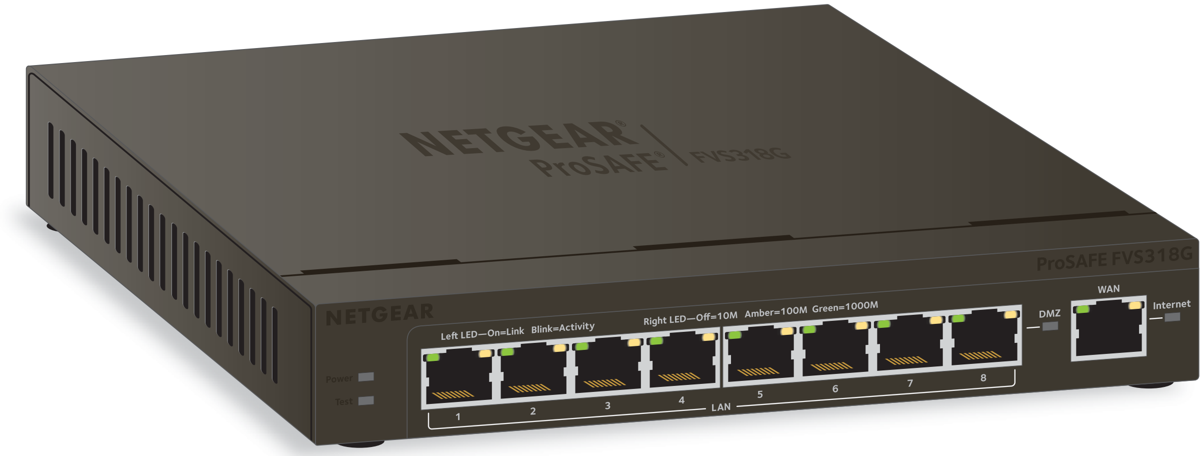
NETGEAR ProSAFE VPN Firewall FVS318G v2

Reference Manual



October 2014
202-11465-01

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*.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Trademarks

Revision History

Publication Part Number	Version	Publish Date	Comments
202-11465-01	1.0	October 2014	First publication

Contents

Chapter 1 Introduction

Chapter 2 IPv4 and IPv6 Internet and Broadband Settings

Chapter 3 LAN Configuration

Chapter 4 Firewall Protection

Chapter 5 Virtual Private Networking Using IPSec and L2TP Connections

Chapter 6 Manage Users, Authentication, and VPN Certificates

Chapter 7 Network and System Management

Chapter 8 Monitor System Access and Performance

Chapter 9 Troubleshooting

Appendix A Default Settings and Technical Specifications

Appendix B Two-Factor Authentication

Index

Introduction

1

This chapter provides an overview of the features and capabilities of the NETGEAR ProSAFE VPN Firewall FVS318G v2 and explains how to log in to the device and use its web management interface. The chapter contains the following sections:

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

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 does not match what is described in this guide, you might need to update your firmware.

What Is the NETGEAR ProSAFE VPN Firewall FVS318G v2?

The NETGEAR ProSAFE VPN Firewall FVS318G v2, hereafter referred to as the VPN firewall, connects your local area network (LAN) to the Internet through an external broadband access device such as a cable or DSL modem, satellite or wireless Internet dish, or another router.

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

The VPN firewall provides advanced IPSec VPN technologies with support for up to 12 IPSec 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 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
- Both IPv4 and IPv6 support
- Advanced IPSec VPN
- 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

This section contains the following topics:

Advanced VPN Support for IPSec

The VPN firewall supports IPSec 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. Advantages include:

- 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)

A Powerful, True Firewall

Unlike simple NAT routers, the VPN firewall is a true firewall, using stateful packet inspection (SPI) to defend against hacker attacks. Its firewall features provide 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 VPN firewall is equipped with several features designed to maintain security:

- **Computers hidden by NAT**. NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the computers on the LAN.
- **Port forwarding with NAT**. Although NAT prevents Internet locations from directly accessing the computers on the LAN, the VPN firewall allows you to direct incoming traffic to specific computers based on the service port number of the incoming request.
- **DMZ port**. Incoming traffic from the Internet is usually discarded by the VPN firewall unless the traffic is a response to one of your local computers or a service for which you 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 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 VPN firewall incorporates Auto Uplink™ technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should use a *normal* connection such as to a computer or an *uplink* connection such as to a switch or hub. That port then configures itself correctly. This feature eliminates the need for you to think about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

Extensive Protocol Support

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

- **IP address sharing by NAT**. The VPN firewall allows many networked computers to share an Internet account using only a single IP address, which might be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.
- **Automatic configuration of attached computers by DHCP**. The VPN firewall dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached computers on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of computers on your local network.
- **DNS proxy**. When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached computers. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE)**. PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection.
- **Quality of Service (QoS)**. The VPN firewall supports QoS.
- **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 VPN firewall within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**. Browser-based configuration allows you to easily configure the VPN firewall from almost any type of operating system, such as Windows, Macintosh, or Linux. Online help documentation is built into the browser-based web management interface.
- **Auto-detection of ISP**. The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **IPSec VPN Wizard**. The VPN firewall includes the NETGEAR IPSec VPN Wizard so that you can easily configure IPSec VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC). This ensures that the IPSec VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.

- **SNMP**. The VPN firewall supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.
- **Diagnostic functions**. The VPN firewall incorporates built-in diagnostic functions such as ping, traceroute, DNS lookup, and remote reboot.
- **Remote management**. The VPN firewall allows you to log in to the web management interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.
- **Visual monitoring**. The VPN firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

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

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

Package Contents

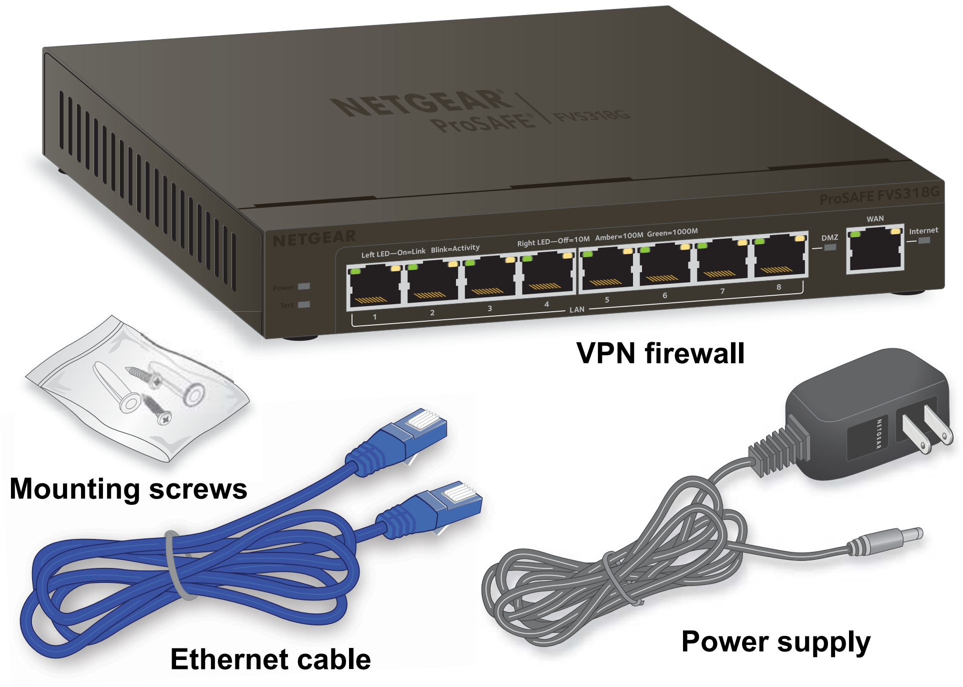


Figure 1. Package contents

The VPN firewall product package contains the following items:

- NETGEAR ProSAFE VPN Firewall FVS318G v2
- One 12V 1A power supply unit for your region
- Mounting screws
- Ethernet cable
- *NETGEAR ProSAFE VPN Firewall FVS318G v2 Installation Guide*

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer.

Hardware Features

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

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

Front Panel

Viewed from left to right, the 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.

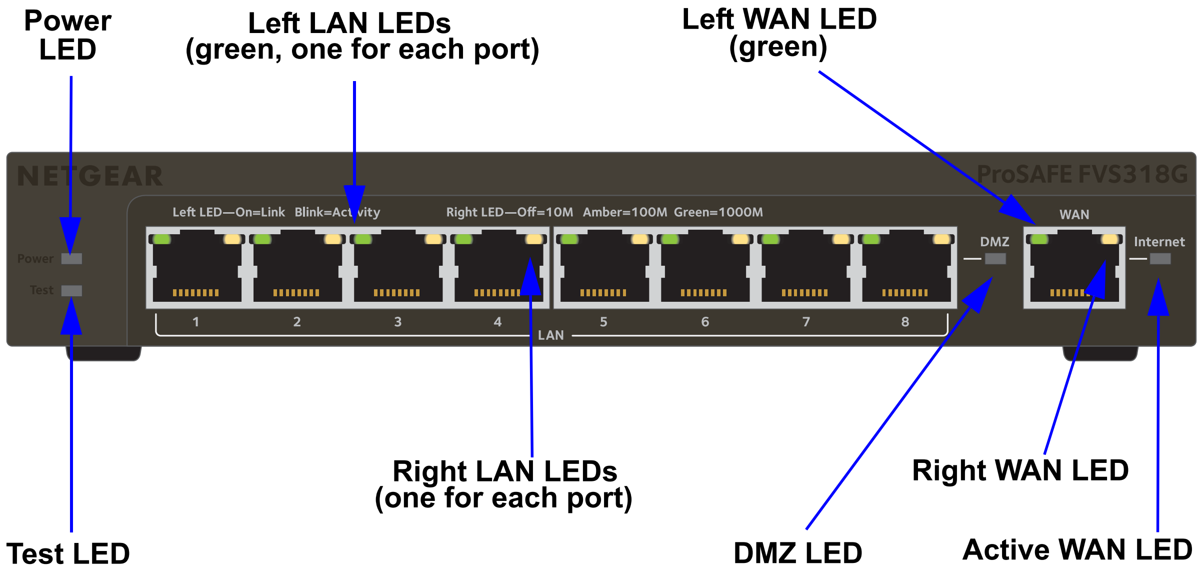

Power LED
Left LAN LEDs (green, one for each port)
Left WAN LED (green)
NETGEAR
ProSAFE FVS318G
Left LED—On=Link Blink=Activity
Right LED—Off=10M Amber=100M Green=1000M
WAN
DMZ
Internet
Power
Test
1
2
3
4
LAN
5
6
7
8
Right LAN LEDs (one for each port)
Right WAN LED
Test LED
DMZ LED
Active WAN LED

Figure 2. Front panel

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 VPN firewall.
	Off	Power is not supplied to the VPN firewall.
Test LED	On (amber) during startup	Test mode. The VPN firewall is initializing. After approximately two minutes, when the VPN firewall completes its initialization, the Test LED turns off.
	On (amber) during any other time	The initialization failed, or a hardware failure occurred.
	Blinking (amber)	The VPN firewall is writing to flash memory (during upgrading or resetting to defaults).
	Off	The VPN firewall booted successfully.

