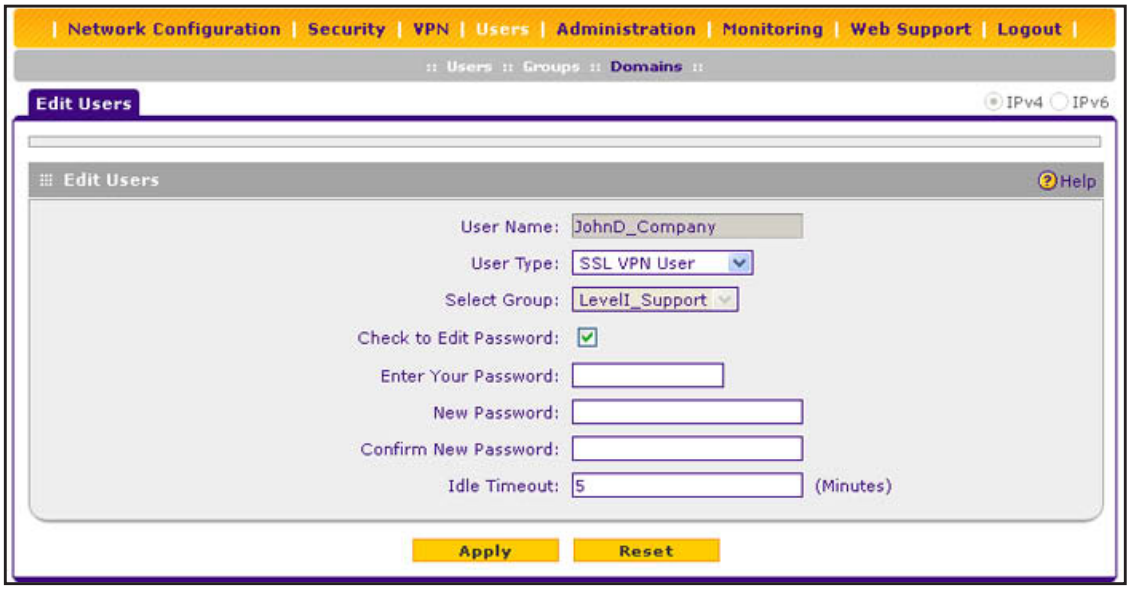

Figure 191.

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 77. 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 wireless VPN firewall configuration (that is, read/write access). • **Guest (readonly)**. User who can only view the wireless 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.

Table 77. Edit User screen settings (continued)

Setting	Description	
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 five minutes.	

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

Manage Digital Certificates for VPN Connections

- *VPN Certificates Screen*
- *Manage VPN CA Certificates*
- *Manage VPN Self-Signed Certificates*
- *Manage the VPN Certificate Revocation List*

The wireless 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 wireless 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 141* on page 226 and *Authentication Method* on page 229).
- On the VPN Client, you can enter a digital certificate on the Authentication pane in the Configuration Panel screen (see *Figure 128* on page 214).

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 wireless VPN firewall when the same digital certificate is being used for secure web management.

On the wireless 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 wireless 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 wireless VPN firewall contains a self-signed digital certificate from NETGEAR. This certificate can be downloaded from the wireless 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 wireless 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 192* on page 318, *Figure 194* on page 320, and *Figure 196* on page 323).

The Certificates screen lets you view the loaded digital certificates, upload a new digital certificate, and generate a certificate signing request (CSR). The wireless 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 319).

- **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 wireless VPN firewall (see *Manage VPN Self-Signed Certificates* on page 319).
- **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 323).

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.)

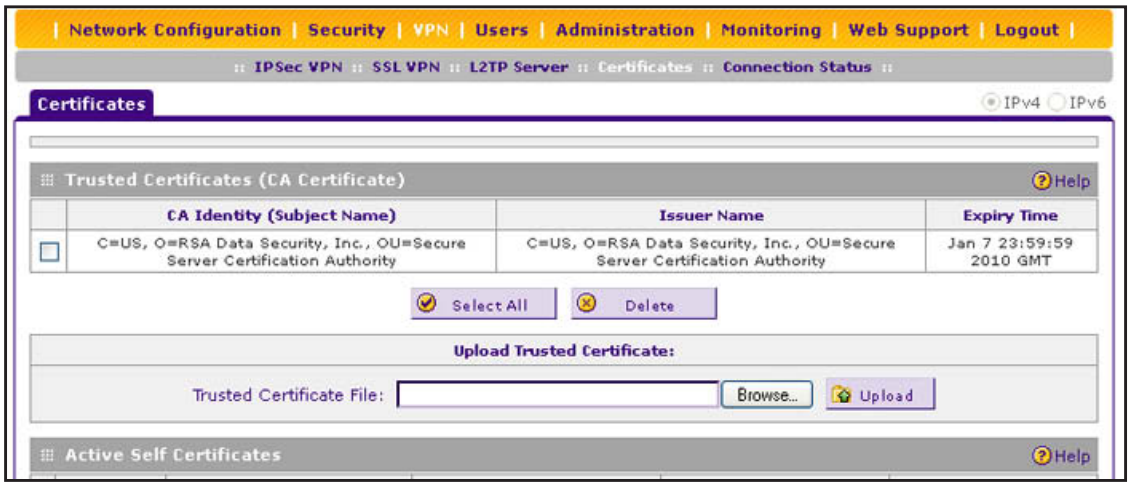

Figure 192. Certificates, screen 1 of 3

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 wireless 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 wireless 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 193.

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 download and activate the digital certificate on the wireless VPN firewall. To request a self-signed certificate from a CA, you need to generate a certificate signing request (CSR) for and on the wireless 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 wireless 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.)

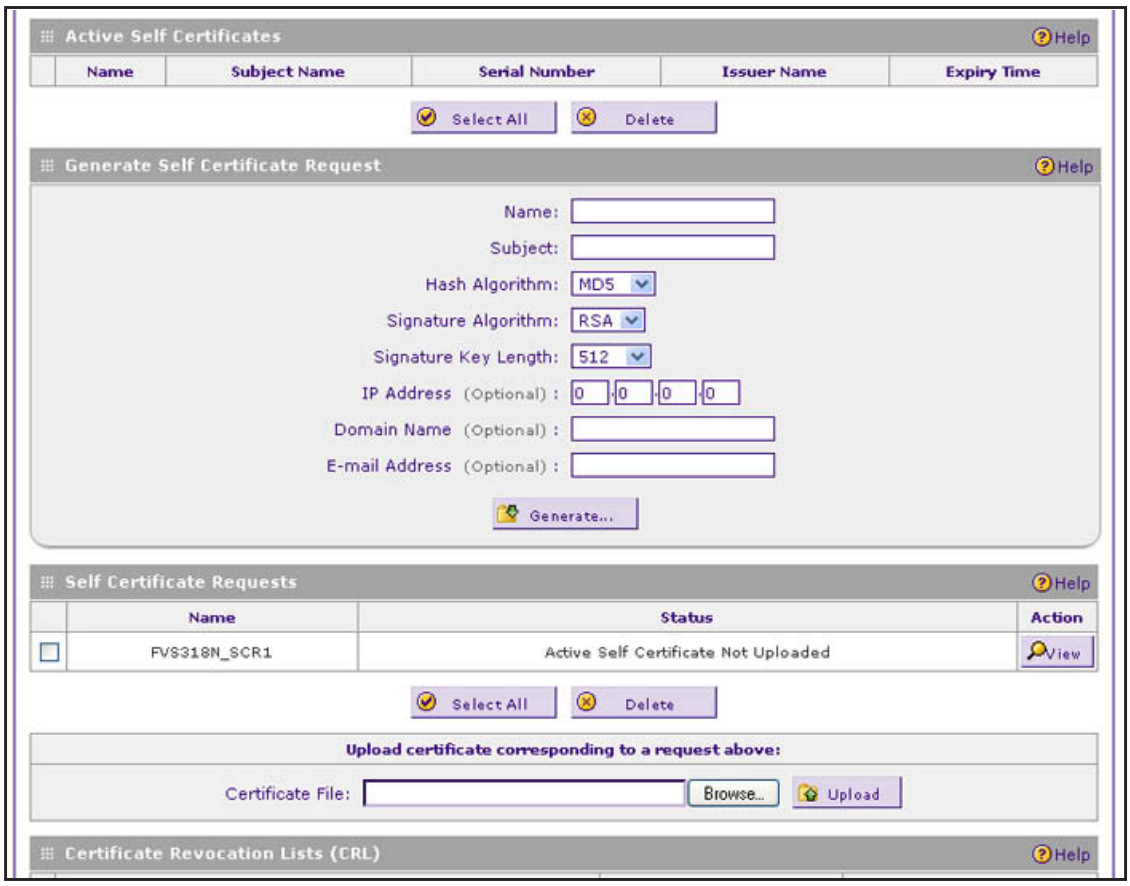

Figure 194. Certificates, screen 2 of 3

2. In the Generate Self Certificate Request section of the screen, enter the settings as described in the following table:

Table 78. 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.

Table 78. Generate self-signed certificate request settings (continued)

Setting	Description	
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.	
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:

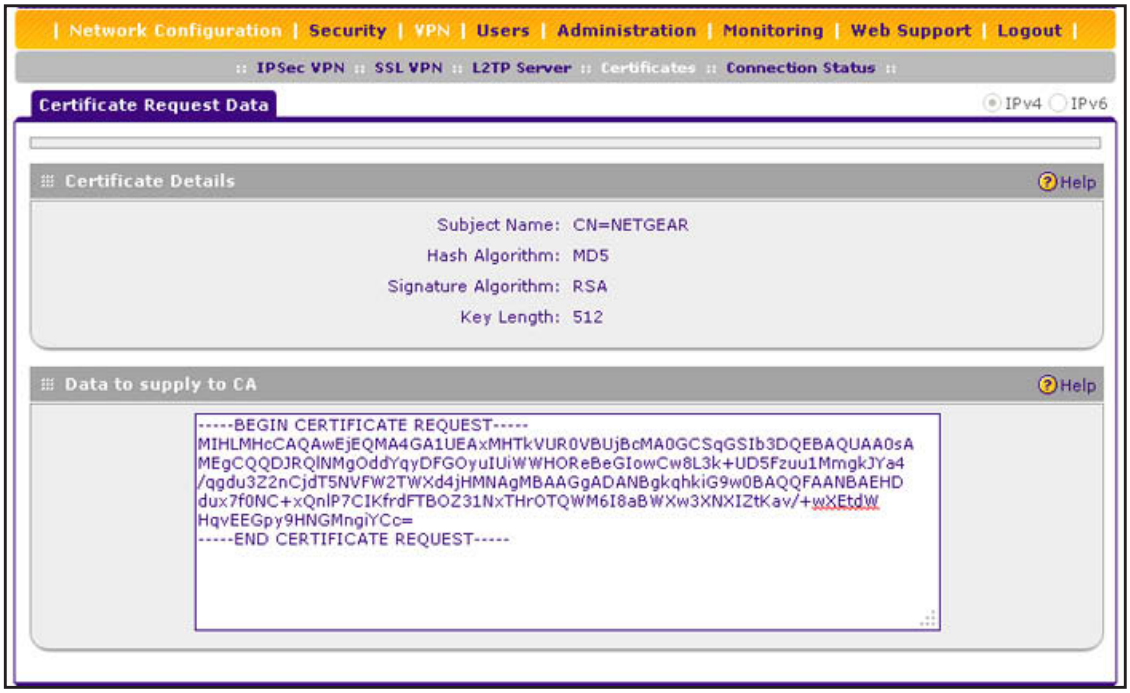

Figure 195.

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 194* on page 320) 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 wireless 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 194* on page 320) 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.)

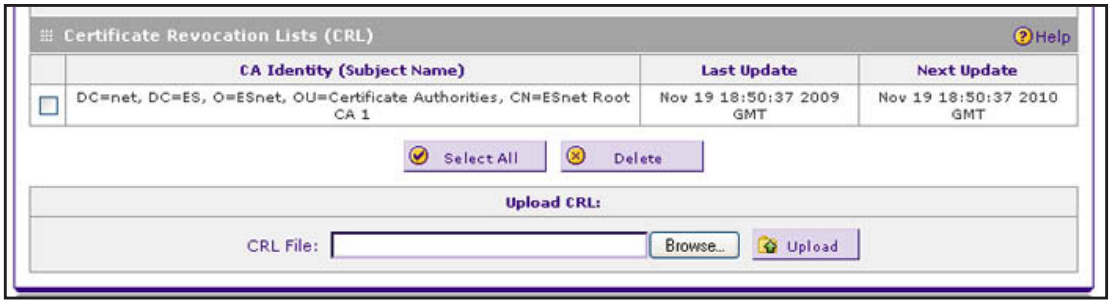

Figure 196. Certificates, screen 3 of 3

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 wireless 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.

9 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 wireless VPN firewall. The chapter contains the following sections:

- *Performance Management*
- *System Management*

Performance Management

Performance management consists of controlling the traffic through the wireless 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 wireless VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

The maximum bandwidth capacity of the wireless VPN firewall in each direction is as follows:

- LAN side. 8000 Mbps (eight LAN ports at 1000 Mbps each).
- WAN side. 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: The typical traffic rate is 1.5 Mbps. As a result, and depending on the traffic that is being carried, the WAN side of the wireless VPN firewall is the limiting factor for the data rate for most installations.

Features That Reduce Traffic

You can adjust the following features of the wireless 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 132. For detailed procedures about how to configure outbound rules, see *Configure LAN WAN Rules* on page 139 and *Configure DMZ WAN Rules* on page 146.

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 132 and *Add Customized Services* on page 173).
- **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.
  - **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 69. 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 68.
- **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.
- **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 183.

- **QoS profile**. You can apply QoS profiles to outbound rules to regulate the priority of traffic. For information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 178.
- **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 176.

Content Filtering

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the wireless 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 wireless 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 wireless 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 184 for the procedure about how to use this feature.

Features That Increase Traffic

The following features of the wireless 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 134. For detailed procedures about how to configure inbound rules, see *Configure LAN WAN Rules* on page 139 and *Configure DMZ WAN Rules* on page 146.

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 134 and *Add Customized Services* on page 173).
- **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.
  - **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 69. 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 68.

- **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.
- **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 183.
- **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 176.

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 about how to configure port triggering, see *Configure Port Triggering* on page 190.

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 eighth LAN port on the wireless 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 86. For the procedures about how to configure DMZ traffic rules, see *Configure DMZ WAN Rules* on page 146.

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 164.

VPN and L2TP Tunnels

The wireless VPN firewall supports site-to-site IPSec VPN tunnels, dedicated SSL VPN tunnels, and L2TP tunnels. Each tunnel requires extensive processing for encryption and authentication, thereby increasing traffic through the WAN ports.

For information about IPSec VPN and L2TP tunnels, see *Chapter 6, Virtual Private Networking Using IPSec and L2TP Connections*. For information about SSL VPN tunnels, see *Chapter 7, 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 wireless VPN firewall.

Set QoS Priorities

The QoS priority settings determine the Quality of Service for the traffic passing through the wireless VPN firewall. You can assign a QoS priority 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 *Preconfigured Quality of Service Profiles* on page 178.