Table 1. LED descriptions (continued)

LED	Activity	Description
LAN Ports		
Left LED	Off	The LAN port does not detect a link.
	On (green)	The LAN port 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 does not detect a physical link, that is, no Ethernet cable is plugged into the VPN firewall.
	On (green)	The WAN port is connected with a device that provides an Internet connection.
	Blinking (green)	Data is being transmitted or received by the WAN port.
Right LED	Off	The WAN port is operating at 10 Mbps.
	On (amber)	The WAN port is operating at 100 Mbps.
	On (green)	The WAN port is operating at 1000 Mbps.
Active LED	Off	The firewall is not connected to the Internet.
	On (green)	The firewall is connected to the Internet.

Rear Panel

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

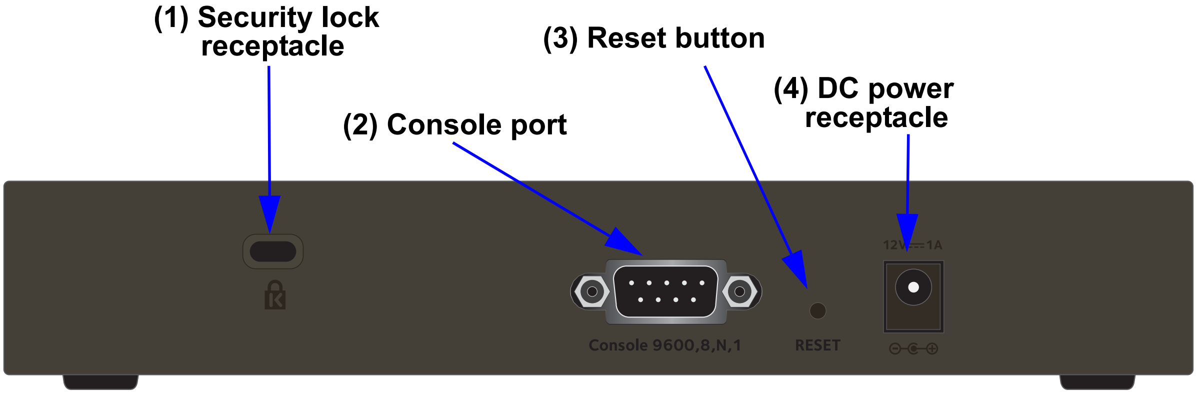


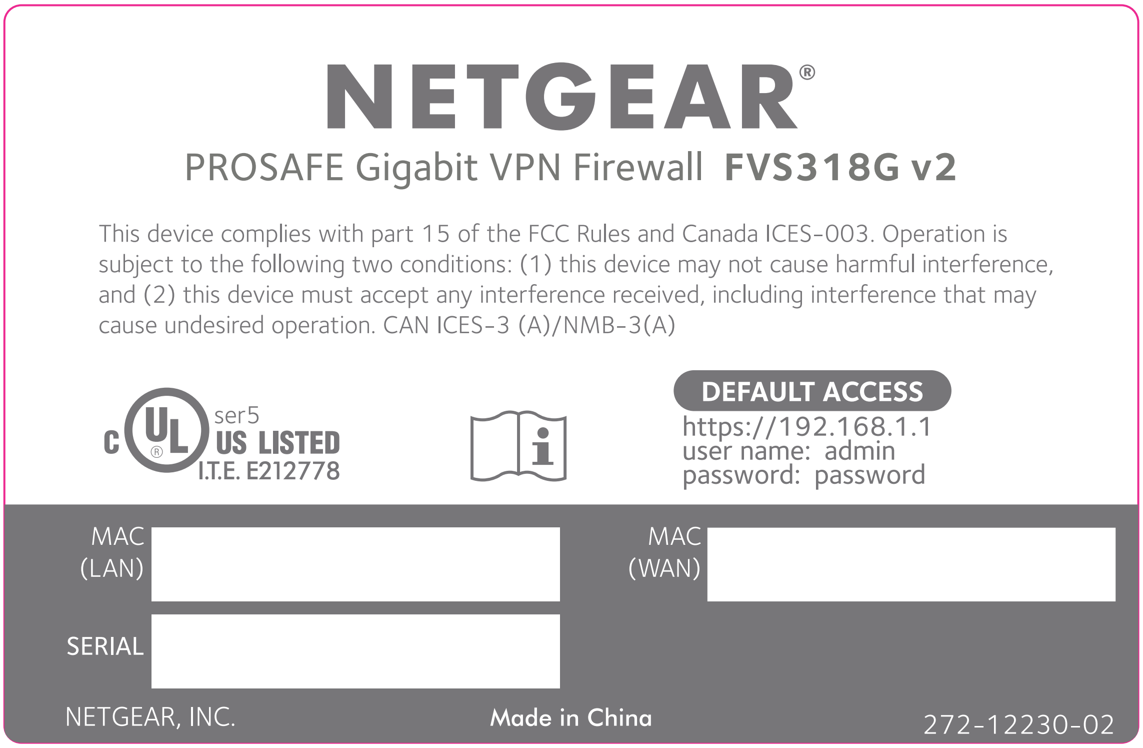
Figure 3. Back panel

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

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

Bottom Panel with Product Label

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



NETGEAR®

PROSAFE Gigabit VPN Firewall **FVS318G v2**

This device complies with part 15 of the FCC Rules and Canada ICES-003. 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. CAN ICES-3 (A)/NMB-3(A)

c UL ser5 US LISTED I.T.E. E212778

DEFAULT ACCESS
https://192.168.1.1
user name: admin
password: password

MAC (LAN)

MAC (WAN)

SERIAL

NETGEAR, INC. Made in China 272-12230-02

Figure 4. Product label

Choose a Location for the VPN Firewall

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

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

- The unit is accessible, and cables can be connected easily.
- Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air-conditioning units.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or 1 inch clearance.
- The air is as free of dust as possible.
- Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information about the recommended operating

temperatures for the VPN firewall, see *Appendix A, Default Settings and Technical Specifications*.

Wall-Mount the VPN Firewall with the Mounting Kit

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

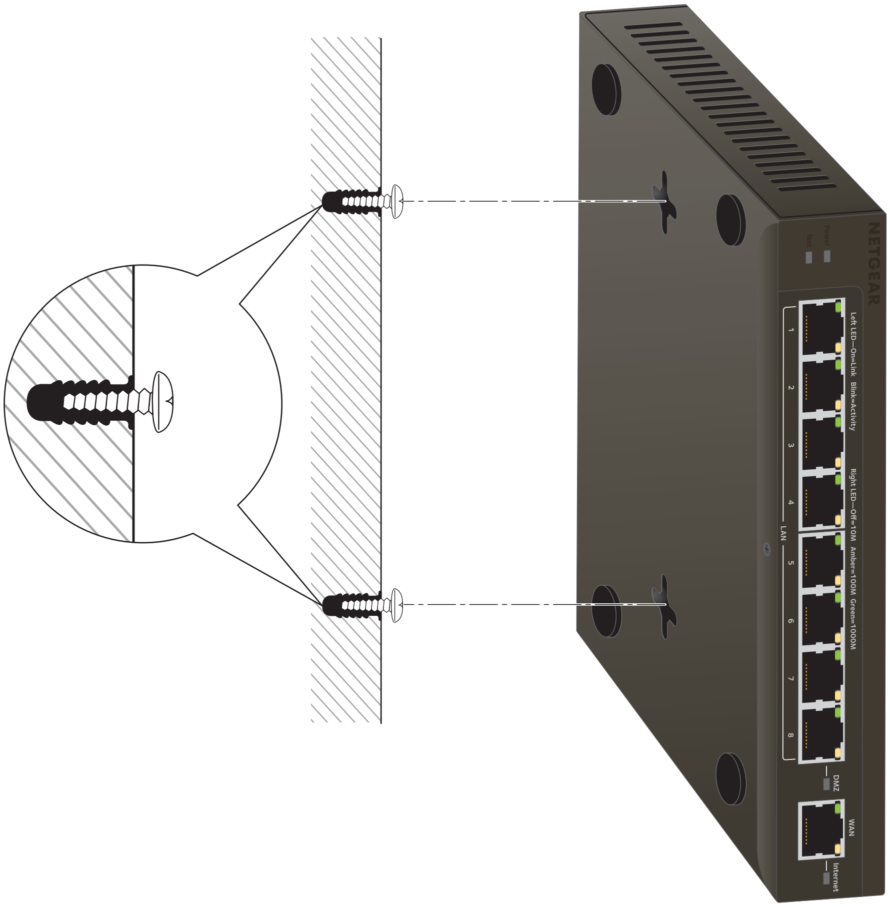

NETGEAR
Power
Test
Left LED—On=Link Blink=Activity
Right LED—Off=10M Amber=100M Green=1000M
1
2
3
4
LAN
5
6
7
8
DMZ
WAN
Internet

Figure 5. Wall mounting

Before mounting the VPN firewall to a wall, verify the following:

- You are using the correct screws (supplied with the installation kit).
- The wall on which you plan to mount the VPN firewall is suitably located.

Log In to the VPN Firewall

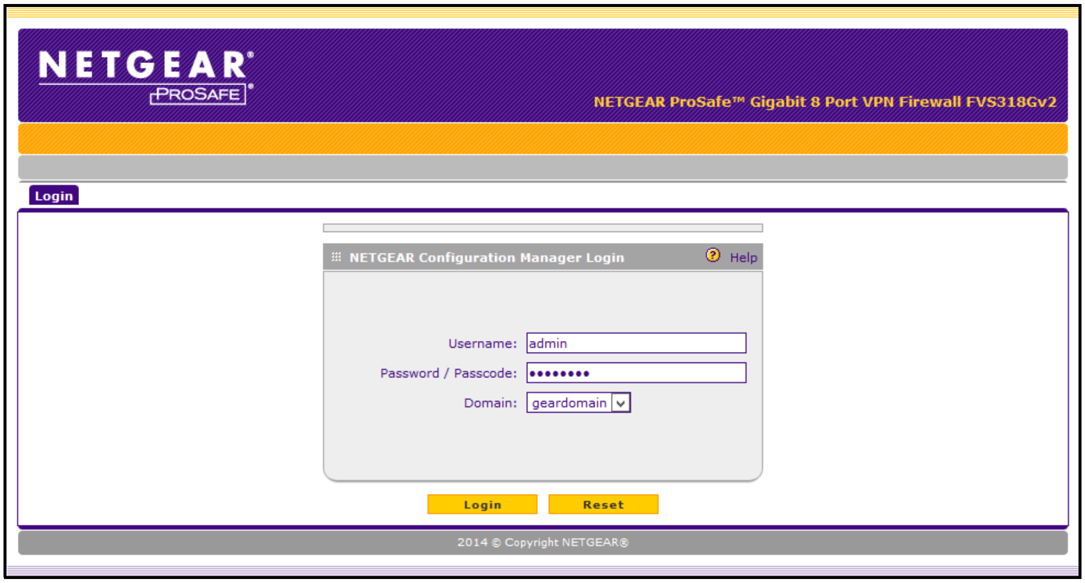
Note: To connect the VPN firewall physically to your network, connect the cables and restart your network according to the instructions in the *NETGEAR ProSAFE VPN Firewall FVS318G v2 Installation Guide*.