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 176.

Monitoring Tools for Traffic Management

The wireless 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 10, 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*
- *Update 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 306 and *Set User Login Policies* on page 309.

➢ **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 wireless VPN firewall's default users—admin and guest—and, as an example, several other users in the List of Users table.)

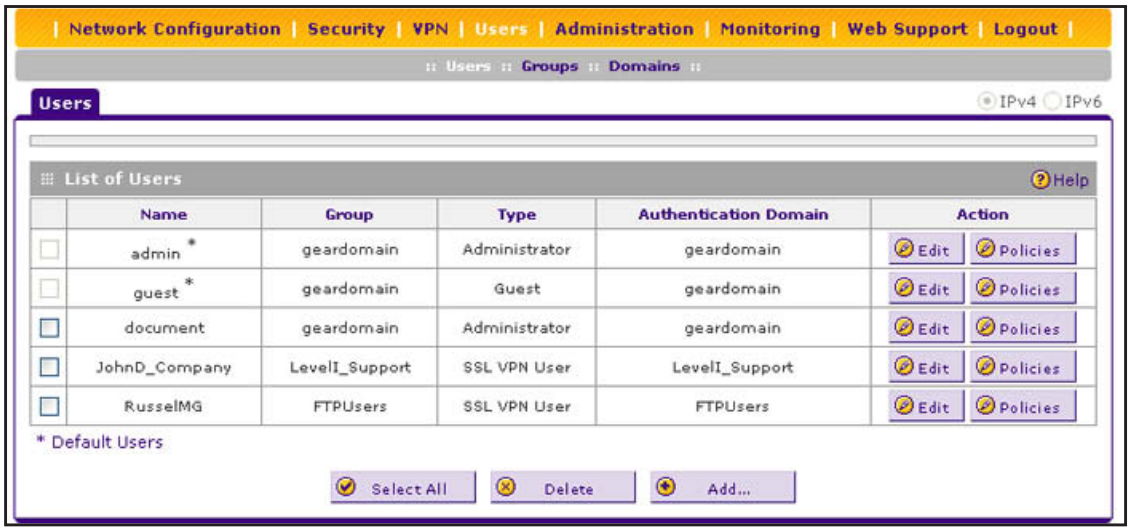

Figure 197.

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:

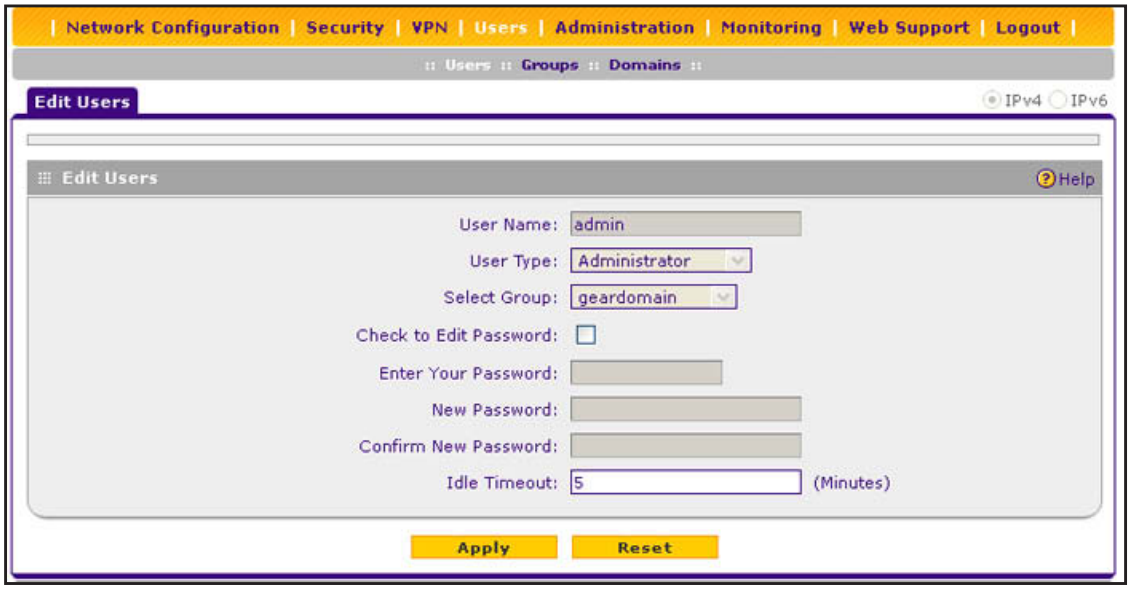

Figure 198.

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 five 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 five minutes, respectively.

You can also change the administrator login policies:

- Disable login. Deny login access.

> **Note:** If you are logged in as an administrator, you obviously do not want to deny login access to yourself.

- 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 309.

Configure Remote Management Access

An administrator can configure, upgrade, and check the status of the wireless 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 309), the wireless 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 wireless 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 331).

➢ **To configure the wireless 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*.

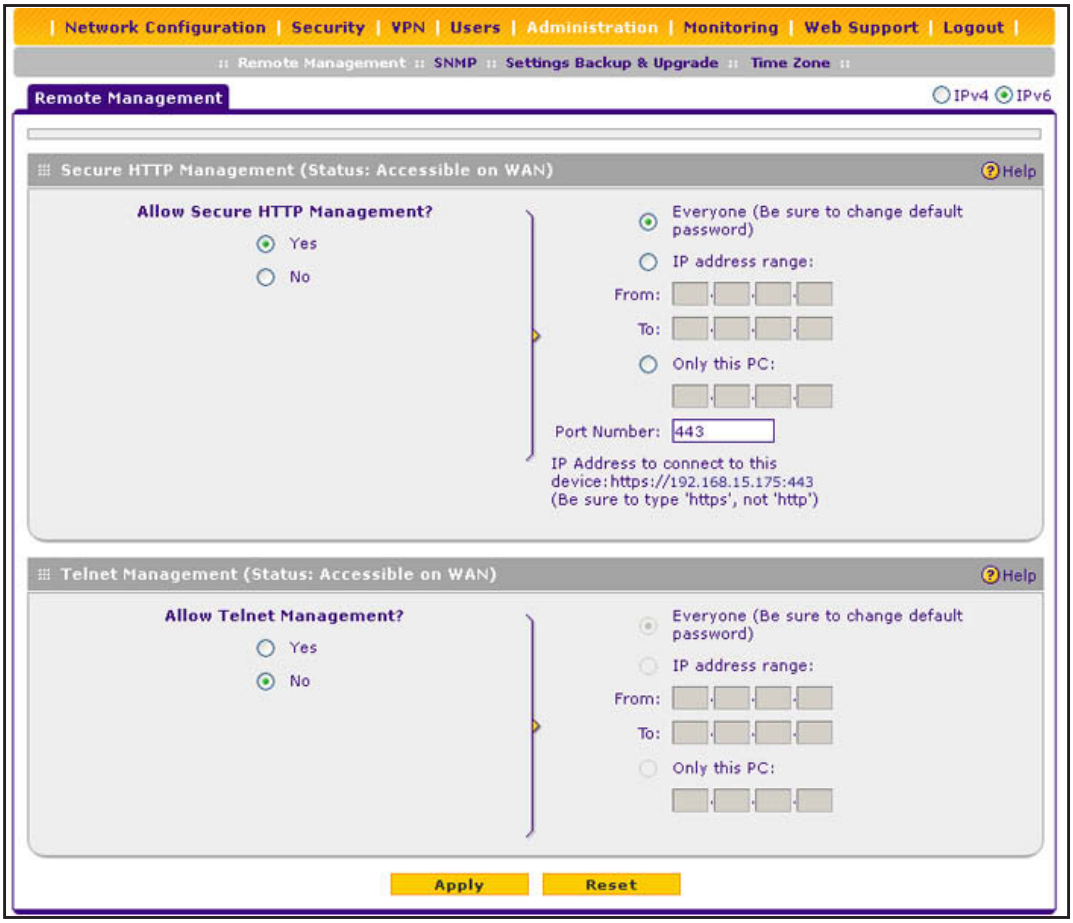

Figure 199. Remote Management screen for IPv4

- **IPv6**. Select the **IPv6** radio button. The Remote Management screen displays the IPv6 settings:

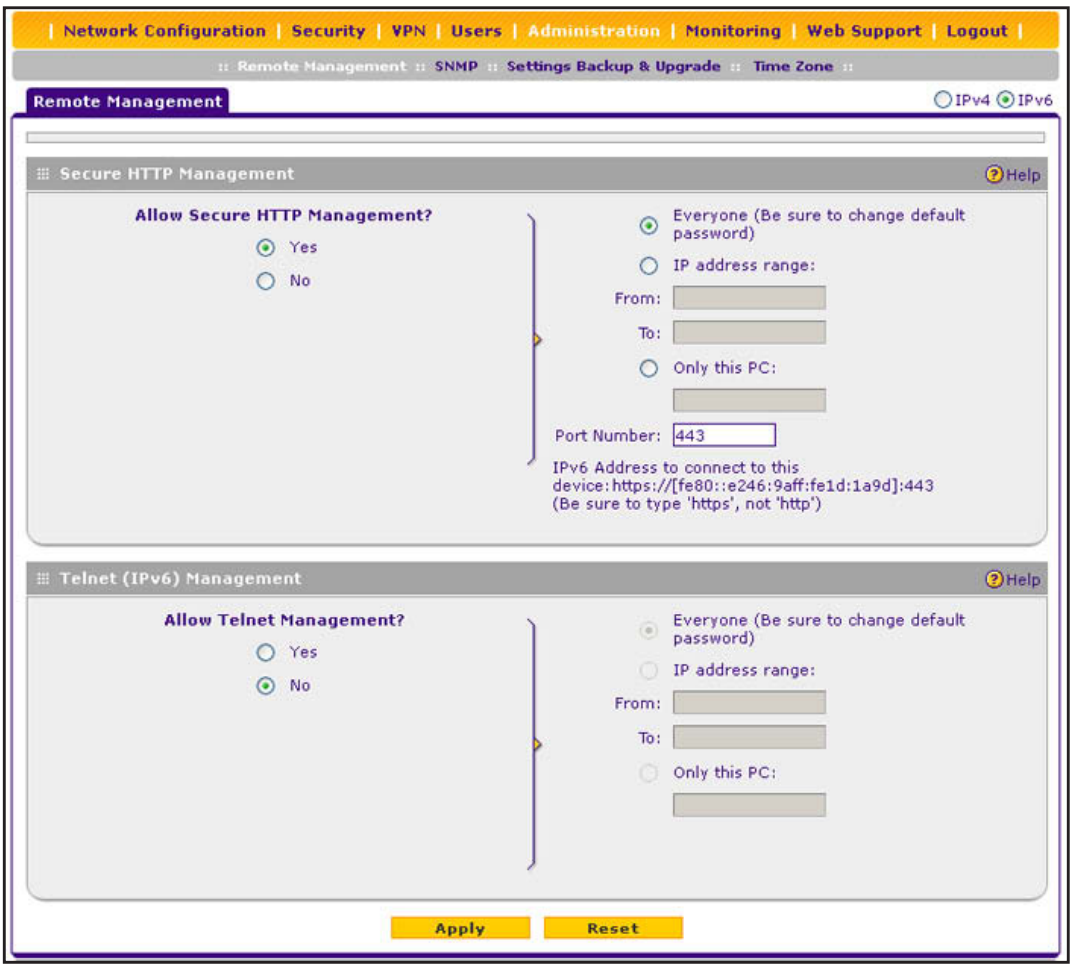

Figure 200. Remote Management screen for IPv6

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

Table 79. 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.
	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.

Table 79. Remote Management screen settings for IPv4 and IPv6 (continued)

Setting	Description	
Allow Secure HTTP Management? (continued)	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.
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 wireless 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 wireless VPN firewall from the Internet. You need to enter https:// (*not* http://) and type the wireless VPN firewall's WAN IP address and port number in your browser. For example, if the wireless 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 wireless 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. For instructions about how to restrict administrator access by IP address, see *Set User Login Policies* on page 309.

- To maintain security, the wireless VPN firewall rejects a login that uses http://*address* rather than the SSL https://*address*.
- The first time that you remotely connect to the wireless 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 wireless VPN firewall by running **`tracert`** from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter **`tracert wireless VPN firewall.mynetgear.net`**, and the WAN IP address that your ISP assigned to the wireless 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 wireless VPN firewall (see *Rear Panel* on page 18).

You can access the CLI from a communications terminal when the wireless 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 wireless 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 your wireless 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 wireless 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.)

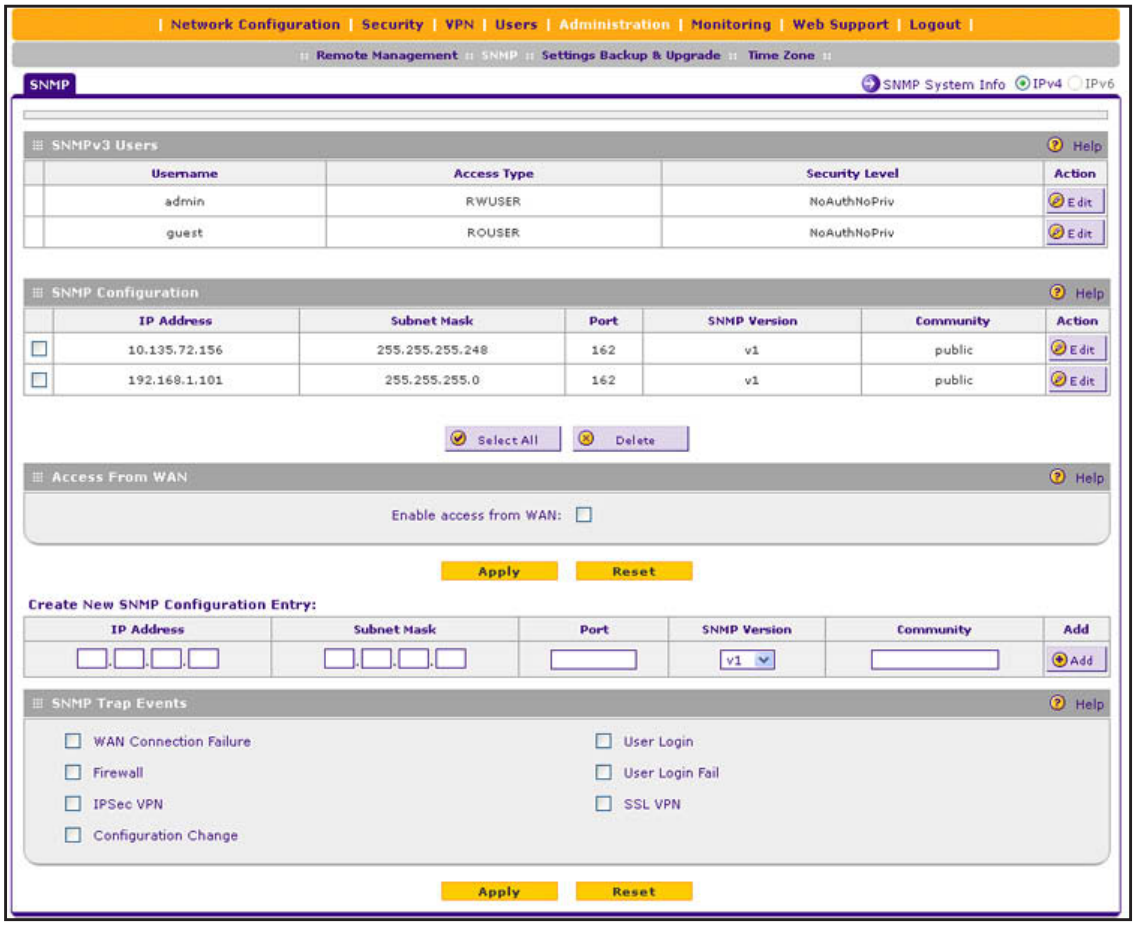

Figure 201.

The SNMPv3 Users table includes the default SNMPv3 users that are preconfigured on the wireless 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 enable access from the WAN, specify a new SNMP configuration, or enable SNMP trap events, enter the settings as described in the following table:

Table 80. 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 wireless 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 wireless 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.
SNMP Version	From the drop-down list, select the SNMP version: • **v1**. SNMPv1. • **v2c**. SNMPv2c. • **v3**. SNMPv3.
Port	Enter the port number of the new SNMP manager. The default port number is 162.
Community	Enter the community string that allows the SNMP manager access to the MIB objects of the wireless VPN firewall for the purpose of reading only.

Table 80. SNMP screen settings (continued)

Setting	Description
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. • **Configuration Change**. Sent when the configuration of the wireless VPN firewall changes. • **User Login**. Sent when a user logs in to the wireless VPN firewall. • **User Login Fail**. Sent when a user attempt to log in to the wireless VPN firewall but fails to do so. • **SSL VPN**. Sent when an SSL VPN tunnel is established or disconnected.	

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:

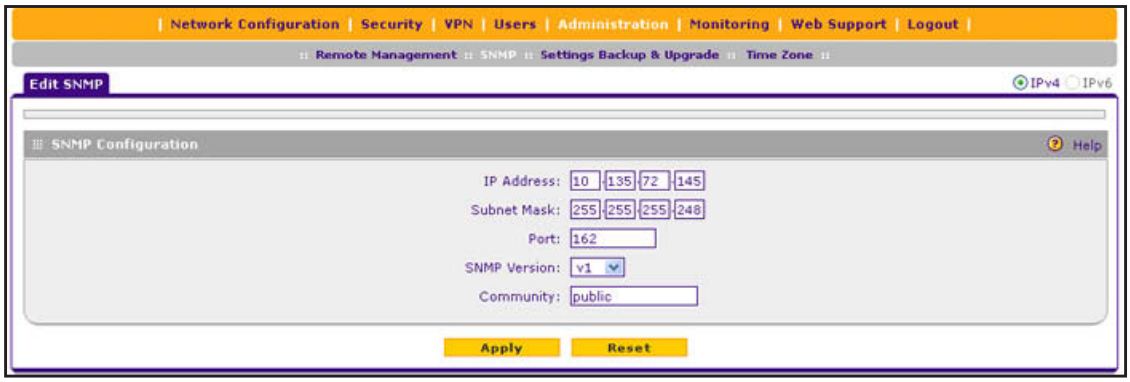

Figure 202.

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 201* on page 338), 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 201* on page 338), 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:

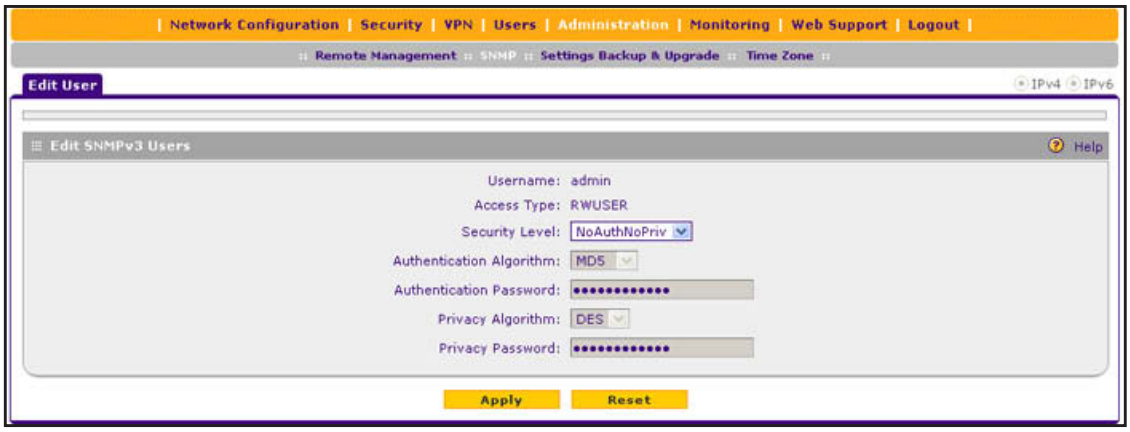

Figure 203.

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

Table 81. 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.
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 wireless 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 wireless VPN firewall.

Table 81. Edit User screen settings for SNMPv3 users (continued)

Setting	Description
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 wireless 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 wireless VPN firewall.

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

➢ **To configure the SNMP system information:**

1. On the SNMP screen (see *Figure 201* on page 338), click the **SNMP System Info** option arrow in the upper right of the screen. The SNMP SysConfiguration screen displays:

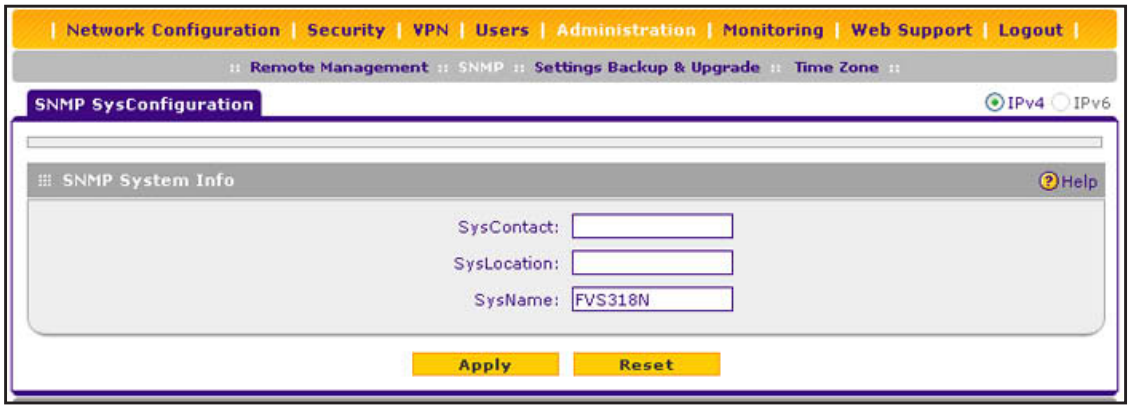

Figure 204.

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

Table 82. 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 wireless VPN firewall. This setting is optional.
SysName	Enter the name of the wireless VPN firewall for SNMP identification purposes. The default name is FVS318N.

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

Manage the Configuration File

The configuration settings of the wireless VPN firewall are stored in a configuration file on the wireless 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 wireless VPN firewall is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the wireless 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 343)
- Restore saved settings from the backed-up file (see *Restore Settings* on page 344)
- Revert to the factory default settings (see *Revert to Factory Default Settings* on page 345)
- Update the firmware (see *Update the Firmware* on page 345)

To display the Settings Backup and Firmware Upgrade screen, select **Administration > Settings Backup & Upgrade**.

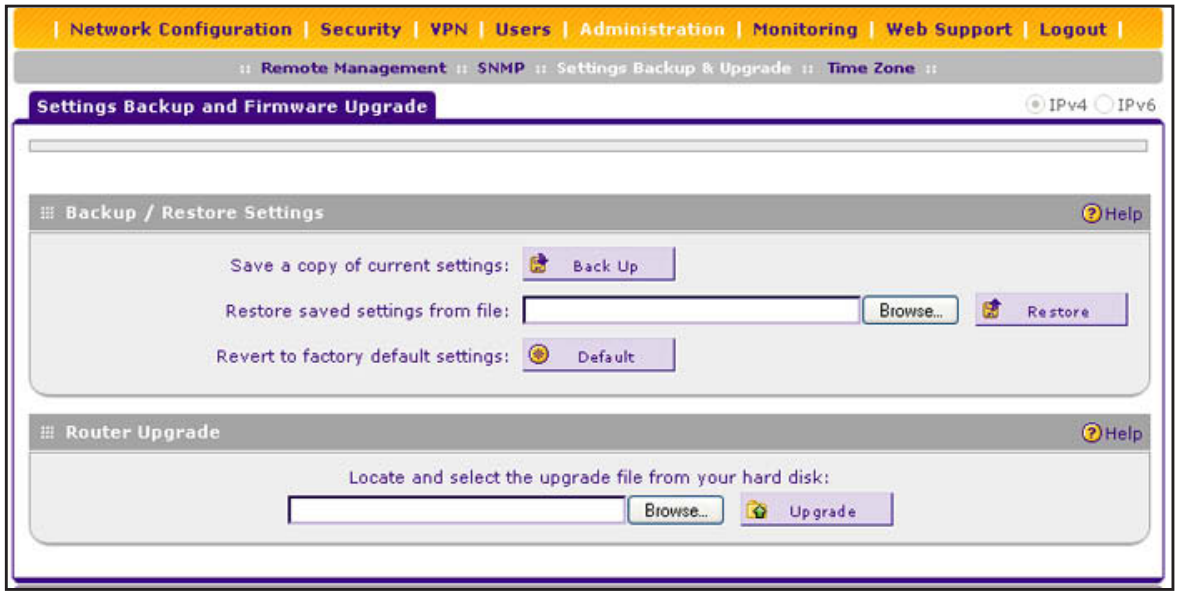

Figure 205.

Back Up Settings

The backup feature saves all wireless 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 wireless VPN firewall that has the same language and management software versions. Remember to change the IP address of the second wireless 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 the previous figure), next to Save a copy of current settings, click the **Backup** button to save a copy of your current settings. A screen displays, showing the file name of the backup file (FVS318N.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 wireless VPN firewall system software.

➢ **To restore settings from a backup file:**

1. On the Settings Backup and Firmware Upgrade screen (see the previous figure), next to Restore saved settings from file, click **Browse**.
2. Locate and select the previously saved backup file (by default, FVS318N.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 wireless 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 165 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 wireless VPN firewall, shut down the computer, or do anything else to the wireless VPN firewall until the settings have been fully restored.

Revert to Factory Default Settings

➢ **To reset the wireless 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 wireless VPN firewall (see *Rear Panel* on page 18) for about eight 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 previous figure), next to Revert to factory defaults settings, click the **Default** button, and confirm your selection.

The wireless 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 165 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 wireless 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 wireless VPN firewall's password is **password**, and the LAN IP address is **192.168.1.1**.

Update the Firmware

You can install a different version of the wireless VPN firewall firmware from the Settings Backup and Firmware Upgrade screen. To view the current version of the firmware that the wireless 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 updated 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 FVS318N 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 wireless VPN firewall's software.
4. On the Settings Backup and Firmware Upgrade screen of the wireless VPN firewall (see the previous figure), 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 wireless 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 wireless VPN firewall, or do anything else to the wireless VPN firewall until the wireless VPN firewall has fully rebooted.

7. When the reboot process is complete, log in to the wireless VPN firewall again. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)
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 wireless VPN firewall after upgrading it. See the firmware release notes that NETGEAR makes available.

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 wireless VPN firewall logs and reports are accurate.

➢ **To set time, date, and NTP servers:**

1. Select **Administration > Time Zone**. The Time Zone screen displays:

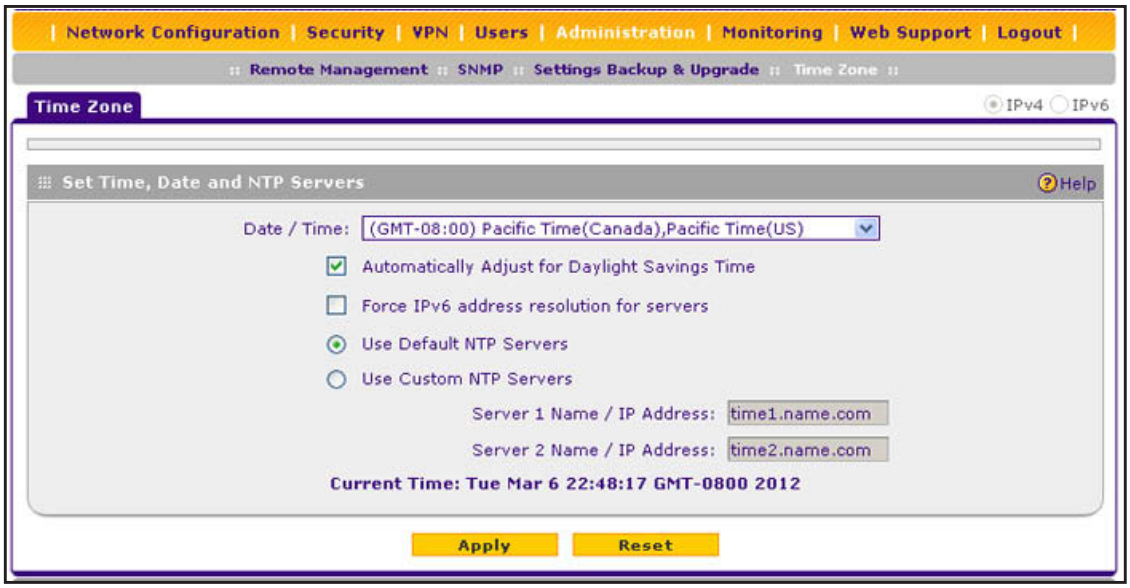

Figure 206.

The bottom of the screen display the current weekday, date, time, time zone, and year (in the example in the previous figure: Current Time: Tue Mar 6 22:48:17 GMT-0800 2012).

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

Table 83. Time Zone screen settings

Setting	Description
Date/Time	From the drop-down list, select the local time zone in which the wireless 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.
Force IPv6 address resolution 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.

Table 83. 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 wireless VPN firewall regularly updates its RTC by contacting a default NETGEAR NTP server on the Internet. • **Use Custom NTP Servers**. The wireless 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 wireless VPN firewall determines the IP address of the NTP server by performing a DNS lookup. Before the wireless VPN firewall can perform this lookup, you need to configure a DNS server address on the Broadband ISP Settings screen (see *Manually Configure an IPv4 Internet Connection* on page 32.)

Monitor System Access and Performance

10

This chapter describes the system-monitoring features of the wireless 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:

- *Enable the WAN 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 352.

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 the WAN port.

➢ **To configure and monitor traffic limits on the WAN port:**

1. Select **Monitoring > Traffic Meter**. The Broadband Traffic Meter screen displays.

   The Internet Traffic Statistics section in the lower part of the screen displays statistics on Internet traffic through the WAN port. If you have not enabled the traffic meter, these statistics are not available.