To configure the VPN firewall, you must 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.

➤ **To log in to the VPN firewall:**

1. Open any of the qualified web browsers.
2. In the address field, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.


NETGEAR
PROSAFE
NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318Gv2
Login
NETGEAR Configuration Manager Login
Help
Login
Reset
2014 © Copyright NETGEAR®

Username: admin
Password / Passcode: ••••••••
Domain: geardomain

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

3. In the **Username** field, enter **admin**.

   Use lowercase letters.

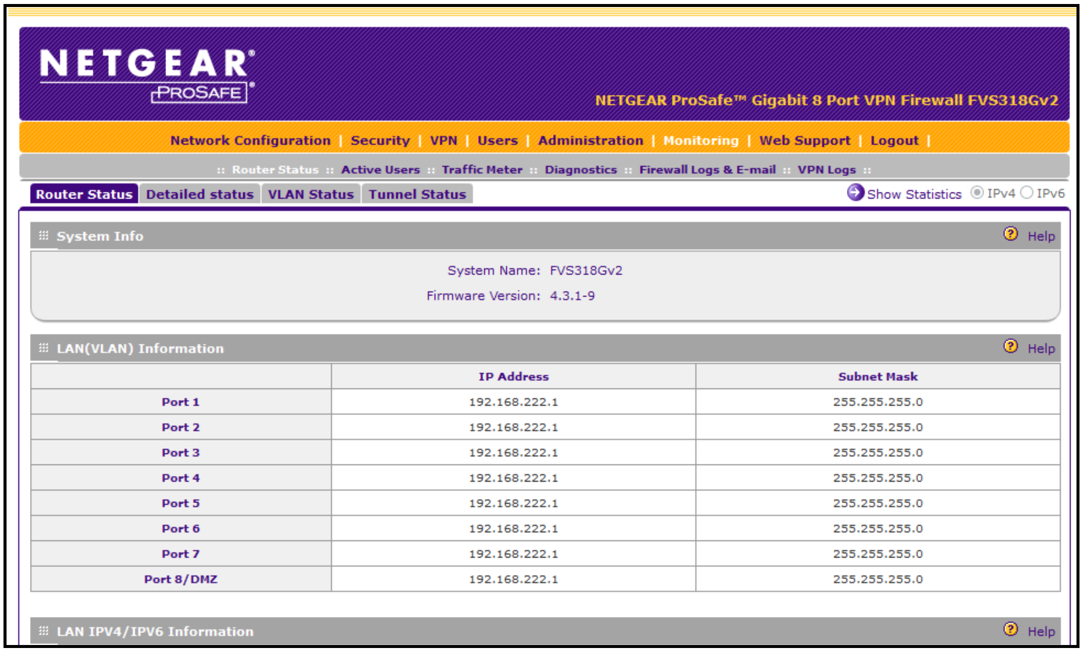
4. In the **Password / Passcode** field, enter **password**.

   Use lowercase letters.

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

Leave the domain as it is (geardomain).

5. Click the **Login** button.


NETGEAR PROSAFE
NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318Gv2
Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
VLAN Status
Tunnel Status
Show Statistics
● IPv4 ○ IPv6
System Info
Help
LAN(VLAN) Information
Help
LAN IPV4/IPV6 Information
Help

System Name: FVS318Gv2

Firmware Version: 4.3.1-9

	IP Address	Subnet Mask
Port 1	192.168.222.1	255.255.255.0
Port 2	192.168.222.1	255.255.255.0
Port 3	192.168.222.1	255.255.255.0
Port 4	192.168.222.1	255.255.255.0
Port 5	192.168.222.1	255.255.255.0
Port 6	192.168.222.1	255.255.255.0
Port 7	192.168.222.1	255.255.255.0
Port 8/DMZ	192.168.222.1	255.255.255.0

The figure shows the top part of the Router Status screen. For more information, see *View the System Status* on page 361.

After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

Web Management Interface Menu Layout

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

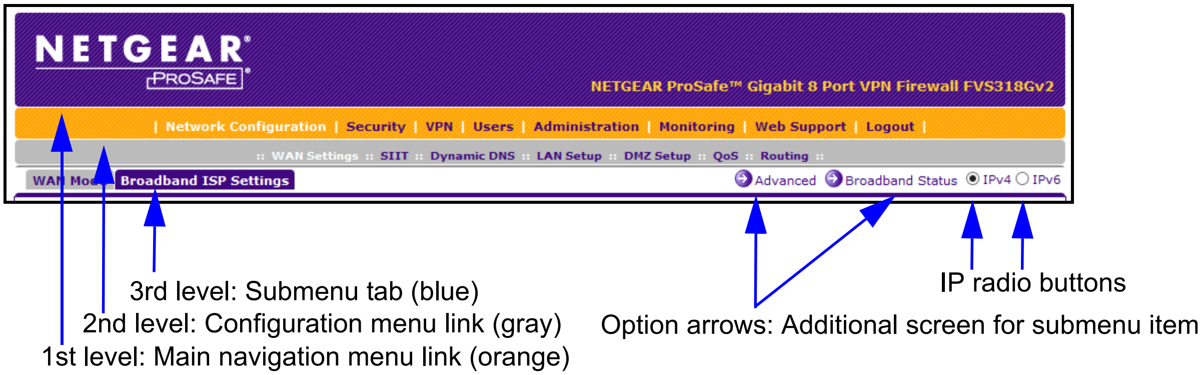

NETGEAR PROSAFE
NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318Gv2
| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
WAN Mode
Broadband ISP Settings
Advanced
Broadband Status
● IPv4 ○ IPv6
3rd level: Submenu tab (blue)
2nd level: Configuration menu link (gray)
1st level: Main navigation menu link (orange)
IP radio buttons
Option arrows: Additional screen for submenu item

Figure 6. Menu layout

The web management interface menu consists of the following components:

- **1st level: Main navigation menu links**. The main navigation menu in the orange bar across the top of the web management interface provides access to all the configuration functions of the VPN firewall and remains constant. When you select a main navigation menu link, the letters are displayed in white against an orange background.
- **2nd level: Configuration menu links**. The configuration menu links in the gray bar (immediately below the main navigation menu bar) change according to the main navigation menu link that you select. When you select a configuration menu link, the letters are displayed in white against a gray background.
- **3rd level: Submenu tabs**. Each configuration menu item includes 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 additional screens for the submenu item are available, 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. Four options are available:
  - **Both buttons are operational**. ● IPv4 ○ IPv6 You can configure the feature onscreen for IPv4 functionality or for IPv6 functionality. After you correctly configure 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**. ● IPv4 ○ IPv6 You can configure the feature onscreen for IPv4 functionality only.
  - **The IPv6 button is operational but the IPv4 button is disabled**. ○ IPv4 ● IPv6 You can configure the feature onscreen for IPv6 functionality only.
  - **Both buttons are disabled**. ● IPv4 ○ IPv6 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:

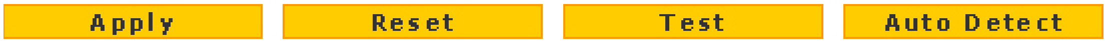


Figure 7. Action buttons

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

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

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

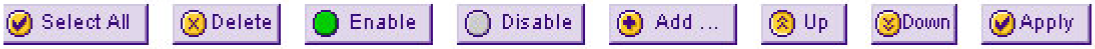


Figure 8. Table buttons

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 connect to an accompanying help screen. To open the help screen, click the ? (question mark) icon.

Requirements for Entering IP Addresses

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

IPv4 Addresses

The fourth octet of an IP address must 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 Addresses

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeros 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

IPv4 and IPv6 Internet and Broadband Settings

2

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

- *Internet and WAN Configuration Tasks*
- *Configure the IPv4 Internet Connection and WAN Settings*
- *Configure the IPv6 Internet Connection and WAN Settings*
- *Configure Advanced WAN Options and Other Tasks*
- *Additional WAN-Related Configuration Tasks*
- *What to Do Next*

Internet and WAN Configuration Tasks

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

IPv4 Internet Connections

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

➢ **To set up an IPv4 Internet connection:**

1. Configure the IPv4 WAN mode.

   Select either NAT or classical routing. This task is described in *Configure the IPv4 WAN Mode* on page 26.

2. Configure the IPv4 Internet connection to your ISP and connect to your ISP.

   Two configuration options are available. These tasks are described in the following sections:

   - *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 28
   - *Manually Configure an IPv4 Internet Connection* on page 31

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 35.

4. (Optional) Configure the WAN options.

   If necessary, change the factory default MTU size, port speed, and MAC address of the VPN firewall. These are advanced features, and you usually do not need to change the settings. This task is described in *Configure Advanced WAN Options and Other Tasks* on page 52.

5. (Optional) Configure the WAN traffic meter.

   This task is described in *Enable the WAN Traffic Meter* on page 349.

IPv6 Internet Connections

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

➢ **To set up an IPv6 Internet connection:**

1. Configure the IPv6 WAN mode.

Select the IPv4 / IPv6 mode to support both IPv4 and IPv6 traffic. For more information, see *Configure the IPv6 Routing Mode* on page 39.

2. Configure the IPv6 Internet connection to your ISP and connect to your ISP.

   Three configuration options are available. 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 were not assigned permanent IPv4 addresses to communicate with IPv4-only devices. For more information, see *Configure Stateless IP/ICMP Translation* on page 51.

5. (Optional) Configure the WAN options.

   If necessary, change the factory default MTU size, port speed, and MAC address of the VPN firewall. These are advanced features, and you usually do not need to change the settings. For more information, *Configure Advanced WAN Options and Other Tasks* on page 52.

Configure the IPv4 Internet Connection and WAN Settings

To set up your VPN firewall for secure IPv4 Internet connections, you must determine the IPv4 WAN mode and then configure the IPv4 Internet connection to your ISP on the WAN port.

The web management interface offers two connection configuration options, described in the following sections:

- *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 28
- *Manually Configure an IPv4 Internet Connection* on page 31

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. For more information, 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, only a single device (the VPN firewall) and a single IP address exist. Computers on your LAN can use any private IP address range, and these IP addresses are not visible from the Internet.

Note the following about NAT:

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

Classical Routing

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

If your ISP allocated a number of static IP addresses to you, and you 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.

You can view the status of the WAN ports on the Router Status screen (see *View the System Status* on page 361).