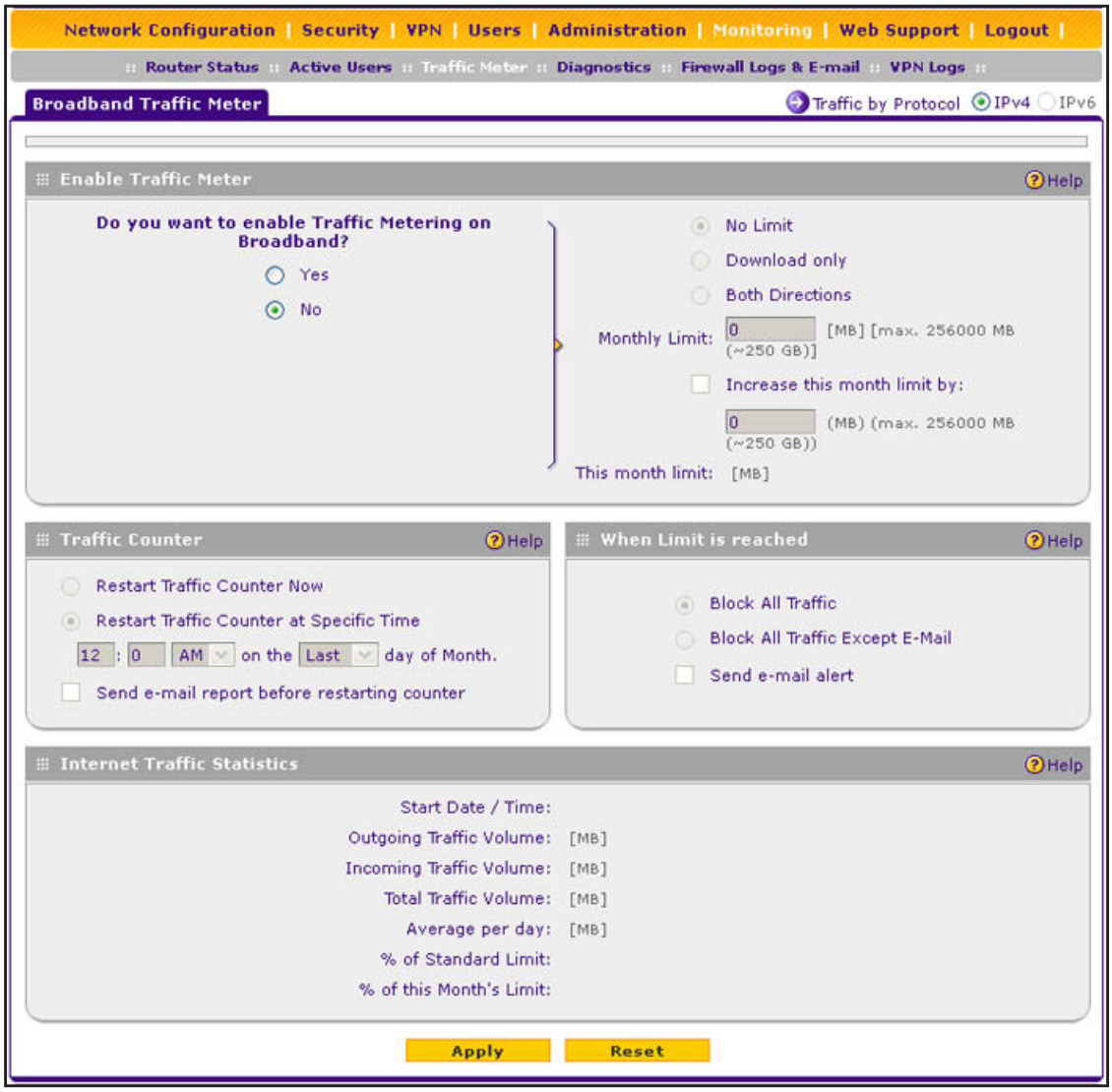

Figure 207.

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

Table 84. Broadband Traffic Meter screen settings

Setting	Description	
Enable Traffic Meter		
Do you want to enable Traffic Metering on Broadband?	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 wireless 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 352).	

Table 84. Broadband 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 wireless 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 352).

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

To display a report of the Internet traffic by type, click the **Traffic by Protocol** option arrow in the upper right of the Broadband 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.

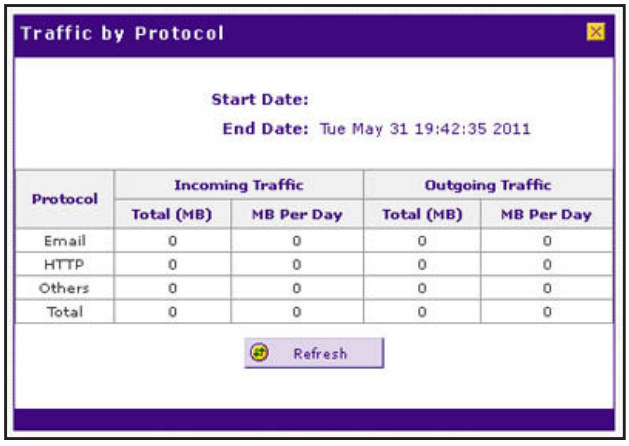

Figure 208.

Configure Logging, Alerts, and Event Notifications

You can configure the wireless 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:

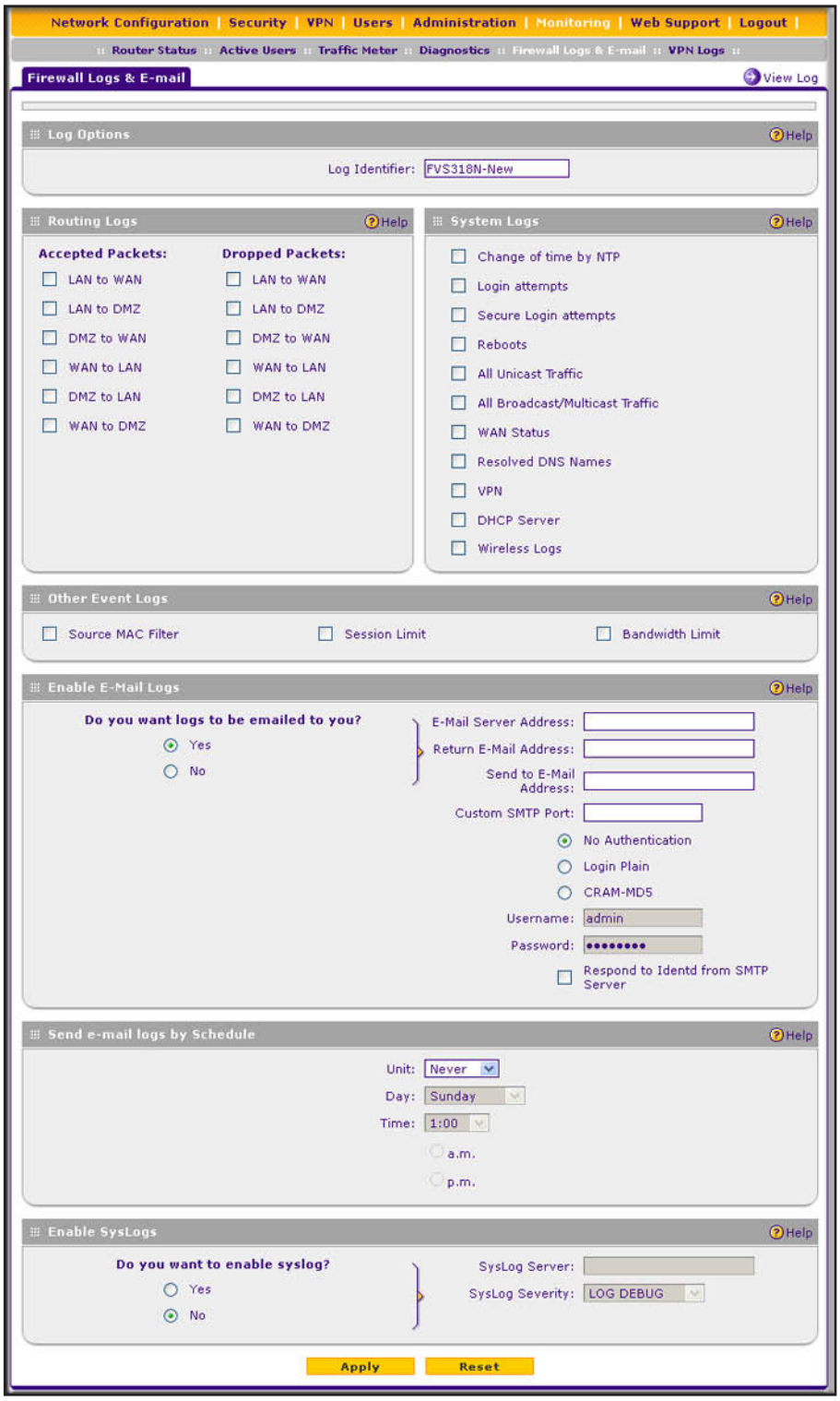

Figure 209.

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

Table 85. 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 FVS318N.
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 wireless 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. • **DHCP Server**. All DHCP server events are logged. • **Wireless Logs**. All wireless events 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 85. 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 wireless 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 wireless 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 fvs_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 85. Firewall Logs & E-mail screen settings (continued)

Setting	Description	
Enable SysLogs		
Do you want to enable syslog?	To enable the wireless 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 wireless 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.

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 wireless 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 wireless VPN firewall:

- Firmware version
- Both IPv4 and IPv6 WAN and LAN port information
- Wireless 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:

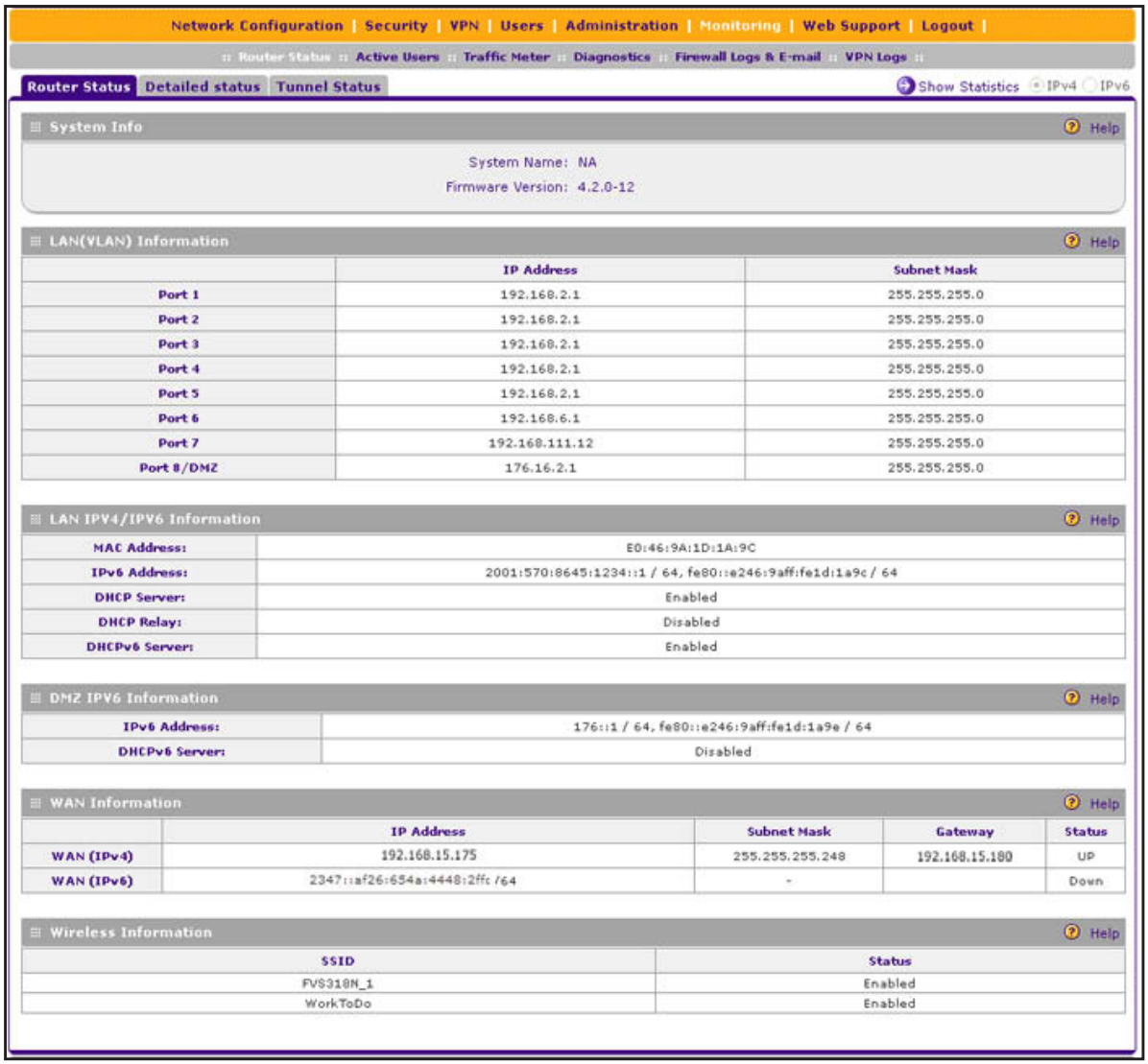

Figure 210.

The following table explains the fields of the Router Status screen:

Table 86. Router Status screen information

Item	Description
System Info	
System Name	The NETGEAR system name.
Firmware Version	The installed firmware version.
LAN (VLAN) Information	
For each of the LAN ports, the screen shows the IP address and subnet mask. For more detailed information, see *Table 88* on page 364.	

Table 86. Router Status screen information (continued)

Item	Description
LAN IPv4/IPv6 Information	
MAC Address	The MAC address of the wireless VPN firewall.
IPv6 Address	The IPv6 address that is assigned to the wireless VPN firewall. For information about configuring the IPv6 address, see *Configure the IPv6 Internet Connection and WAN Settings* on page 38.
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 60.
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 60.
DHCPv6 Server	The status of the DHCPv6 server (Enabled or Disabled) for the LAN. For information about configuring the DHCPv6 server for the LAN, see *Manage the IPv6 LAN* on page 74.
DMZ IPv6 Information	
IPv6 Address	The IPv6 address that is assigned to the DMZ port. For information about configuring the IPv6 address for the DMZ, see *Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic* on page 86.
DHCPv6 Server	The status of the DHCPv6 server (Enabled or Disabled) for the DMZ. For information about configuring the DHCPv6 server for the DMZ, see *Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic* on page 86.
WAN Information	
WAN (IPv4)	The screen shows the IPv4 address, subnet mask, gateway, and status of the port (UP or Down). For more detailed information, see *Table 88* on page 364.
WAN (IPv6)	The screen shows the IPv6 address, gateway, and status of the port (UP or Down). For more detailed information, see *Table 88* on page 364.
Wireless Information	
SSID	The status of the SSID (Enabled or Disabled). For more detailed information, see *Table 88* on page 364.

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 211.