Configure the IPv4 Routing Mode

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

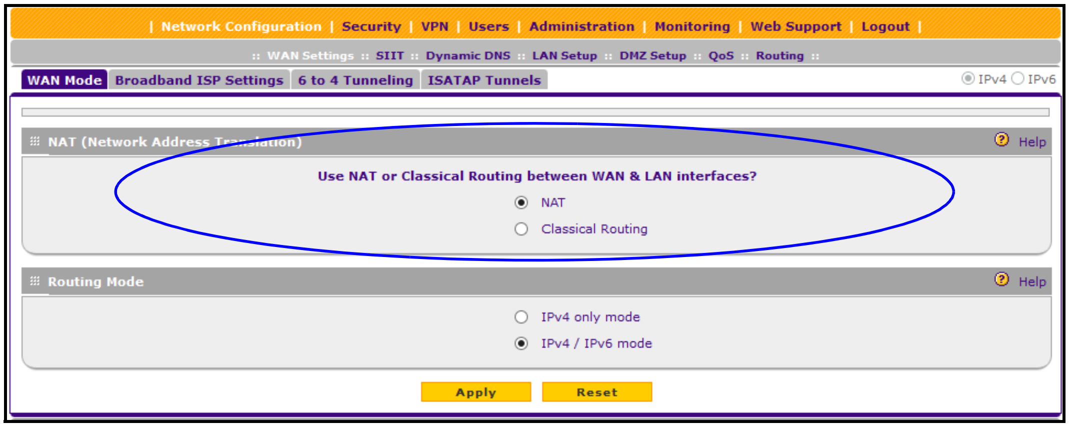
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
WAN Mode
Broadband ISP Settings
6 to 4 Tunneling
ISATAP Tunnels
● IPv4 ○ IPv6
Help
Help
Apply
Reset

NAT (Network Address Translation)

Use NAT or Classical Routing between WAN & LAN interfaces?

● NAT
○ Classical Routing

Routing Mode

○ IPv4 only mode
● IPv4 / IPv6 mode

3. 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.

4. Click the **Apply** button.

   Your settings are saved.

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

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

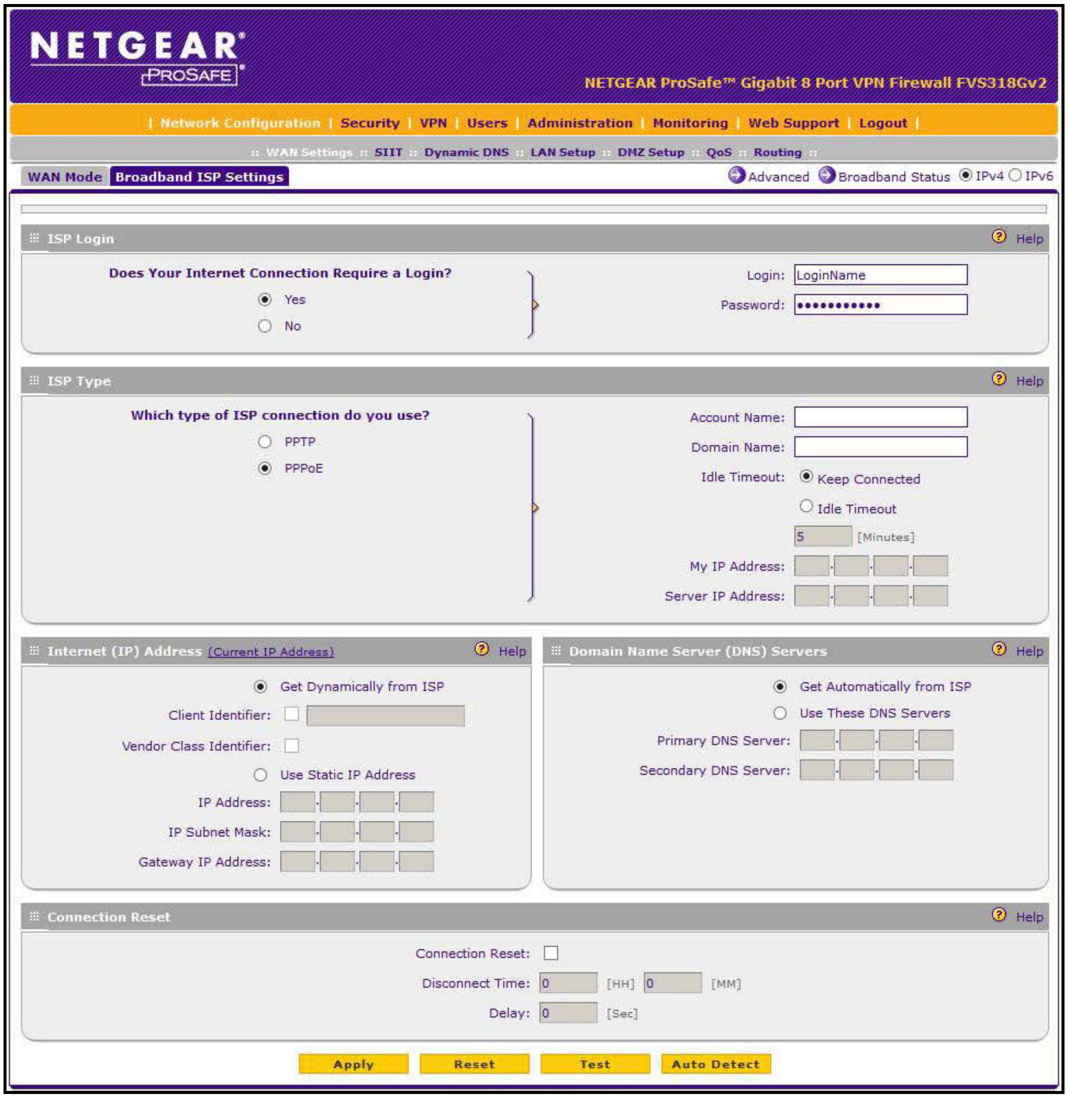
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > Broadband ISP Settings**.


NETGEAR PROSAFE
NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318Gv2
| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
WAN Mode
Broadband ISP Settings
Advanced
Broadband Status
Help
Apply
Reset
Test
Auto Detect

● IPv4 ○ IPv6

ISP Login

Does Your Internet Connection Require a Login?

● Yes

○ No

Login: LoginName

Password: •••••••••••

ISP Type

Which type of ISP connection do you use?

○ PPTP

● PPPoE

Account Name:

Domain Name:

Idle Timeout: ● Keep Connected

○ Idle Timeout

5 [Minutes]

My IP Address:

Server IP Address:

Internet (IP) Address (Current IP Address)

● Get Dynamically from ISP

Client Identifier: □

Vendor Class Identifier: □

○ Use Static IP Address

IP Address:

IP Subnet Mask:

Gateway IP Address:

Domain Name Server (DNS) Servers

● Get Automatically from ISP

○ Use These DNS Servers

Primary DNS Server:

Secondary DNS Server:

Connection Reset

Connection Reset: □

Disconnect Time: 0 [HH] 0 [MM]

Delay: 0 [Sec]

In the upper right of the screen, the **IPv4** radio button is selected by default. The ISP Broadband Settings screen displays the IPv4 settings.

3. Click the **Auto Detect** button at the bottom of the screen.

The autodetect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support.

The autodetect process returns one of the following results:

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

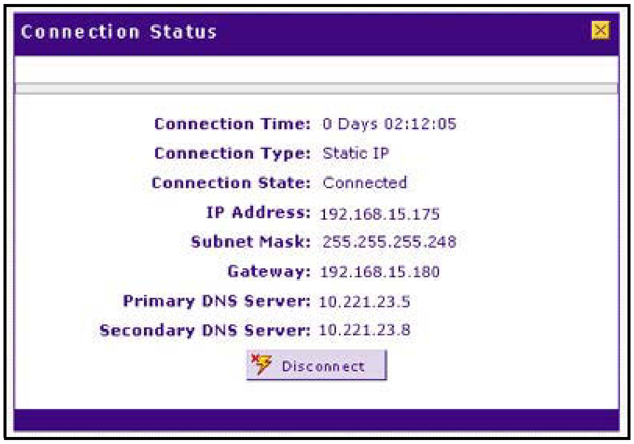
- If the autodetect process senses a connection method that requires input from you, it prompts you for the information. The following table explains the settings that you might need to enter:

Table 2. IPv4 Internet connection methods

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

- If the autodetect process does not find a connection, you are prompted either to check the physical connection between your VPN firewall and the cable, DSL line, or satellite or wireless Internet dish, or to check your VPN firewall's MAC address. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 52 and *Troubleshoot the ISP Connection* on page 389.

4. To verify the connection, click the **Broadband Status** option arrow.



Connection Time: 0 Days 02:12:05
Connection Type: Static IP
Connection State: Connected
IP Address: 192.168.15.175
Subnet Mask: 255.255.255.248
Gateway: 192.168.15.180
Primary DNS Server: 10.221.23.5
Secondary DNS Server: 10.221.23.8

The Connection Status screen shows 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 31, or see *Troubleshoot the ISP Connection* on page 389.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 373.

Manually Configure an IPv4 Internet Connection

Unless your ISP automatically assigns your configuration through a DHCP server, you must 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 30.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

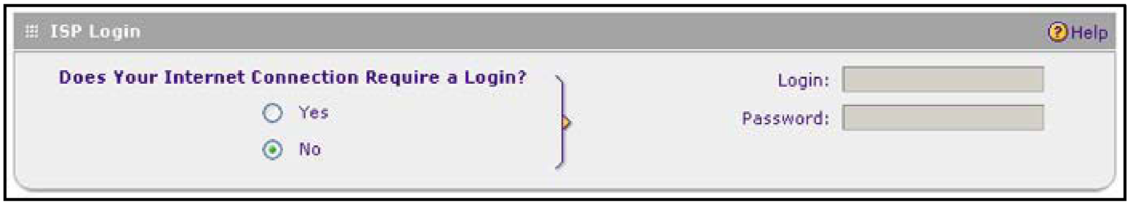
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. 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.

3. Locate the ISP Login section.



ISP Login

Help

Does Your Internet Connection Require a Login?

○ Yes

● No

Login:

Password:

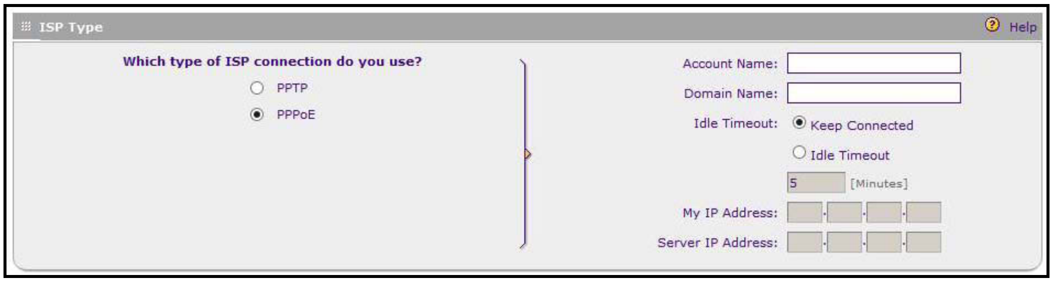
4. Select one of the following options:

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

5. If you selected the **Yes** radio button, enter the login name in the **Login** field and the password in the **Password** field.