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 87. Router Statistics screen information

Item	Description
System up Time. The period since the last time that the wireless VPN firewall was started up.	
Router Statistics	
The following statistics are displayed for the broadband (WAN) interface, for all LAN interfaces combined, and for the DMZ port.	
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 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:

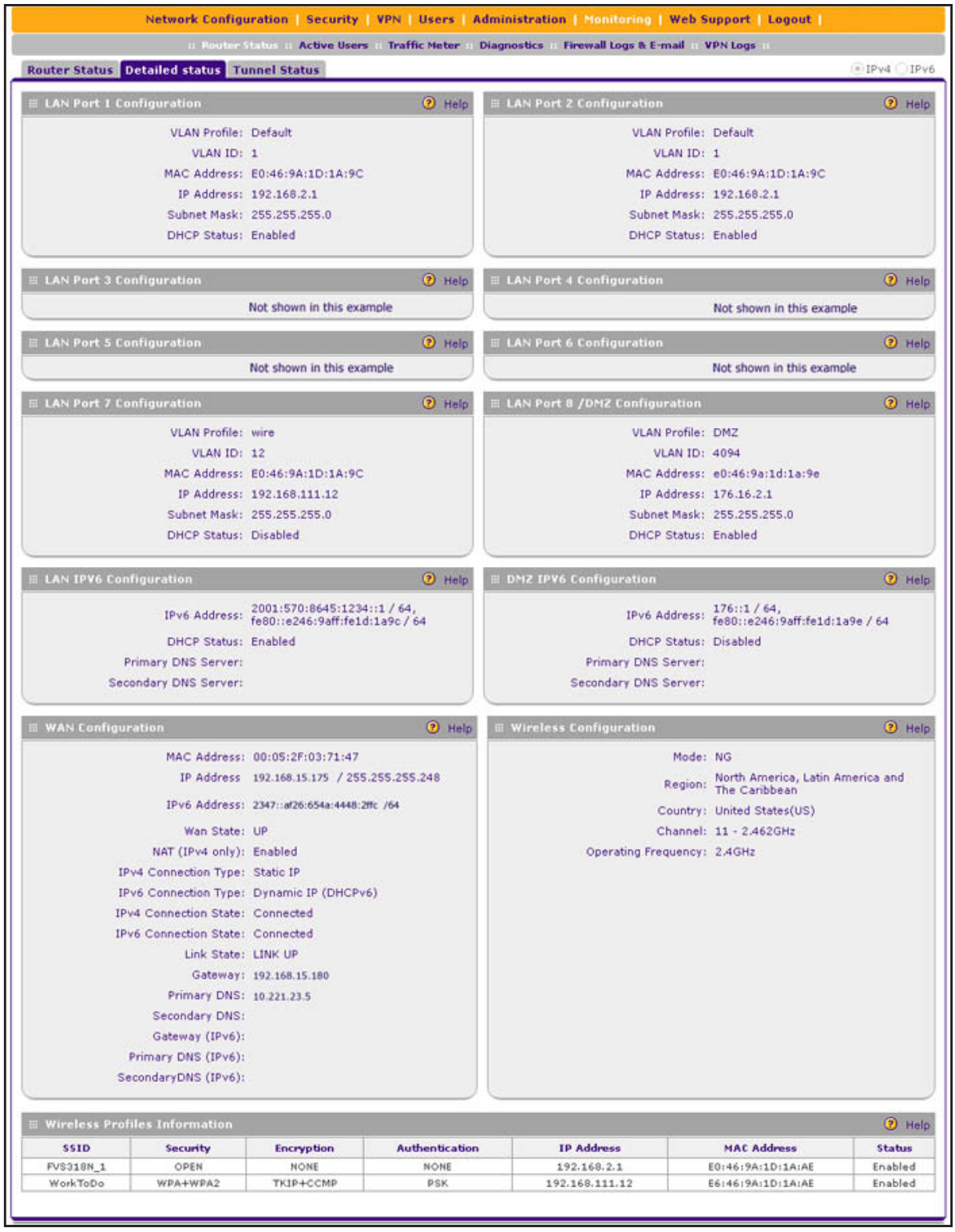
Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
Tunnel Status
IPv4 IPv6
LAN Port 1 Configuration
Help
VLAN Profile: Default
VLAN ID: 1
MAC Address: E0:46:9A:1D:1A:9C
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled
LAN Port 2 Configuration
Help
VLAN Profile: Default
VLAN ID: 1
MAC Address: E0:46:9A:1D:1A:9C
IP Address: 192.168.2.1
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 Port 5 Configuration
Help
Not shown in this example
LAN Port 6 Configuration
Help
Not shown in this example
LAN Port 7 Configuration
Help
VLAN Profile: wire
VLAN ID: 12
MAC Address: E0:46:9A:1D:1A:9C
IP Address: 192.168.111.12
Subnet Mask: 255.255.255.0
DHCP Status: Disabled
LAN Port 8 /DMZ Configuration
Help
VLAN Profile: DMZ
VLAN ID: 4094
MAC Address: e0:46:9a:1d:1a:9e
IP Address: 176.16.2.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled
LAN IPV6 Configuration
Help
IPv6 Address: 2001:570:8645:1234::1 / 64, fe80::e246:9aff:fe1d:1a9c / 64
DHCP Status: Enabled
Primary DNS Server:
Secondary DNS Server:
DMZ IPV6 Configuration
Help
IPv6 Address: 176::1 / 64, fe80::e246:9aff:fe1d:1a9e / 64
DHCP Status: Disabled
Primary DNS Server:
Secondary DNS Server:
WAN Configuration
Help
MAC Address: 00:05:2F:03:71:47
IP Address 192.168.15.175 / 255.255.255.248
IPv6 Address: 2347::af26:654a:4448:2ffc /64
Wan State: UP
NAT (IPv4 only): Enabled
IPv4 Connection Type: Static IP
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Connected
IPv6 Connection State: Connected
Link State: LINK UP
Gateway: 192.168.15.180
Primary DNS: 10.221.23.5
Secondary DNS:
Gateway (IPv6):
Primary DNS (IPv6):
SecondaryDNS (IPv6):
Wireless Configuration
Help
Mode: NG
Region: North America, Latin America and The Caribbean
Country: United States(US)
Channel: 11 - 2.462GHz
Operating Frequency: 2.4GHz
Wireless Profiles Information
Help
SSID | Security | Encryption | Authentication | IP Address | MAC Address | Status
FVS318N_1 | OPEN | NONE | NONE | 192.168.2.1 | E0:46:9A:1D:1A:AE | Enabled
WorkToDo | WPA+WPA2 | TKIP+CCMP | PSK | 192.168.111.12 | E6:46:9A:1D:1A:AE | Enabled

Figure 212.

The following table explains the fields of the Detailed Status screen:

Table 88. 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 this port on the LAN Setup screen (see *Assign and Manage VLAN Profiles* on page 58). If the VLAN is not enabled on this port, the default profile (with VLAN ID 1) is assigned automatically.
VLAN ID	The VLAN ID that you assigned to this port on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 60). If the default VLAN profile is used, the VLAN ID is 1, which means that all tagged and untagged traffic can pass on this port.
MAC Address	The MAC address 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, 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 65). • 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 8 can be assigned as the DMZ port, in which case it has a MAC address that differs from the other LAN ports. For information about configuring the DMZ port, see *Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic* on page 86.
IP Address	The IP address for this 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 60.
Subnet Mask	The subnet mask for this 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 60.
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 60.
WAN Configuration	
MAC Address	The default MAC address for the port or the MAC address that you have specified on the Broadband Advanced Options screen for the port. For information about configuring the MAC address, see *Configure Advanced WAN Options and Other Tasks* on page 51.
IP Address	The IPv4 address and subnet mask 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 27.
IPv6 Address	The IPv6 address of the WAN port. For information about configuring the IPv4 address of the WAN port, see *Configure the IPv6 Internet Connection and WAN Settings* on page 38.
WAN State	The WAN state can be either UP or DOWN, depending on whether the port is connected to the Internet.

Table 88. Detailed Status screen information (continued)

Item	Description	
NAT (IPv4 only)	The NAT state can be either Enabled or Disabled, depending on whether NAT is enabled (see *Network Address Translation* on page 28) or classical routing is enabled (see *Classical Routing* on page 28).	
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 27.	
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 38.	
IPv4 Connection State	The IPv4 connection state can be either Connected or Not 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 27.	
IPv6 Connection State	The IPv6 connection state can be either Connected or Not 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 38.	
Link State	The link state can be either LINK UP or LINK DOWN, depending on whether the WAN port is physically connected to a modem, dish, or router. For information about connecting a WAN port, see the *ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N Installation Guide*.	
Gateway	The IP address of the gateway.	These IPv4 settings are either obtained dynamically from your ISP or specified by you on the Broadband ISP Settings (IPv4) screen (see *Manually Configure an IPv4 Internet Connection* on page 32).
Primary DNS Server	The IP address of the primary DNS server.	
Secondary DNS Server	The IP address of the secondary DNS server.	
Gateway (IPv6)	The IP address of the gateway.	These IPv6 settings are either obtained dynamically from your ISP or specified by you on the Broadband ISP Settings (IPv6) screen (see *Configure a Static IPv6 Internet Connection* on page 42).
Primary DNS Server (IPv6)	The IP address of the primary DNS server.	
Secondary DNS Server (IPv6)	The IP address of the secondary DNS server.	
Wireless Configuration		
Mode	The wireless mode of the radio.	For information about how to configure the wireless radio, see *Configure the Basic Radio Settings* on page 109.
Region	The region that is assigned to the radio.	
Country	The country that is assigned to the radio.	
Channel	The active channel on the radio.	
Operating Frequency	The operating frequency of the radio.	

Table 88. Detailed Status screen information (continued)

Item	Description	
Wireless Profile Information		
SSID	The SSID of the wireless profile.	For information about configuring wireless profiles, see *Configure and Enable Wireless Profiles* on page 116.
Security Settings	The security settings of the wireless profile.	
Encryption	The encryption that is configured on the wireless profile,	
Authentication	The authentication that is configured on the wireless profile,	
IP Address	The IP address of the wireless profile.	
AP MAC Address	The MAC address of the wireless profile.	
Status	The status can be Enabled or Disabled, depending on whether the wireless profile is enabled.	

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:

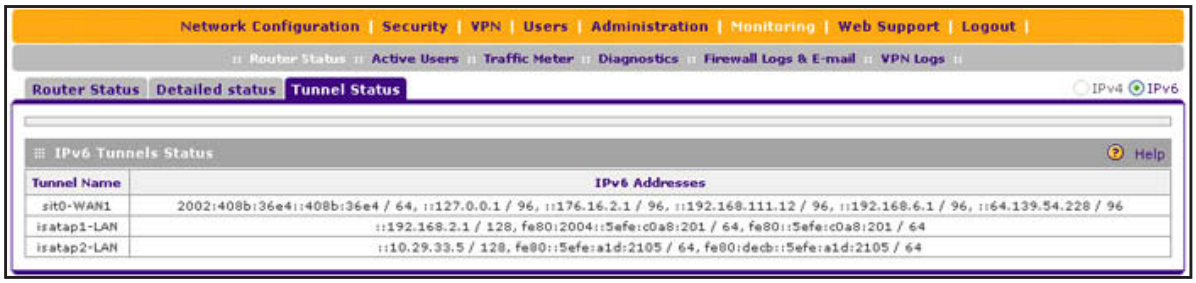

Figure 213.

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 and L2TP Users

The Connection Status screens display a list of IPSec VPN connections, SSL VPN connections, and L2TP users who are logged in to the wireless 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:

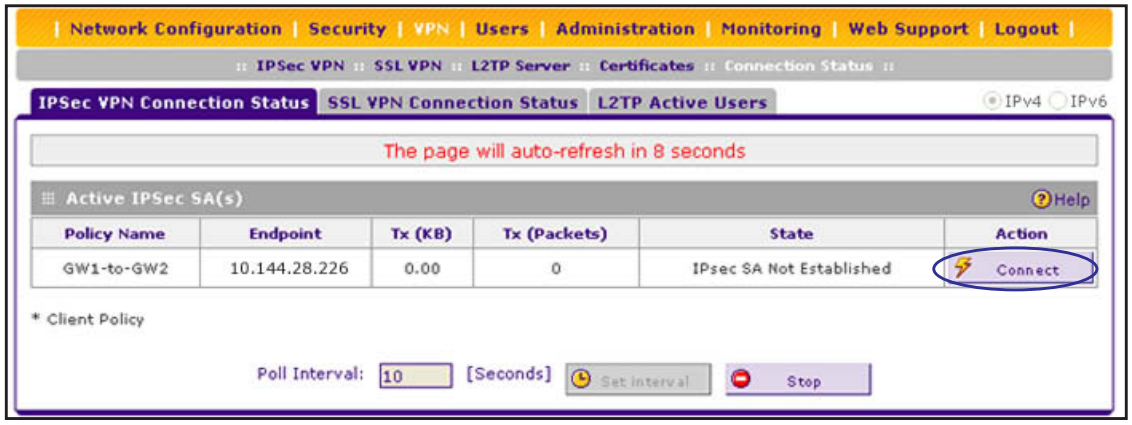

Figure 214.

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.

- **To view the active SSL VPN connections:**

Select **VPN > Connection Status > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:

Figure 215.

The active user's user name, group, and IP address are listed in the table with a time stamp indicating the time and date that the user connected.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

- **To view the active L2TP tunnel users:**

  Select **VPN > Connection Status > L2TP Active Users**. The L2TP Active Users screen displays:

Figure 216.

The active user name, client's IP address on the remote LAC, and IP address that is assigned by the L2TP server on the wireless VPN firewall are listed in the table.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

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.

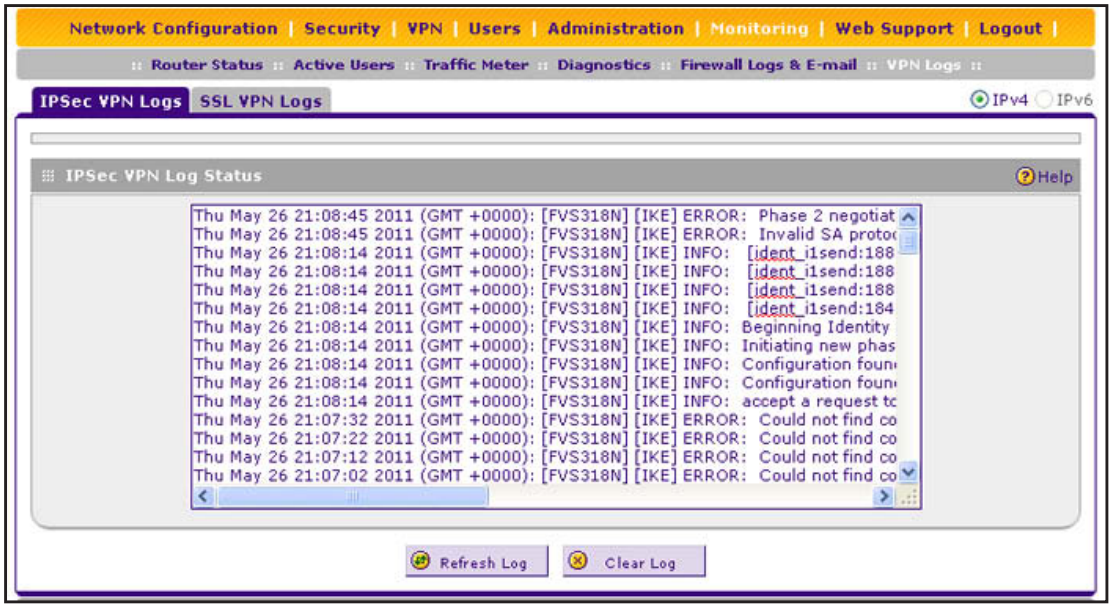

Figure 217.

➢ **To display the SSL VPN log:**

Select **Monitoring > VPN Logs > SSL VPN Logs**. The SSL VPN Logs screen displays:

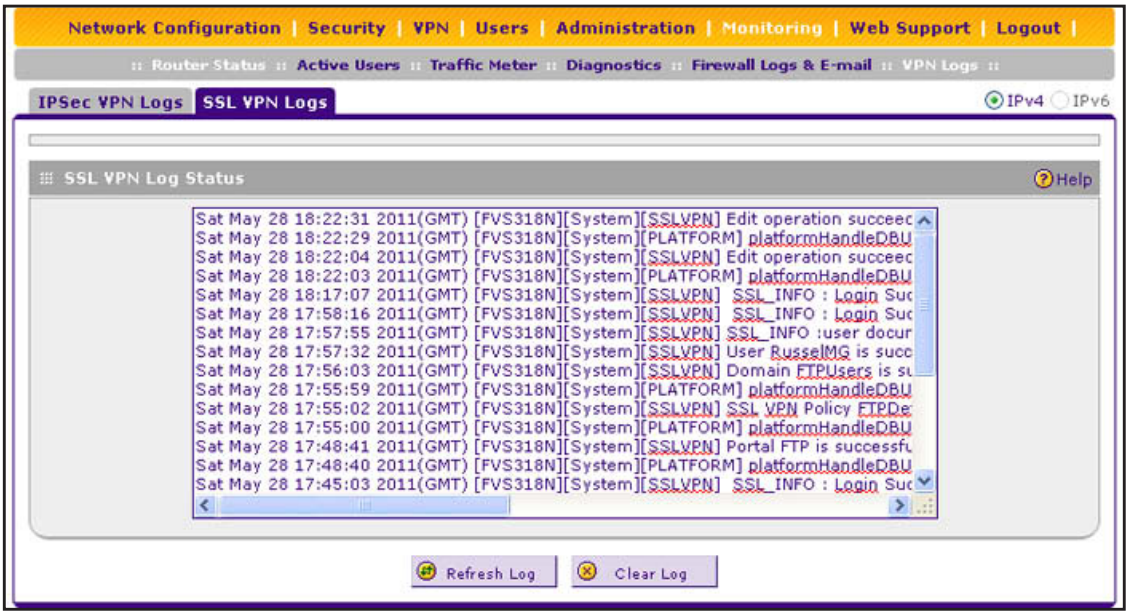

Figure 218.

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.)

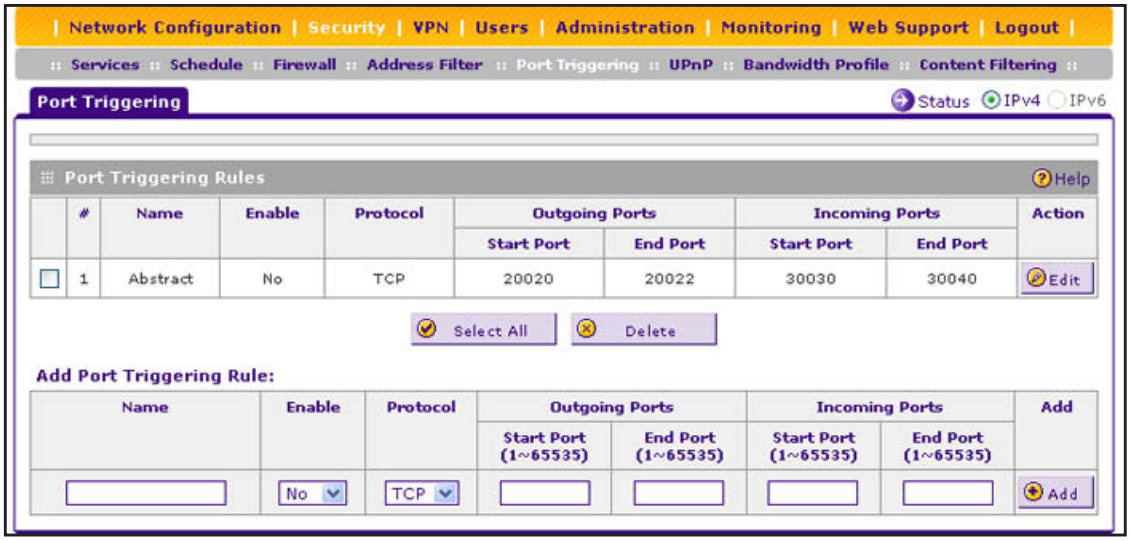

Figure 219.

2. Click the **Status** option arrow in the upper right of the Port Triggering screen. The Port Triggering Status pop-up screen displays.

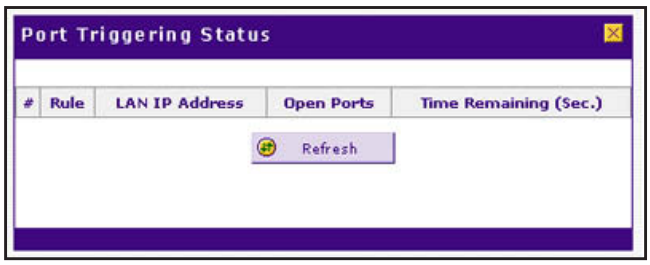

Figure 220.

The Port Triggering Status screen displays the information that is described in the following table:

Table 89. 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 the WAN port:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv4)**. The Broadband ISP Settings (IPv4) screen displays (see *Figure 10* on page 30).
2. Click the **Broadband Status** option arrow in the upper right of the screen to display the Connection Status pop-up screen. (The following figure shows a static IP address configuration.)

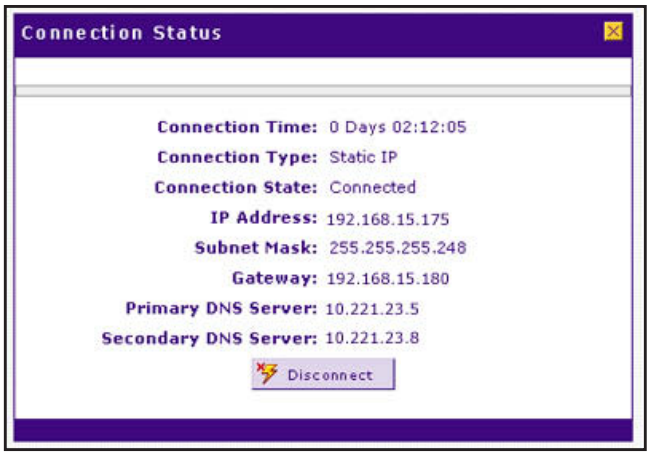

Figure 221.

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 90. Connection Status screen information for an IPv4 connection

Item	Description
Connection Time	The period that the wireless 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 Broadband ISP Settings (IPv4) screen. **Note:** For more information, see *Let the Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 29 and *Manually Configure an IPv4 Internet Connection* on page 32.
Subnet Mask	
Gateway	
DNS Server	
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 Broadband ISP Settings screen. **Note:** For more information, see *Let the Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 29 and *Manually Configure an IPv4 Internet Connection* on page 32.
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 > Broadband ISP Settings (IPv6)**. The Broadband ISP Settings (IPv6) screen displays (see *Figure 20* on page 41).
2. Click the **Status** option arrow in the upper right of the screen to display the Connection Status pop-up screen. (The following figure shows a dynamic IP address configuration.)

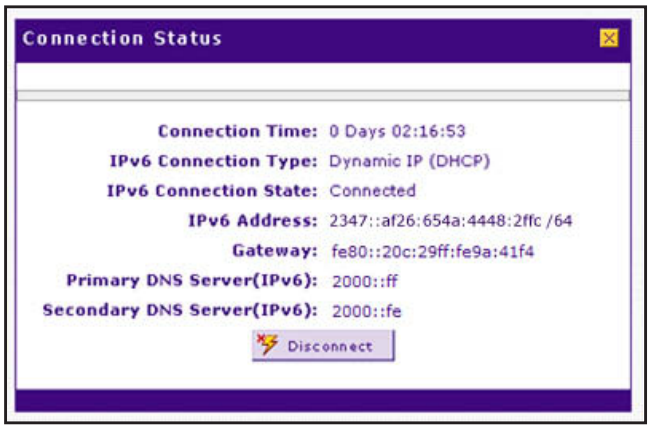

Figure 222.

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 91. Connection Status screen information for an IPv6 connection

Item	Description
Connection Time	The period that the wireless 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.
IP Address	The IPv6 addresses that were automatically detected or that you configured on the Broadband ISP Settings (IPv6) 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 40 and *Configure a Static IPv6 Internet Connection* on page 42.
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 wireless 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 Setup > LAN Groups**. The LAN Groups screen displays. (The following figure shows some examples in the Known PCs and Devices table.)

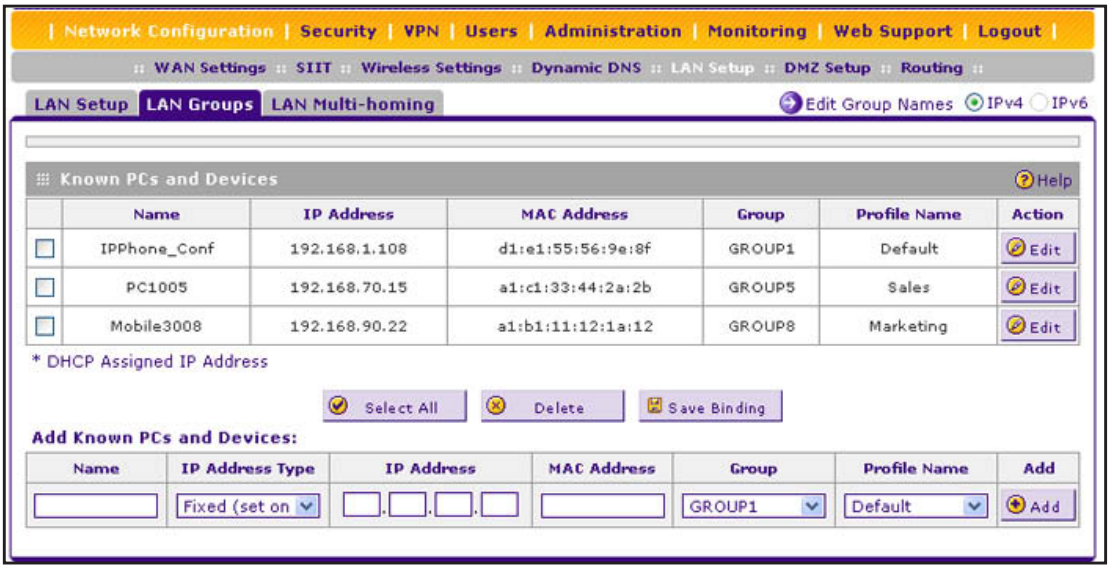

Figure 223.

The Known PCs and Devices table contains a list of all known computers and network devices that are assigned dynamic IP addresses by the wireless 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 69.

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 wireless 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 wireless VPN firewall is rebooted, the data in the Known PCs and Devices table is lost until the wireless VPN firewall rediscovers the devices.

View the DHCP Log

➢ **To review the most recent entries in the DHCP log:**

1. Select **Network Configuration > LAN Setup**. The LAN Setup screen displays the IPv4 settings. (see *Figure 32* on page 60).
2. Click the **DHCP Log** option arrow to the right of the LAN Setup tab. The DHCP Log screen displays:

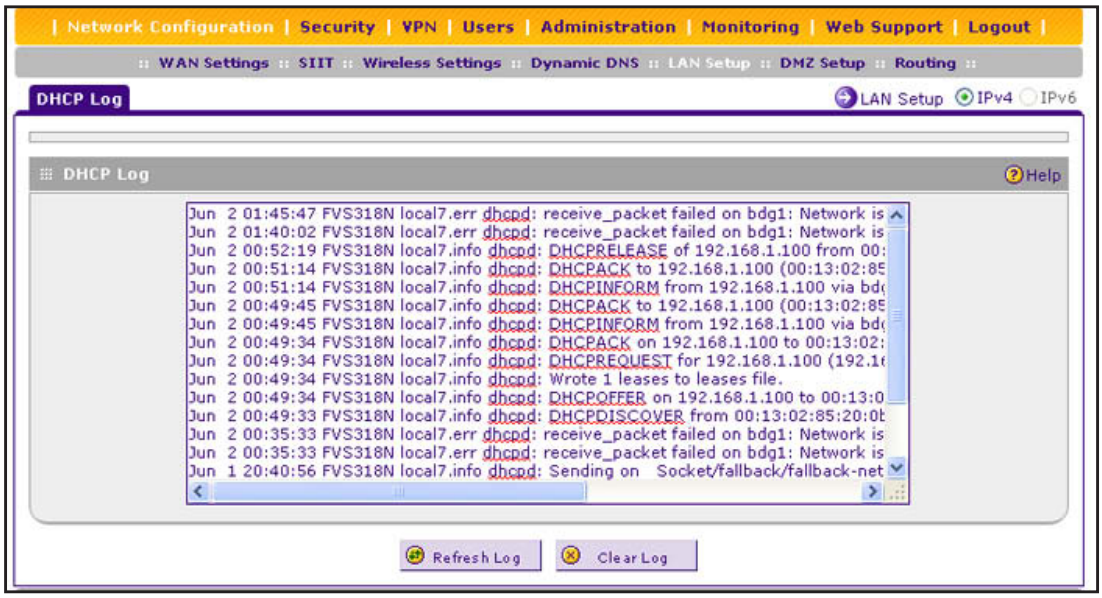

Figure 224.

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 (IPv4) screen, from which you can modify the DHCP settings (see *Configure a VLAN Profile* on page 60).

View the Status of a Wireless Profile

➢ **To view the status of a specific wireless profile:**

1. Select **Network Configuration > Wireless Settings > Wireless Profiles**. The Wireless Profiles screen displays.
2. Click the **Status** button in the Status column for the wireless profile for which you want to display the status information. The Wireless Profile Status screen displays:

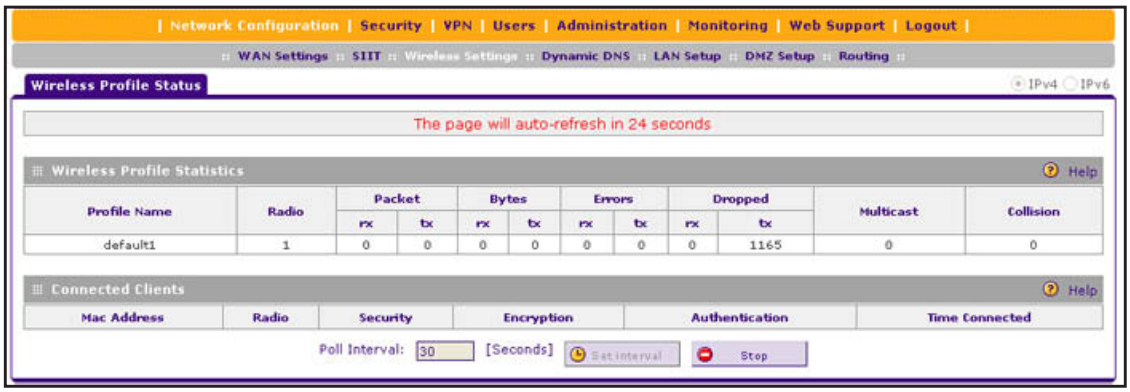

Figure 225.