   This information is provided by your ISP.

6. In the ISP Type section, select the type of ISP connection that you use from the two listed options.



ISP Type

Which type of ISP connection do you use?

○ PPTP

● PPPoE

Account Name:

Domain Name:

Idle Timeout: ● Keep Connected ○ Idle Timeout

5 [Minutes]

My IP Address:

Server IP Address:

7. 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

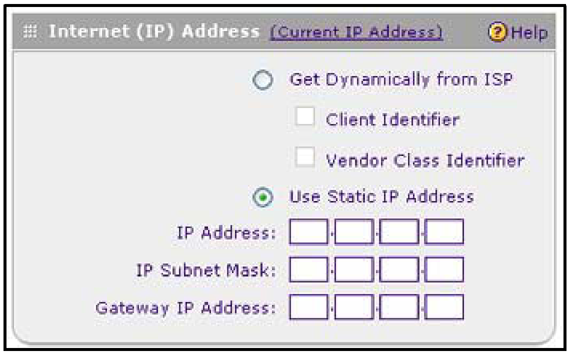
Setting	Description	
PPTP **Note:** For login and password information, see *Step 3* and *Step 5*.	If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this radio button, and enter the following settings:	
	Account Name	The account name is also known as the host name or system 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 are logged in.
	My IP Address	The IP address assigned by the ISP to make the connection with the ISP server.
	Server IP Address	The IP address of the PPTP server.

Table 3. PPTP and PPPoE settings (continued)

Setting	Description		
Other (PPPoE) **Note:** For login and password information, see *Step 3* and *Step 5*.	If you 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 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 are 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 is reestablished.

8. In the Internet (IP) Address section of the screen, configure the IP address settings as described in the following table.

   See the following figure. Click the **Current IP Address** link to see the assigned IP address.



Internet (IP) Address (Current IP Address) ? Help

○ Get Dynamically from ISP

□ Client Identifier

□ Vendor Class Identifier

● Use Static IP Address

IP Address: □.□.□.□

IP Subnet Mask: □.□.□.□

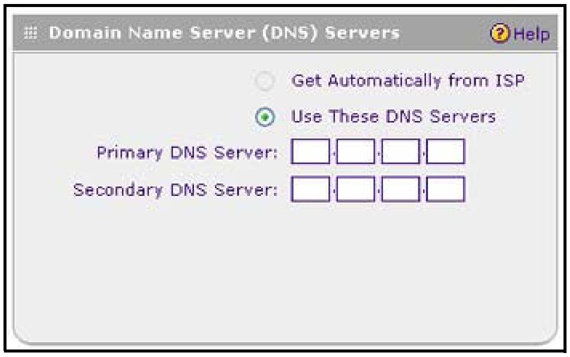
Gateway IP Address: □.□.□.□

Table 4. Internet IP address settings

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

9. In the Domain Name Server (DNS) Servers section, specify the DNS settings as described in the following table.

   See the following figure.



Domain Name Server (DNS) Servers

○ Get Automatically from ISP

● Use These DNS Servers

Primary DNS Server: □.□.□.□

Secondary DNS Server: □.□.□.□

Table 5. DNS server settings

Setting	Description
Get Automatically from ISP	If your ISP did not assign any Domain Name Server (DNS) addresses, select the **Get Automatically from ISP** radio button.

Table 5. DNS server settings (continued)

Setting	Description	
Use These DNS Servers	If your ISP 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.

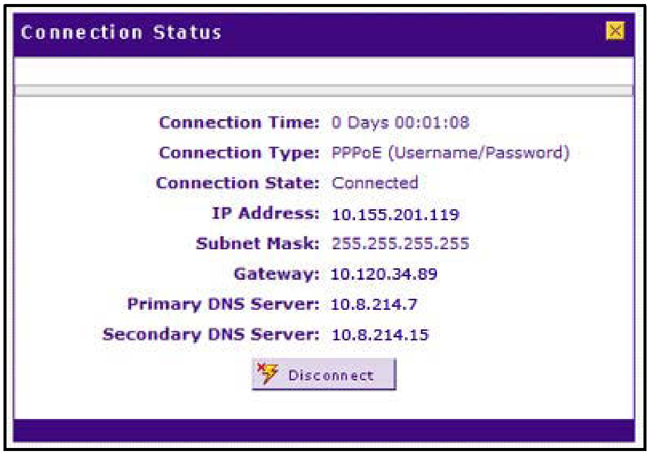
10. Click the **Apply** button.

    Your settings are saved.

11. To evaluate your entries, click the **Test** button.

    The VPN firewall attempts to make a connection according to the settings that you entered.

12. To verify the connection, click the **Broadband Status** option arrow.



Connection Time: 0 Days 00:01:08
Connection Type: PPPoE (Username/Password)
Connection State: Connected
IP Address: 10.155.201.119
Subnet Mask: 255.255.255.255
Gateway: 10.120.34.89
Primary DNS Server: 10.8.214.7
Secondary DNS Server: 10.8.214.15

If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must enter that address on the Broadband Advanced Options screen for the WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 52).

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 must set up an account with a DDNS provider such as Dyn, TZO, Oray, or 3322. (Links to Dyn, TZO, Oray, and 3322 are provided for your convenience as option arrows on the DDNS configuration screens.) The VPN firewall firmware includes software that notifies DDNS servers of changes in the WAN IP address so that the services running on this network can be accessed by others on the Internet.

If your network uses a permanently assigned IP address, you can register a domain name and link that name with your IP address using 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 configure your account information on the VPN firewall, when your ISP-assigned IP address changes, your VPN firewall automatically contacts your DDNS service provider, logs in to your account, and registers your new IP address.

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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

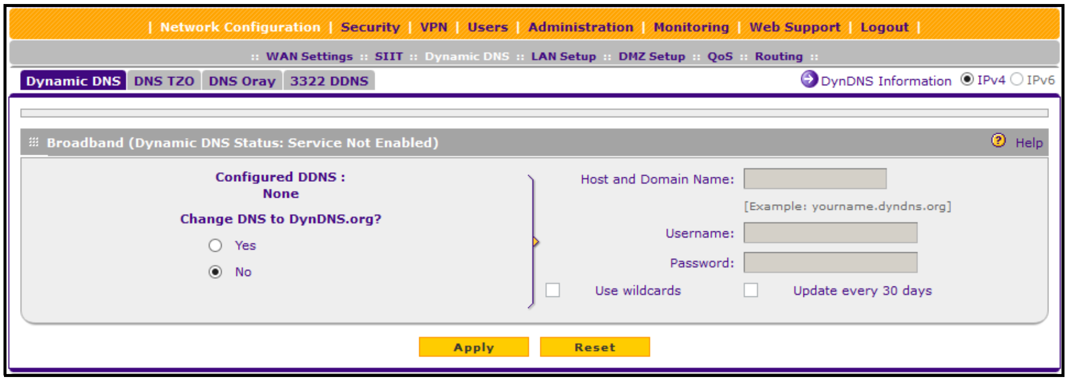
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > Dynamic DNS**.

   The Dynamic DNS screen displays.

3. Click the submenu tab for your DDNS service provider:
   - **Dynamic DNS** for Dyn (which is shown in the following figure)
   - **DNS TZO** for TZO
   - **DNS Oray** for Oray
   - **3322 DDNS** for 3322


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Dynamic DNS
DNS TZO
DNS Oray
3322 DDNS
DynDNS Information
Help
Apply
Reset

● IPv4 ○ IPv6

Broadband (Dynamic DNS Status: Service Not Enabled)

Configured DDNS :
None

Change DNS to DynDNS.org?

○ Yes

● No

Host and Domain Name:

[Example: yourname.dyndns.org]

Username:

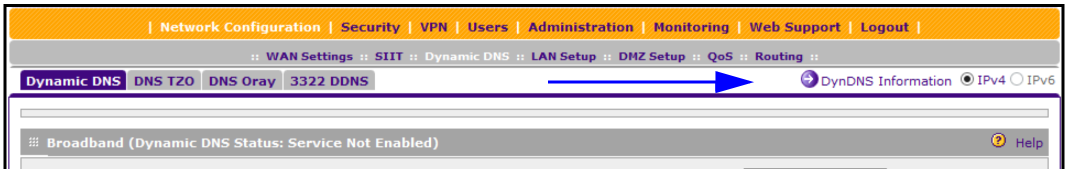
Password:

□ Use wildcards

□ Update every 30 days

4. For registration information, click the **Information** option arrow in the upper right of a DNS screen.

   For example, DynDNS Information.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Dynamic DNS
DNS TZO
DNS Oray
3322 DDNS
DynDNS Information
Help

● IPv4 ○ IPv6

Broadband (Dynamic DNS Status: Service Not Enabled)

5. Access the website of the DDNS service provider, and register for an account.

   For example, for Dyn, visit *http://dyn.com/dns/*.

6. 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 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.dyn.com/dns to be aliased to the same IP address as yourhost.dyn.com/dns.
	Update every 30 days	If your WAN IP address does not often change, you must 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.

7. Click the **Apply** button.

Your configuration is saved.

Configure the IPv6 Internet Connection and WAN Settings

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

- **Native IPv6 network**. Your network is a native IPv6 network if the VPN firewall uses an IPv6 address and is connected to an IPv6 ISP and if your network consists of IPv6-only devices.
- **Isolated IPv6 network**. If your network is an isolated IPv6 network that is not connected to an IPv6 ISP, you must 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 must 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).

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

After you configure the IPv6 routing mode, you must configure the WAN port with a global unicast address to enable secure IPv6 Internet connections on your VPN firewall. A global unicast address is a public and routable IPv6 WAN address that can be statically or dynamically assigned. The web management interface offers two connection configuration options:

- Automatic configuration of the network connection (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 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)

This section contains the following topics:

- *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*

Configure the IPv6 Routing Mode

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

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

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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

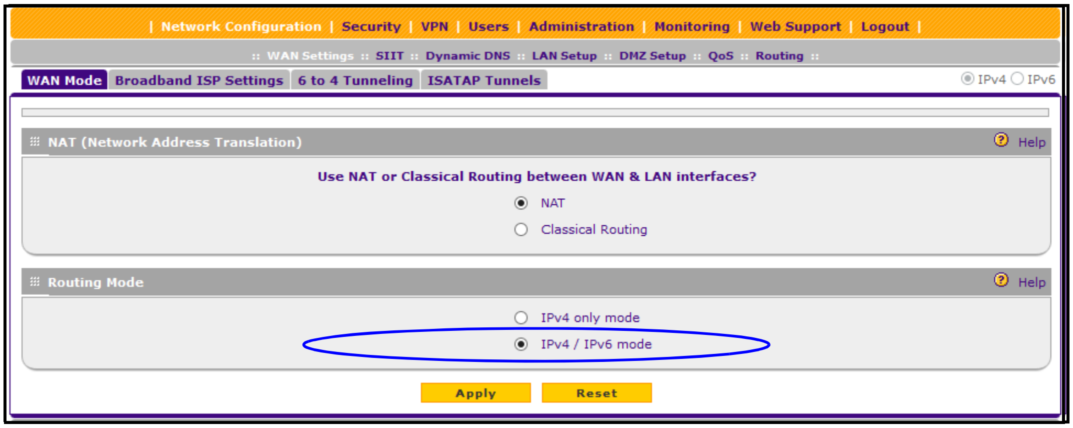
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
WAN Mode
Broadband ISP Settings
6 to 4 Tunneling
ISATAP Tunnels
● IPv4 ○ IPv6
Help
Help
Apply
Reset

NAT (Network Address Translation)

Use NAT or Classical Routing between WAN & LAN interfaces?