To change the poll interval period, enter a new value in the Poll Interval field, and click **Set interval**. To stop polling, click **Stop**.

The following table explains the fields of the Wireless Profile Status screen.

Table 92. Wireless Profile Status screen fields

Item	Description
Wireless Profile Statistics	
Profile Name	The name of the wireless profile.
Radio	The radio to which the client is connected. By default, the radio is always 1, indicating the 2.4 GHz radio.
Packet	The number of received (rx) and transmitted (tx) packets on the access point in bytes.
Bytes	The number of received (rx) and transmitted (tx) bytes on the access point.
Errors	The number of received (rx) and transmitted (tx) errors on the access point.
Dropped	The number of received (rx) and transmitted (tx) dropped packets on the access point.
Multicast	The number of received (rx) and transmitted (tx) multicast packets on the access point.
Collisions	The number of signal collisions that occurred on the access point. A collision occurs when the access point attempts to send data at the same time as a wireless station that is connected to the access point.
Connected Clients	
MAC Address	The MAC address of the client.

Table 92. Wireless Profile Status screen fields (continued)

Item	Description
Radio	The radio to which the client is connected. By default, the radio is always 1, indicating the 2.4 GHz radio.
Security	The type of security that the client is using (Open, WEP, WPA, WPA2, or WPA+WPA2).
Encryption	The type of encryption that the client is using (CCMP, TKIP, or TKIP + CCMP).
Authentication	The type of authentication that the client is using (Open, PSK, RADIUS, or PSK+RADIUS).
Time Connected	The period in minutes since the connection was established between the access point and the client.

Diagnostics Utilities

- *Send a Ping Packet*
- *Trace a Route*
- *Look Up a DNS Address*
- *Display the Routing Tables*
- *Capture Packets in Real Time*
- *Reboot the Wireless VPN Firewall Remotely*

The wireless 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.

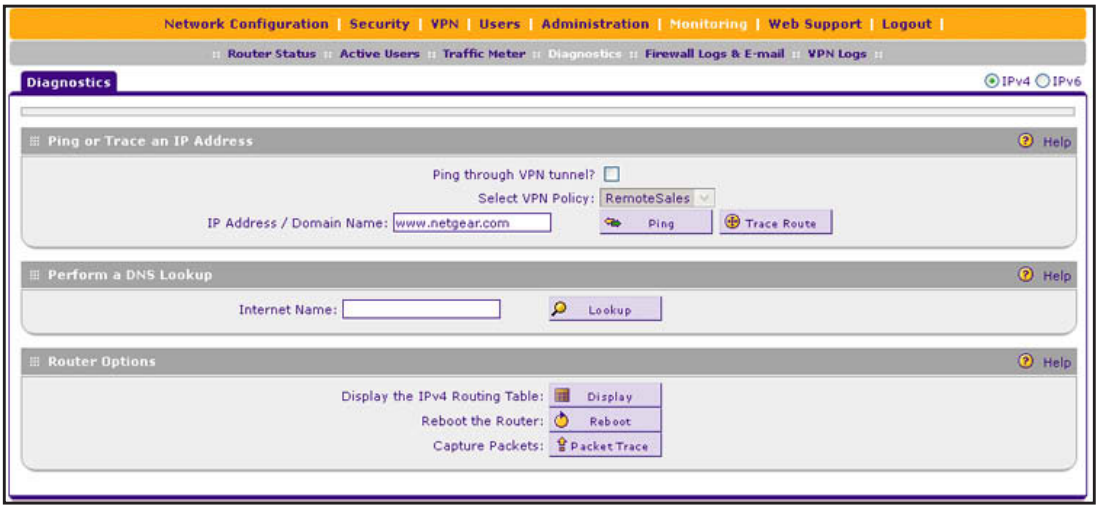

Figure 226.

   - **IPv6**. Select the **IPv6** radio button. The Diagnostics screen displays the IPv6 settings:

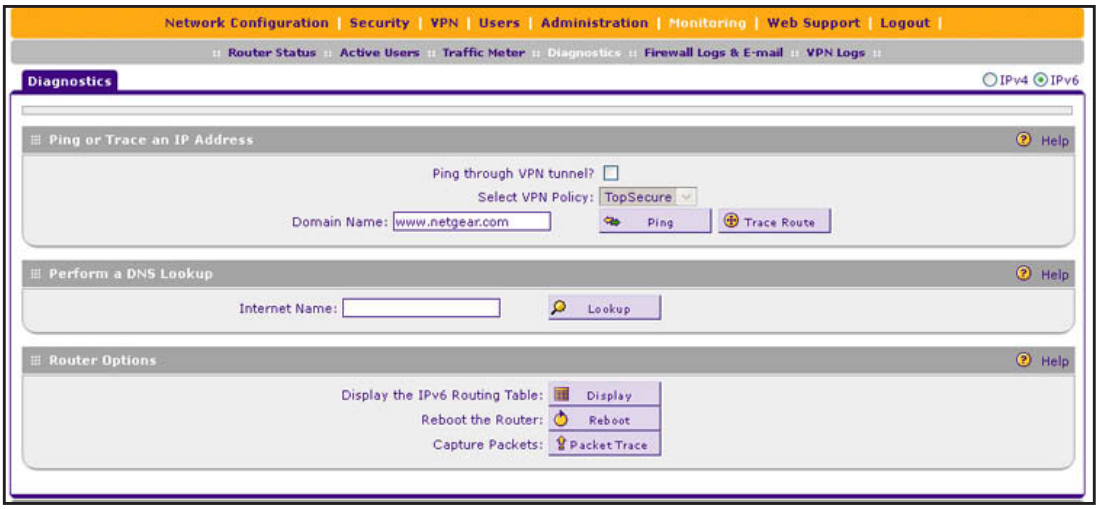

Figure 227.

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 wireless 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. If the specified address is reached through a VPN tunnel, select the **Ping through VPN tunnel?** check box, and select a VPN policy from the Select VPN Policy drop-down list.
3. Click the **Ping** button. The results of the ping are displayed in a new screen.
4. 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 wireless 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. If the specified address is reached through a VPN tunnel, select the **Ping through VPN tunnel?** check box, and select a VPN policy from the Select VPN Policy drop-down list.
3. Click the **Trace Route** 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:

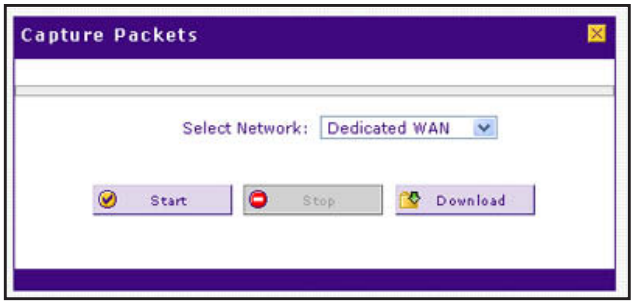

Figure 228.

  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 Wireless VPN Firewall Remotely

You can perform a remote reboot, for example, when the wireless VPN firewall seems to have become unstable or is not operating normally.

Rebooting breaks any existing connections either to the wireless VPN firewall (such as your management session) or through the wireless VPN firewall (for example, LAN users accessing the Internet). However, connections to the Internet are automatically reestablished when possible.

- **To reboot the wireless VPN firewall:**

  In Router Options section of the screen, next to Reboot the Router, click the **Reboot** button. The wireless 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 165 seconds.

11. Troubleshooting

This chapter provides troubleshooting tips and information for the wireless 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 wireless VPN firewall on?

  Go to *Basic Functioning* on page 382.
- Have I connected the wireless VPN firewall correctly?

  Go to *Basic Functioning* on page 382.
- I cannot access the wireless VPN firewall's web management interface.

  Go to *Troubleshoot the Web Management Interface* on page 383.
- A time-out occurs.

  Go to *When You Enter a URL or IP Address, a Time-Out Error Occurs* on page 384.
- I cannot access the Internet or the LAN.

  Go to *Troubleshoot the ISP Connection* on page 385.
- I have problems with the IPv6 connection.

  Go to *Troubleshooting the IPv6 Connection* on page 386
- I have problems with the LAN connection.

  Go to *Troubleshoot a TCP/IP Network Using a Ping Utility* on page 389.
- I want to clear the configuration and start over again.

  Go to *Restore the Default Configuration and Password* on page 391.
- The date or time is not correct.

  Go to *Address Problems with Date and Time* on page 392.
- I need more information.

  Go to *Access the Knowledge Base and Documentation* on page 392.

Note: The wireless VPN firewall's diagnostic tools are described in *Diagnostics Utilities* on page 376.

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 wireless 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 two 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 wireless VPN firewall is turned on, make sure that the power cord is correctly connected to your wireless 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 wireless VPN firewall is powered on, the Test LED turns on for approximately two minutes and then turns off when the wireless VPN firewall has completed its initialization. If the Test LED remains on, a fault occurred within the wireless 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 wireless VPN firewall recovers.
  - Reset the wireless VPN firewall's configuration to factory default settings. Doing so sets the wireless VPN firewall's IP address to **192.168.1.1**. This procedure is described in *Restore the Default Configuration and Password* on page 391.

  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 wireless 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 wireless 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 wireless 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 wireless 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 wireless VPN firewall and reboot your computer.
  - If your wireless VPN firewall's IP address has been changed and you do not know the current IP address, reset the wireless VPN firewall's configuration to factory default settings. This sets the wireless VPN firewall's IP address to **192.168.1.1**. This procedure is described in *Restore the Default Configuration and Password* on page 391.

    Tip: If you do not want to revert to the factory default settings and lose your configuration settings, you can reboot the wireless VPN firewall and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the wireless 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 wireless VPN firewall, your computer's IP address does not need to be on the same subnet as the wireless VPN firewall.

If the wireless 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 the Broadband ISP Settings screen. For more information, see *Manually Configure an IPv4 Internet Connection* on page 32.
- If the computer is configured correctly, but still not working, ensure that the wireless VPN firewall is connected and turned on. Connect to the web management interface, and check the wireless VPN firewall's settings. If you cannot connect to the wireless VPN firewall, see the information in the previous section (*Troubleshoot the Web Management Interface* on page 383).
- If the wireless 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 wireless VPN firewall is unable to access the Internet, you should first determine whether the wireless VPN firewall is able to obtain a WAN IP address from the ISP. Unless you were assigned a static IP address, your wireless 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 wireless VPN firewall's configuration at https://192.168.1.1.
3. Select **Network Configuration > WAN Settings > Broadband ISP Settings**. The Broadband ISP Settings screen for IPv4 displays.
4. Take one of the following actions:
   - **For IPv4**. Click the **Broadband Status** option arrow. The Connection Status pop-up screen for IPv4 displays (see *Figure 11* on page 31).
   - **For IPv6**. In the upper right of the screen, select the **IPv6** radio button. The ISP Broadband Settings screen displays the IPv6 settings. Then click the **Status** option arrow. The Connection Status pop-up screen for IPv6 displays (see *Figure 21* on page 42).
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 wireless VPN firewall has not obtained an IP address from your ISP, or for IPv6, has not obtained or generated an IP address.

➢ **If your wireless 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 wireless 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 wireless VPN firewall.
3. Wait five 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 wireless VPN firewall.

If your wireless 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 the Broadband ISP Settings screen for IPv4, 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 32.

- 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 wireless VPN firewall's MAC address.
  - Configure your wireless VPN firewall to spoof your computer's MAC address. You can do this in the Router's MAC Address section on the Broadband Advanced Options screen. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 51.

If your wireless 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 wireless 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 wireless VPN firewall or the computer from which you are trying to connect to the wireless VPN firewall:

Check the wireless VPN firewall:

- By default, the wireless VPN firewall is set to IPv4-only mode. Make sure that the wireless VPN firewall is set to IPv4/IPv6 mode (see *Configure the IPv6 Routing Mode* on page 39).
- Make sure that the ISP settings are correct (see *Configure a Static IPv6 Internet Connection* on page 42). The wireless VPN firewall cannot receive a valid IPv6 address if the Internet connection is not correctly configured.
- Make sure that the wireless VPN firewall can provide IPv6 addresses to the computers on the LAN (see *Manage the IPv6 LAN* on page 74). Check the settings on the LAN Setup (IPv6) screen, 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 wireless VPN firewall. The Local Area Connection Properties screen displays:

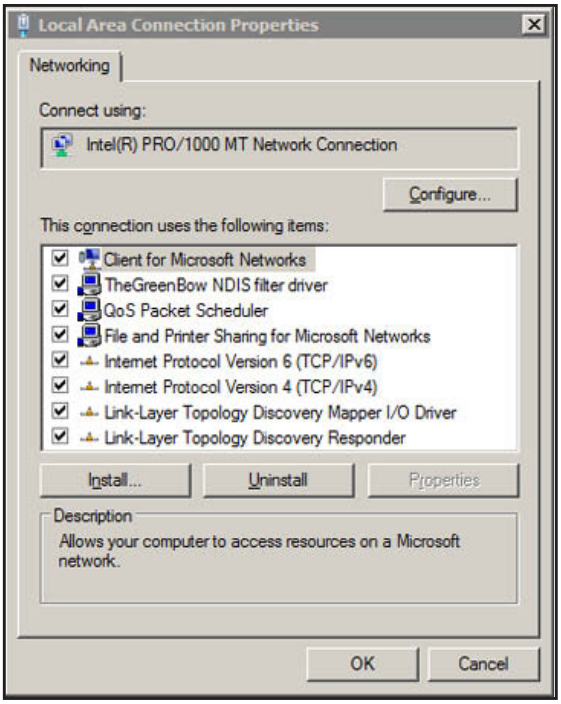

Figure 229.

  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 wireless 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 wireless VPN firewall.
  - **c.** Click or double-click **View status of this connection**. The Local Area Connection Status screen displays:

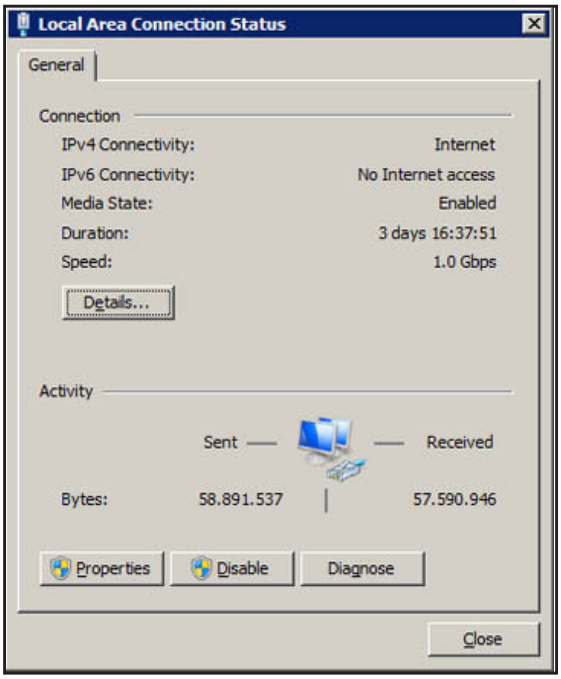

Figure 230.