● NAT

○ Classical Routing

Routing Mode

○ IPv4 only mode

● IPv4 / IPv6 mode

3. Select the **IPv4 / IPv6 mode** radio button.

   By default, the **IPv4 only mode** radio button is selected, and IPv6 is disabled.

WARNING:

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

4. Click the **Apply** button.

   Your settings are saved.

Use a DHCPv6 Server to Configure an IPv6 Internet Connection

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

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

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

  As an option for stateless address autoconfiguration, the ISP's *stateful* DHCPv6 server can assign a prefix through prefix delegation. The VPN firewall's own *stateless* DHCPv6 server can assign this prefix to its IPv6 LAN clients. For more information about prefix delegation, see *Stateless DHCPv6 Server with Prefix Delegation* on page 79.

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

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

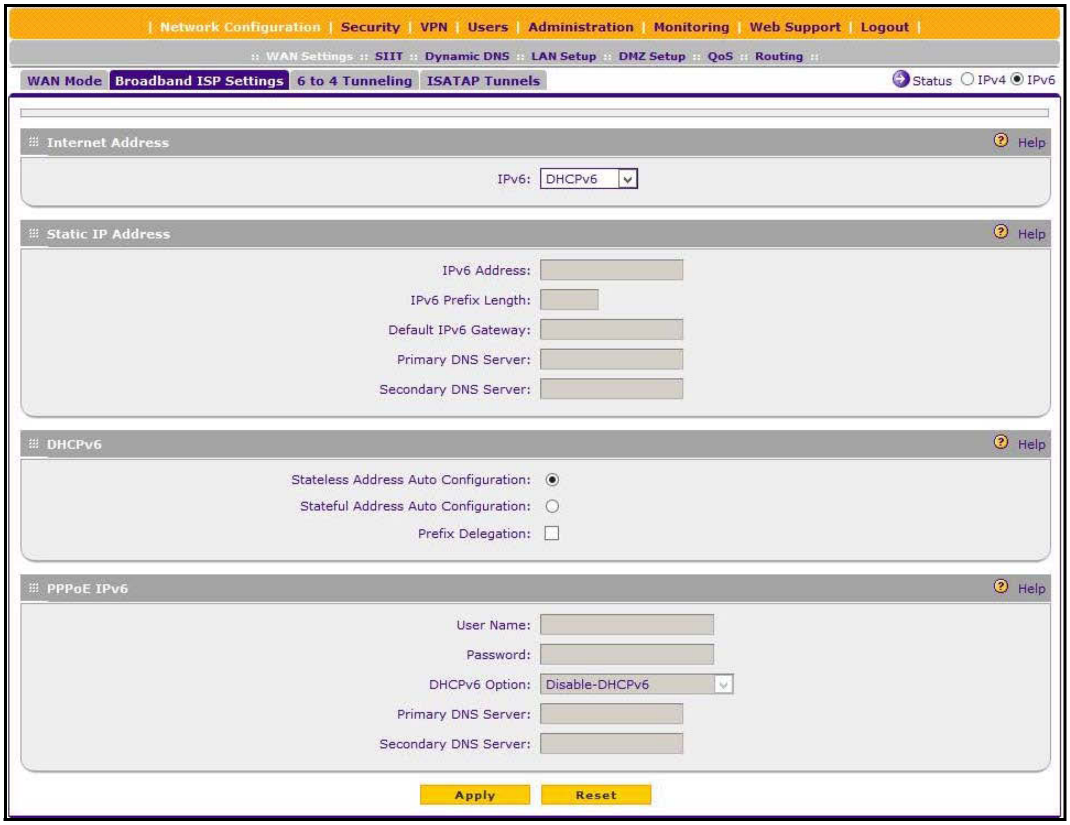
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > Broadband ISP Settings**.

   The Broadband ISP Settings screen displays.

3. Select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
WAN Mode
Broadband ISP Settings
6 to 4 Tunneling
ISATAP Tunnels
Status
Help
Apply
Reset

○ IPv4 ● IPv6

Internet Address

IPv6: DHCPv6

Static IP Address

IPv6 Address:

IPv6 Prefix Length:

Default IPv6 Gateway:

Primary DNS Server:

Secondary DNS Server:

DHCPv6

Stateless Address Auto Configuration: ●

Stateful Address Auto Configuration: ○

Prefix Delegation: □

PPPoE IPv6

User Name:

Password:

DHCPv6 Option: Disable-DHCPv6

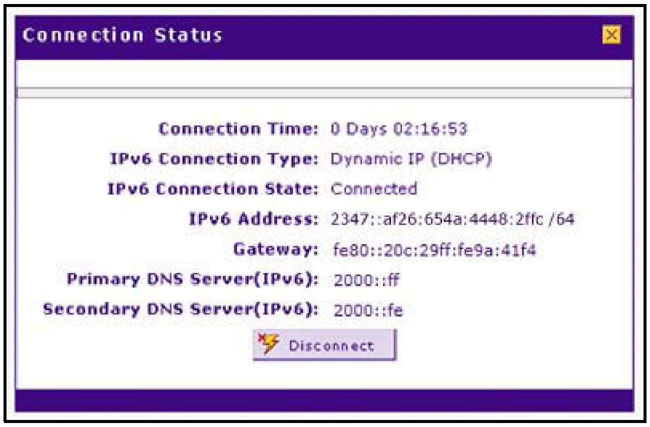
Primary DNS Server:

Secondary DNS Server:

4. In the Internet Address section, from the **IPv6** list, select **DHCPv6**.
5. In the DHCPv6 section, select a configuration option:
   - **Stateless Address Auto Configuration**
   - **Stateful Address Auto Configuration**
6. (Optional) If you m selected the **Stateless Address Auto Configuration** radio button, you can select the **Prefix Delegation** check box:
   - **Prefix delegation check box is selected**. A prefix is assigned by the ISP's *stateful* DHCPv6 server through prefix delegation, for example, 2001:db8:: /64. The VPN firewall's own *stateless* DHCPv6 server can assign this prefix to its IPv6 LAN clients. For more information about prefix delegation, see *Stateless DHCPv6 Server with Prefix Delegation* on page 79.
   - **Prefix delegation check box is cleared**. Prefix delegation is disabled. This is the default setting.
7. Click the **Apply** button.

   Your changes are saved.

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



Connection Status

Connection Time: 0 Days 02:16:53
IPv6 Connection Type: Dynamic IP (DHCP)
IPv6 Connection State: Connected
IPv6 Address: 2347::af26:654a:4448:2ffc /64
Gateway: fe80::20c:29ff:fe9a:41f4
Primary DNS Server(IPv6): 2000::ff
Secondary DNS Server(IPv6): 2000::fe

The Connection Status screen shows 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 389.

For more information about the Connection Status screen, see *View the WAN Port Status* on page 373.

Configure a Static IPv6 Internet Connection

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

➤ **To configure static IPv6 broadband ISP settings:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

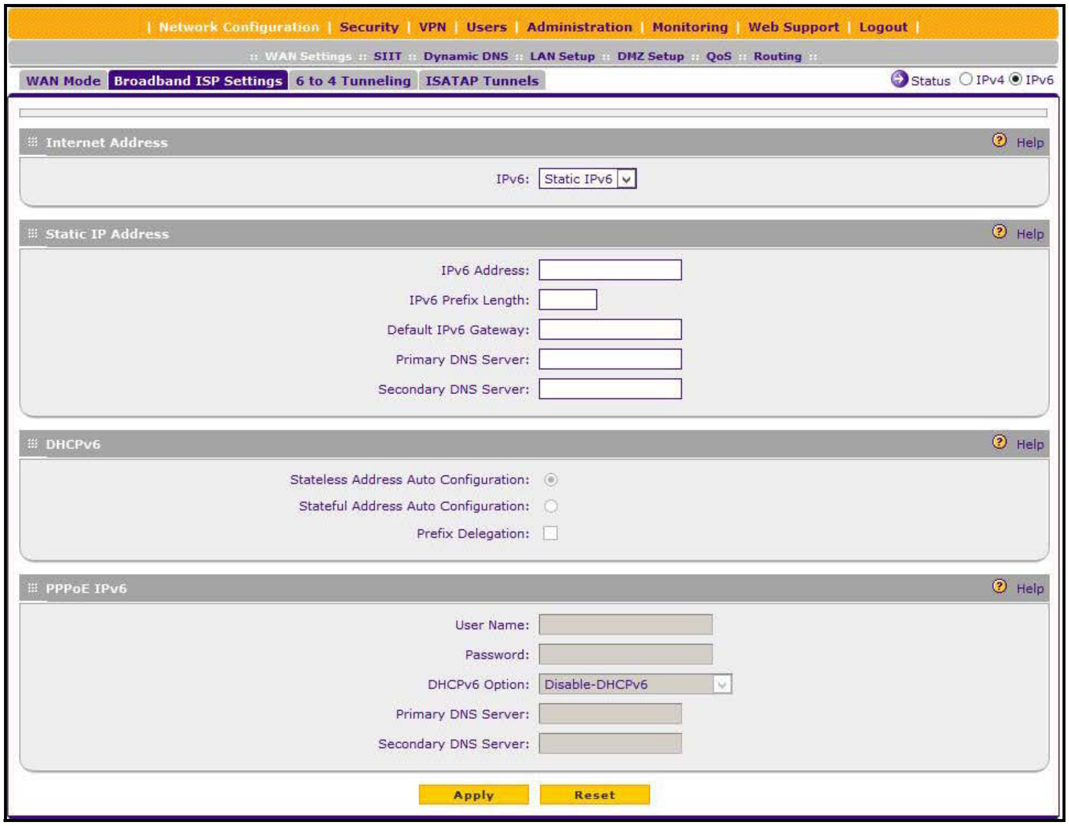
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > Broadband ISP Settings**.

   The Broadband ISP Settings screen displays.

3. Select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
WAN Mode
Broadband ISP Settings
6 to 4 Tunneling
ISATAP Tunnels
Status ○ IPv4 ● IPv6
Help
Apply
Reset

Internet Address

IPv6: Static IPv6

Static IP Address

IPv6 Address:

IPv6 Prefix Length:

Default IPv6 Gateway:

Primary DNS Server:

Secondary DNS Server:

DHCPv6

Stateless Address Auto Configuration: ●

Stateful Address Auto Configuration: ○

Prefix Delegation: □

PPPoE IPv6

User Name:

Password:

DHCPv6 Option: Disable-DHCPv6

Primary DNS Server:

Secondary DNS Server:

4. In the Internet Address section, from the **IPv6** list, select **Static IPv6**.
5. In the Static IP Address section, enter the settings as described in the following table.

   Your IPv6 ISP gave you your static IPv6 information.

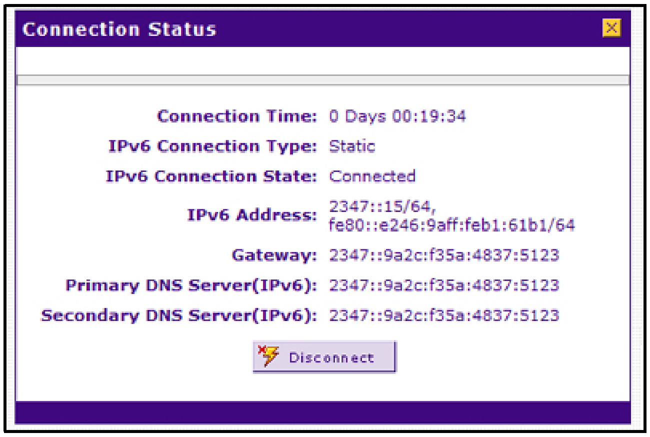
Table 7. Broadband ISP Settings screen settings for a static IPv6 address

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.

6. Click the **Apply** button.

   Your changes are saved.

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



Connection Status

Connection Time: 0 Days 00:19:34
IPv6 Connection Type: Static
IPv6 Connection State: Connected
IPv6 Address: 2347::15/64, fe80::e246:9aff:feb1:61b1/64
Gateway: 2347::9a2c:f35a:4837:5123
Primary DNS Server(IPv6): 2347::9a2c:f35a:4837:5123
Secondary DNS Server(IPv6): 2347::9a2c:f35a:4837:5123

The Connection Status screen shows 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 389.

For more information about the Connection Status screen, see *View the WAN Port Status* on page 373.

If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must enter that address on the Broadband Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 52).

Configure a PPPoE IPv6 Internet Connection

To configure a PPPoE IPv6 Internet connection, you must enter the PPPoE IPv6 information that you received from your ISP.

➢ **To configure PPPoE IPv6 broadband ISP settings:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

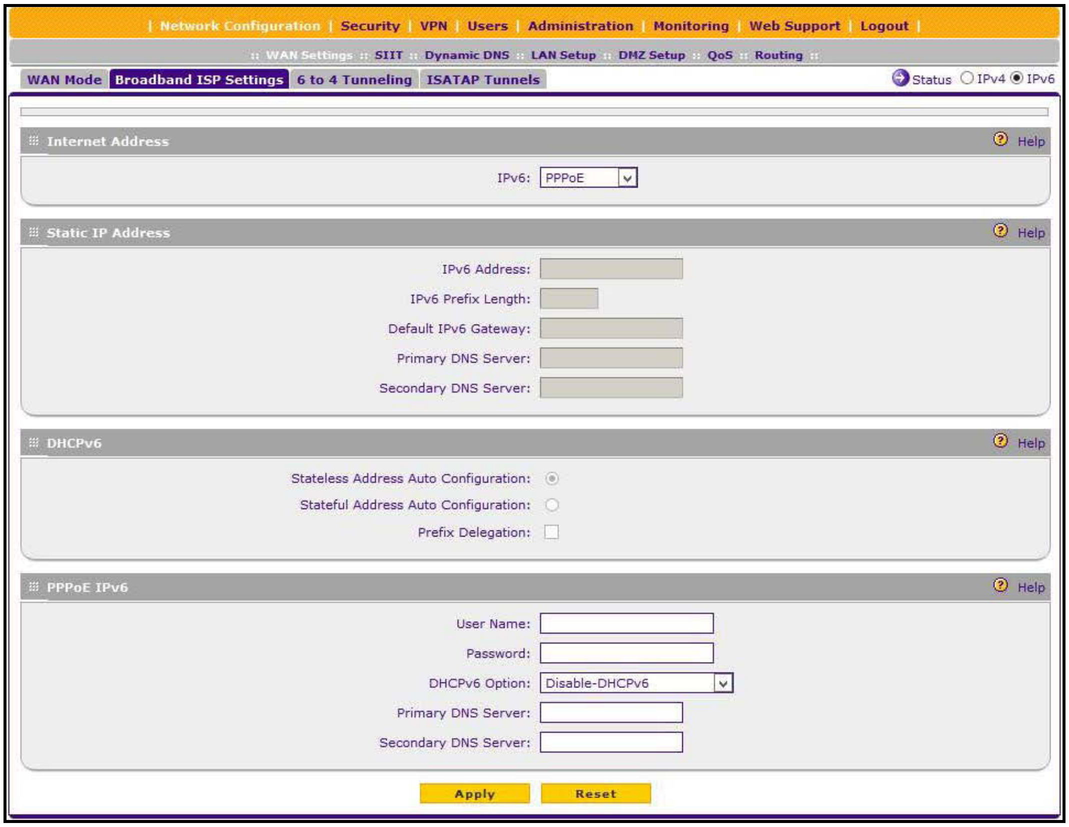
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > Broadband ISP Settings**.

   The Broadband ISP Settings screen displays.

3. Select the **IPv6** radio button.



IPv6: PPPoE

Stateless Address Auto Configuration: ●
Stateful Address Auto Configuration: ○
Prefix Delegation: □

DHCPv6 Option: Disable-DHCPv6

4. In the Internet Address section, from the **IPv6** list, select **PPPoE**.

5. In the PPPoE IPv6, enter the settings as described in the following table.

   Your IPv6 ISP gave you your PPPoE IPv6 information.

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** list, select one of the following DHCPv6 server options, as directed by your ISP: • **Disable-DHCPv6**. DHCPv6 is disabled. You must specify the DNS servers in the **Primary DNS Server** and **Secondary DNS Server** fields to receive an IP address from the ISP. • **DHCPv6 StatelessMode**. The VPN firewall generates its own IP address by using a combination of locally available information and router advertisements but receives DNS server information from the ISP's DHCPv6 server. Router advertisements include a prefix that identifies the subnet that is associated with the WAN port. The IP address is formed from a combination of this prefix and the MAC address of the WAN port. The IP address is a dynamic address. • **DHCPv6 StatefulMode**. The VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from the ISP's DHCPv6 server. The IP address is a dynamic address. • **DHCPv6 Prefix Delegation**. The VPN firewall obtains a prefix from the ISP's DHCPv6 server through prefix delegation, for example, 2001:db8::/64. The VPN firewall's own stateless DHCPv6 server can assign this prefix to its IPv6 LAN clients. For more information about prefix delegation, see *Stateless DHCPv6 Server with Prefix Delegation* on page 79.
Primary DNS Server	If you selected **Disable-DHCPv6** from the **DHCPv6 Options** list, the IPv6 IP address of the ISP's primary DNS server.
Secondary DNS Server	If you selected **Disable-DHCPv6** from the **DHCPv6 Options** list, the IPv6 IP address of the ISP's secondary DNS server.

6. Click the **Apply** button.

   Your changes are saved.

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

   The Connection Status pop-up screen displays, which shows a static IP address configuration; the screen for PPPoE is similar.)

   The Connection Status screen shows 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 389.

   For more information about the Connection Status screen, see *View the WAN Port Status* on page 373.

   If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must enter that address on the Broadband Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 52).

Configure 6to4 Automatic Tunneling

If your network is an isolated IPv6 network that is not connected to an IPv6 ISP, you must 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.

If the VPN firewall functions as the endpoint for 6to4 tunnels in your network, make sure that the VPN firewall uses a static IPv4 address (see *Manually Configure an IPv4 Internet Connection* on page 31). A dynamic IPv4 address can cause routing problems on the 6to4 tunnels.

If you do not use a stateful DHCPv6 server in your LAN, you must 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 78.

Typically, 6to4 tunnel addresses start with a 2002 prefix (decimal notification). On the VPN firewall, a 6to4 tunnel is indicated by sit0-WAN1 (see *View the Tunnel Status and IPv6 Addresses* on page 51).

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

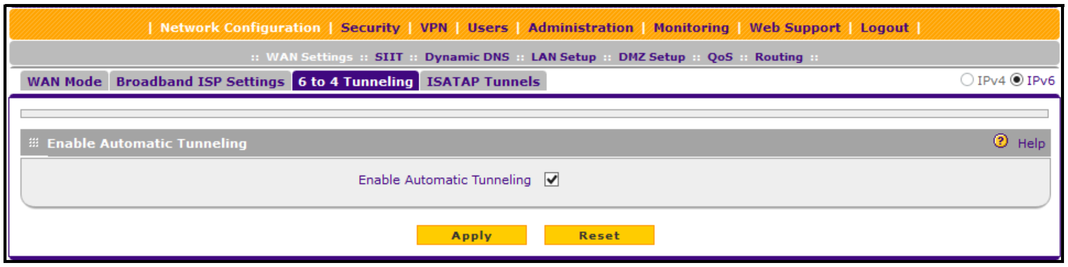
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

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


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
WAN Mode
Broadband ISP Settings
6 to 4 Tunneling
ISATAP Tunnels
○ IPv4 ● IPv6
Enable Automatic Tunneling
Help
Apply
Reset

Enable Automatic Tunneling ☑

3. Select the **Enable Automatic Tunneling** check box.
4. Click the **Apply** button.

   Your changes are saved.

Configure ISATAP Automatic Tunneling

If your network is an IPv4 network or IPv6 network that consists of both IPv4 and IPv6 devices, you must 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 78.

If you do not use a stateful DHCPv6 server in your LAN, you must 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 78.