  - **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:

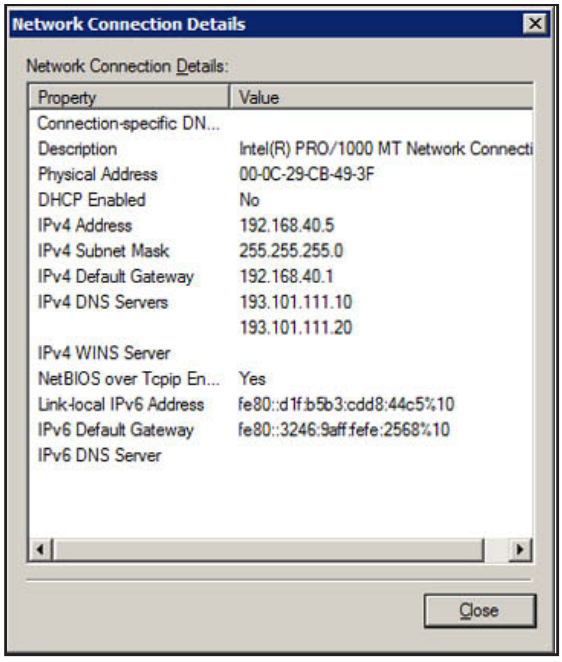

Figure 231.

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

- *Test the LAN Path to Your Wireless VPN Firewall*
- *Test the Path from Your Computer to a Remote Device*

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 Wireless VPN Firewall

You can ping the wireless VPN firewall from your computer to verify that the LAN path to the wireless VPN firewall is set up correctly.

➢ **To ping the wireless 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 wireless 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 383.
     - 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 wireless 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 wireless 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 wireless 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 the Broadband ISP Settings (IPv4) 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 32.

- 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 wireless 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 51.

Restore the Default Configuration and Password

➢ **To reset the wireless 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 wireless VPN firewall (see *Rear Panel* on page 18) and hold the button for about eight 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**:

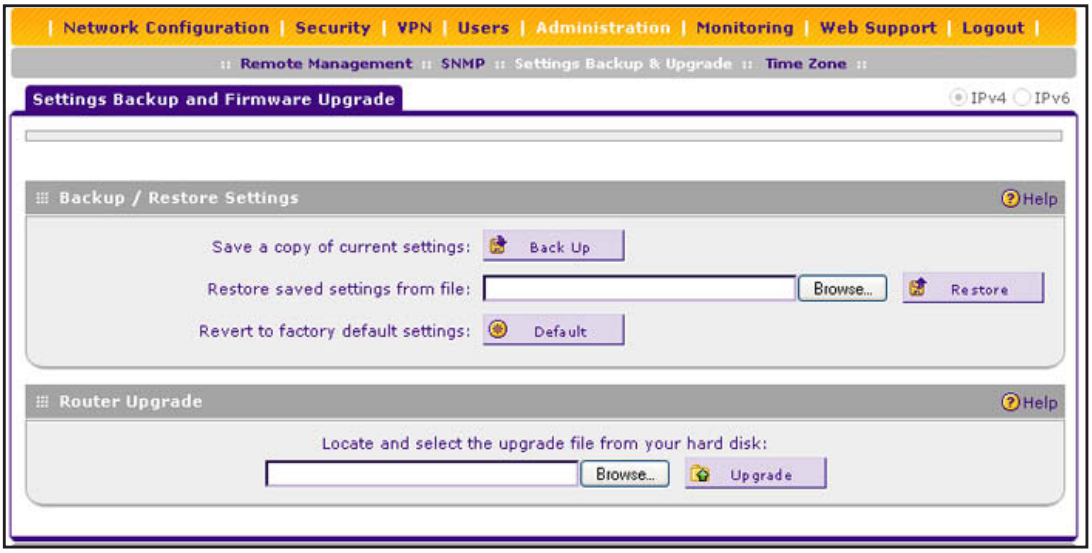

Figure 232.

  b. Click the **Default** button.

  The wireless 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 165 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 wireless 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 wireless 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 346). The wireless 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 wireless 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 wireless VPN firewall, wait at least five minutes, and check the date and time again.
- Time is off by one hour. Cause: The wireless 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 wireless VPN firewall:**

  Select **Web Support > Knowledgebase**.

- **To access NETGEAR's documentation library for your wireless 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 wireless 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 345):

- To perform a hard reset, press and hold the factory default Reset button for approximately eight seconds (until the Test LED blinks rapidly). The wireless 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 wireless VPN firewall to reboot.

The following table shows the default configuration settings for the wireless VPN firewall:

Table 93. Wireless 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	NAT
	WAN IPv6 mode	IPv4 only mode
	Stateless IP/ICMP Translation (SIIT)	Disabled
	WAN MAC address	Use default MAC address of the wireless VPN firewall
	WAN MTU size	1500 bytes 1492 bytes for PPPoE connections
	Port speed	AutoSense
	Dynamic DNS for IPv4	Disabled

Table 93. Wireless 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 8)	172.16.2.1
	DMZ IPv4 subnet mask (Port 8)	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 8)	176::1
	DMZ IPv6 prefix length (Port 8)	64
	DMZ DHCPv6 server	Disabled

Table 93. Wireless 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
	Jumbo frames	Disabled
	Session limits	Disabled
	TCP time-out	1800 seconds
	UDP time-out	120 seconds
	ICMP time-out	60 seconds
	SIP ALG	Disabled
	Source MAC filtering	Disabled
	IP/MAC bindings	Disabled
	Port triggering rules	None
	UPnP	Disabled
	Bandwidth profiles	None

Table 93. Wireless VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
	QoS profiles	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
Wireless radio and access point settings		
	Wireless radio	Enabled
	Region	Nonconfigurable: set for the region in which you purchased the wireless VPN firewall.
	Country	The selection is limited to the countries in the region in which you purchased the wireless VPN firewall. The default settings are: • Africa. Algeria • Asia. Azerbaijan • Europe. Albania • Middle East. Bahrain • North America, Latin America, and The Caribbean. United States • Oceania. Australia
	Operating frequency	Nonconfigurable: Set at 2.4 GHz
	Default security profile	default1
	Default network name (SSID)	FVS318N_1
	Broadcast SSID	Enabled
	Security	Open
	Encryption	None

Table 93. Wireless VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
	Authentication	None
	Transmission rate	Best[1]
	Default transmit power	Full
	802.11 wireless mode	802.11ng (for most countries)
	802.11b/g/n radio frequency channel	Auto
	802.11n channel spacing	20 MHz
	Beacon interval	100 ms
	DTIM interval	2
	RTS threshold	2346 bytes
	Fragmentation threshold	2346 bytes
	Preamble mode	Long
	Protection mode	None
	Power save	Disabled
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	Eight hours
VPN IPsec Wizard: VPN policy settings for IPv4 and IPv6 gateway-to-gateway tunnels		
	Encryption algorithm	3DES
	Authentication algorithm	SHA-1
	Life time	One hour
	Key group	DH-Group 2 (1024 bit)
	NetBIOS	Enabled

Table 93. Wireless 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	Eight hours
VPN IPsec Wizard: VPN policy settings for IPv4 gateway-to-client tunnels		
	Encryption algorithm	3DES
	Authentication algorithm	SHA-1
	Life time	One 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	Four
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 93. Wireless 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

1. The maximum wireless signal rate derived from IEEE Standard 802.11 specifications. The actual throughput varies. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Physical and Technical Specifications

The following table shows the physical and technical specifications for the wireless VPN firewall:

Table 94. Wireless 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 plug (localized to the country of sale)		
	North America	120V, 60 Hz, input
	United Kingdom, Australia	240V, 50 Hz, input
	Europe	230V, 50 Hz, input
	Input, for all regions	12VDC @ 1A output

Table 94. Wireless VPN firewall physical and technical specifications (continued)

Feature		Specification
Dimensions and weight		
	Dimensions (W x H x D)	19 x 12.5 x 3.5 cm (7.5 X 4.9 X 1.4 in)
	Weight	0.59 kg (1.3 lb)
Environmental specifications		
	Operating temperatures	0º to 40ºC
		32º to 104ºF
	Storage temperatures	–20º to 70ºC
		–4º to 158ºF
	Operating humidity	90% maximum relative humidity, noncondensing
	Storage humidity	95% maximum relative humidity, noncondensing
Electromagnetic emissions		
	Meets requirements of	FCC Part 15 Class B
		VCCI Class B
		EN 55 022 (CISPR 22), Class B
Wired compliance		
	See *Appendix C, Notification of Compliance (Wired)*.	
Wireless compliance		
	See *Appendix D, Notification of Compliance (Wireless)*.	
Interface specifications		
	LAN	Eight LAN autosensing 10/100/1000BASE-T, RJ-45, one of which is a configurable DMZ interface
	WAN	One WAN autosensing 10/100/1000BASE-T, RJ-45
	One administrative console port	RS-232

The following table shows the IPSec VPN specifications for the wireless VPN firewall:

Table 95. Wireless VPN firewall IPSec VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	12
IPSec authentication algorithm	SHA-1, MD5

Table 95. Wireless VPN firewall IPSec VPN specifications (continued)

Setting	Specification
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 wireless VPN firewall:

Table 96. Wireless VPN firewall SSL VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	Five
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

The following table shows the wireless specifications for the wireless VPN firewall:

Table 97. Wireless VPN firewall wireless specifications

Setting	Specification
802.11bg data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps, and auto-rate capable
802.11ng/n data rates	Data rates for a channel width of 20 MHz and a (short) guard interval of 400 ms: Best (automatic), 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps
	Data rates for a channel width of 40 MHz and a (short) guard interval of 400 ms: Best (automatic), 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps
802.11b/bg/ng/n operating frequencies	• 2.412–2.462 GHz (US) • 2.457–2.462 GHz (Spain) • 2.457–2.472 GHz (France) • 2.412–2.472 GHz (Europe ETSI)

Table 97. Wireless VPN firewall wireless specifications (continued)

Setting	Specification
802.11 b/bg/ng/n encryption	64-bits and 128-bits WEP, TKIP, CCMP data encryption
Network management	Web-based configuration and status monitoring

Two-Factor Authentication

B

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 six to eight digits in length.
- Something you are—for example, biometrics such as fingerprints or retinal prints.

This appendix focuses on and describes 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 two 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:

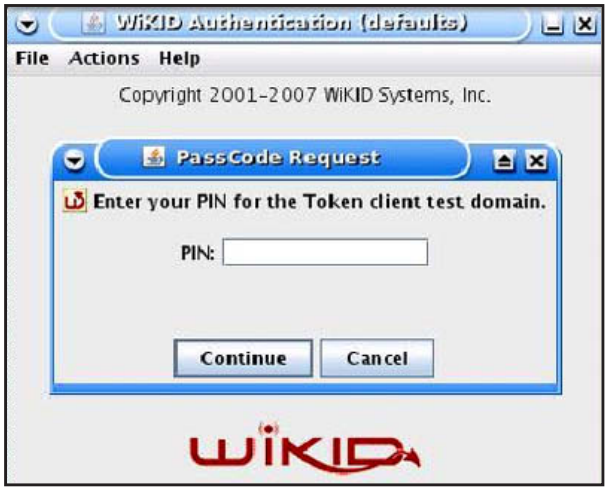

Figure 233.

2. A one-time passcode (*something the user has*) is generated.

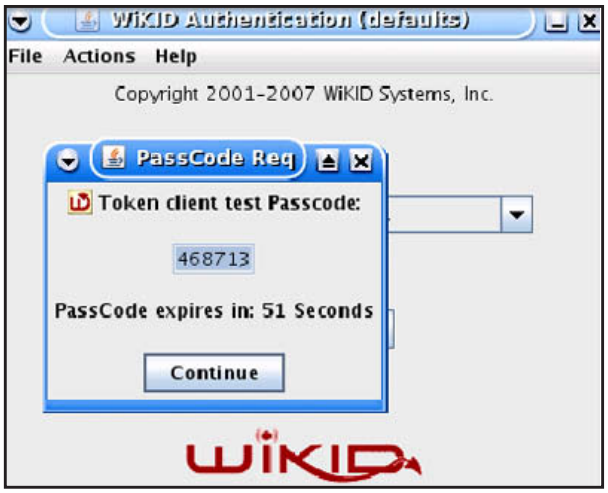

Figure 234.

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.

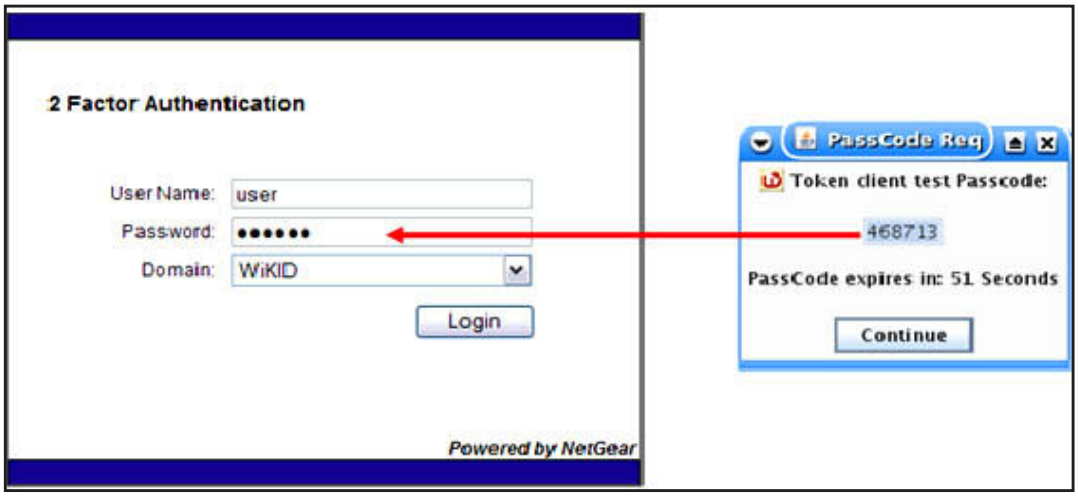

Figure 235.

Notification of Compliance (Wired)

C

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 Wireless-N 8-Port Gigabit VPN Firewall FVS318N 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.

Notification of Compliance (Wireless)

D

NETGEAR wireless routers, gateways, APs

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.

For indoor use only. Valid in all EU member states, EFTA states, and Switzerland.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSAFE Wireless-N 8-Port Gigabit VPN Firewall FVS318N complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Interference Reduction Table

The table below shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

X