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

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

➢ **To configure an ISATAP tunnel:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

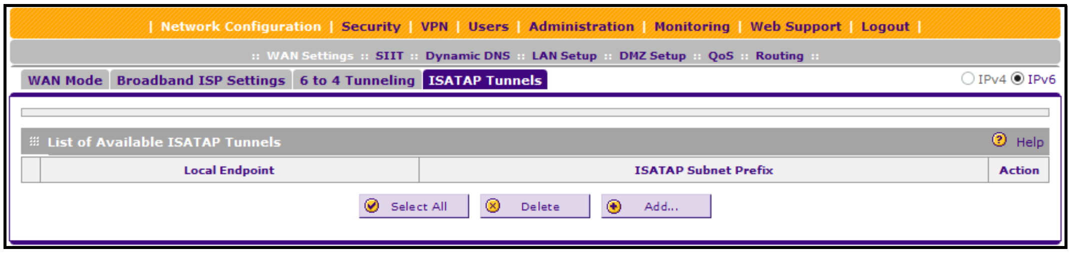
b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

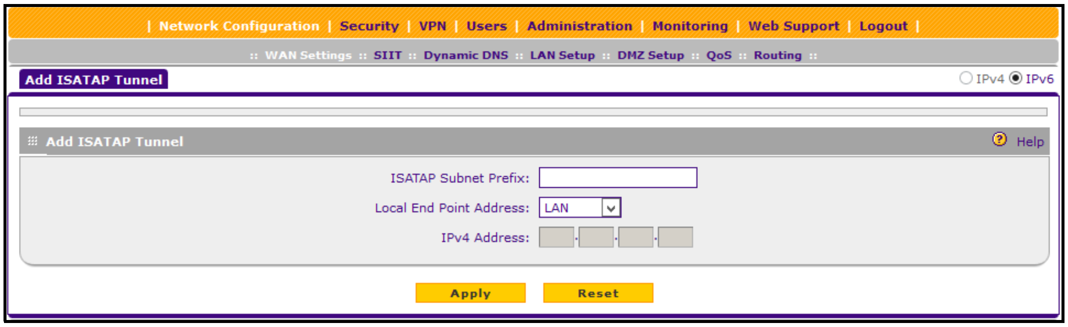
2. Select **Network Configuration > WAN Settings > ISATAP Tunnels**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
WAN Mode
Broadband ISP Settings
6 to 4 Tunneling
ISATAP Tunnels
○ IPv4 ● IPv6
Help
Select All
Delete
Add...

List of Available ISATAP Tunnels

	Local Endpoint	ISATAP Subnet Prefix	Action

3. Click the **Add** table button under the List of Available ISATAP Tunnels table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Add ISATAP Tunnel
○ IPv4 ● IPv6
Help
Apply
Reset

Add ISATAP Tunnel

ISATAP Subnet Prefix:

Local End Point Address: LAN

IPv4 Address: . . .

4. 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 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 must specify in the **IPv4 Address** fields.
IPv4 Address	If you select **Other IP** from the **Local End Point Address** list, enter the IPv4 address.

5. Click the **Apply** button.

   Your changes save.

➢ To edit an ISATAP tunnel:

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > ISATAP Tunnels**.

   The ISATAP Tunnels screen displays.

3. In the Action column for the tunnel that you want to modify, click the **Edit** button.

   The Edit ISATAP Tunnel screen displays. This screen is identical to the Add ISATAP Tunnel screen.

4. Modify the settings as described in *Table 9* on page 49.
5. Click the **Apply** button.

   Your changes are saved.

➢ **To delete one or more tunnels:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > ISATAP Tunnels**.

   The ISATAP Tunnels screen displays.

3. 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.
4. Click the **Apply** button.

   Your changes are saved.

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:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

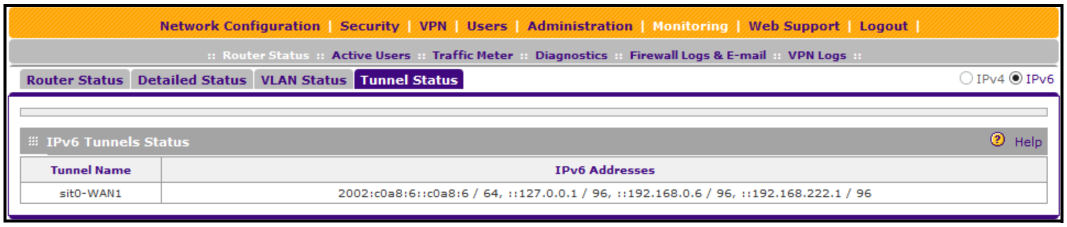
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Router Status > Tunnel Status**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status | Detailed Status | VLAN Status | Tunnel Status
○ IPv4 ● IPv6
IPv6 Tunnels Status
Help

Tunnel Name	IPv6 Addresses
sit0-WAN1	2002:c0a8:6::c0a8:6 / 64, ::127.0.0.1 / 96, ::192.168.0.6 / 96, ::192.168.222.1 / 96

3. View the IPv6 Tunnel Status table 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 use a permanently assigned IPv4 addresses can communicate with an IPv4-only device.

SIIT functions with IPv4-translated addresses, which are addresses in 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 must be IPv4 / IPv6. NETGEAR’s implementation of SIIT lets you enter a single IPv4 address on the SIIT screen. This IPv4 address is then used in the IPv4-translated address for IPv6 devices to enable communication between IPv4-only devices on the VPN firewall's LAN and IPv6-only devices on the WAN.

➤ **To configure SIIT:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

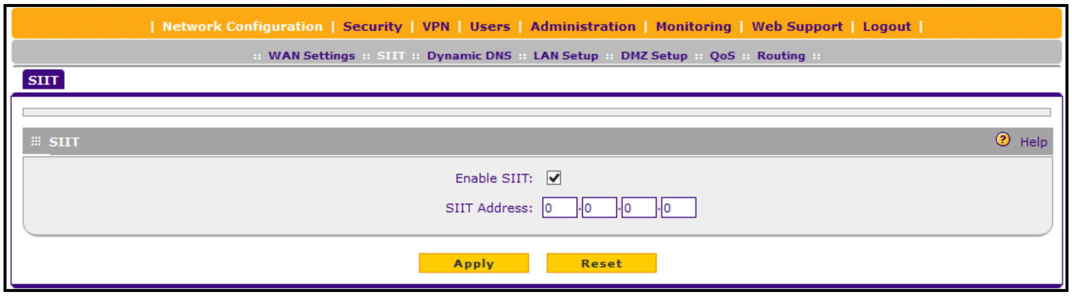
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > SIIT**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
SIIT
SIIT
Help
Apply
Reset

Enable SIIT: ☑

SIIT Address: 0 . 0 . 0 . 0

3. Select the **Enable SIIT** check box.
4. In the **SIIT Address** fields, enter the IPv4 address to be used in the IPv4-translated address for IPv6 devices.
5. Click the **Apply** button.

   Your changes are saved.

Configure Advanced WAN Options and Other Tasks

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

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. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

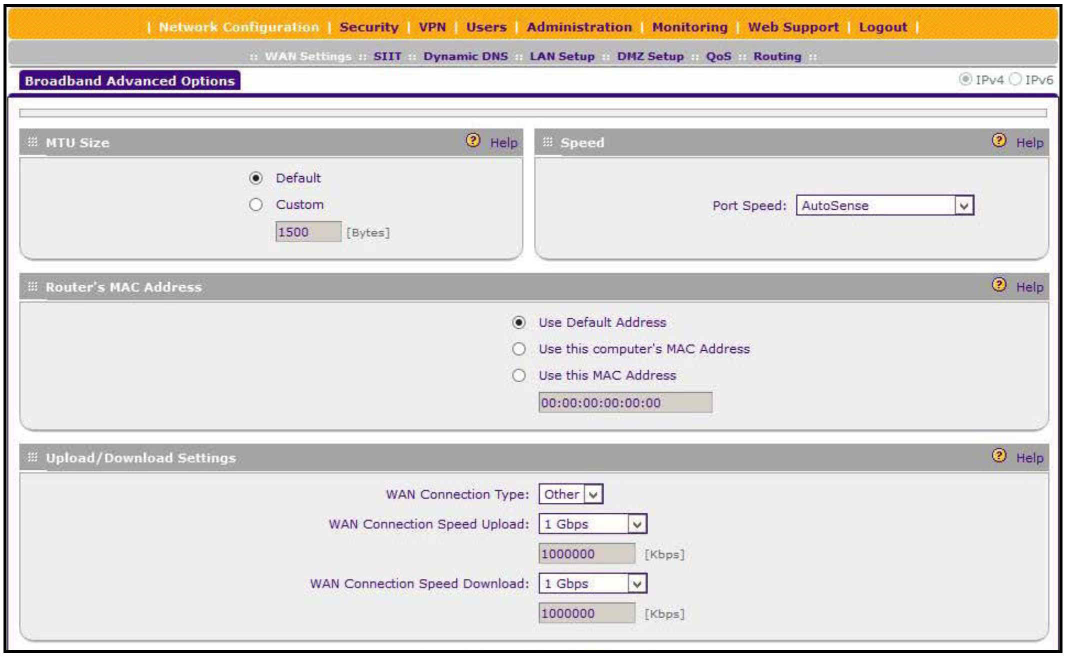
c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > Broadband ISP Settings**.

   The Broadband ISP Settings screen displays the IPv4 settings.

3. Click the **Advanced** option arrow in the upper right of the screen.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Help
Help
Help
Help

Broadband Advanced Options

● IPv4 ○ IPv6

MTU Size

● Default

○ Custom

1500 [Bytes]

Speed

Port Speed: AutoSense

Router's MAC Address

● Use Default Address

○ Use this computer's MAC Address

○ Use this MAC Address

00:00:00:00:00:00

Upload/Download Settings

WAN Connection Type: Other

WAN Connection Speed Upload: 1 Gbps

1000000 [Kbps]

WAN Connection Speed Download: 1 Gbps

1000000 [Kbps]

4. 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.

Table 10. Broadband Advanced Options screen settings (continued)

Setting	Description
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. Do not do this unless you are sure that it is necessary for your ISP connection.
Speed	
In most cases, the VPN firewall can automatically determine the connection speed of the WAN port of the device (modem, dish, or router) that provides the WAN connection. If you cannot establish an Internet connection, you might need to manually select the port speed. If you know the Ethernet port speed of the modem, dish, or router, select it from the mlist. Use the half-duplex settings only if the full-duplex settings do not function correctly. Select one of the following speeds from them list: • **AutoSense**. Speed autosensing. This is the default setting. The firewall 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 is assigned a unique 48-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. By default the **Use Default Address** radio button is selected. Make one of the following selections:	
Use Default Address	Each computer or router on your network is assigned a unique 32-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. To use the VPN firewall's own MAC address, select the **Use Default Address** radio button.
Use this computer's MAC Address	Select the **Use this computer's MAC Address** radio button to allow the VPN firewall to use the MAC address of the computer that 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 requires for MAC authentication. **Note:** The format for the MAC address is 01:23:45:67:89:AB (numbers 0–9 and either uppercase or lowercase letters A–F). If you enter a MAC address, the existing entry is overwritten.
Upload/Download Settings You can configure the WAN's maximum bandwidth of upstream and downstream settings for the other components in the system to operate optimally.	
WAN connection type	The type of connection being used to connect to the internet.

Table 10. Broadband Advanced Options screen settings (continued)

Setting	Description
WAN connection speed upload	The maximum bandwidth of upstream provided by your Internet service provider.
WAN connection speed download	The maximum bandwidth of downstream provided by your Internet service provider.

5. Click the **Apply** button.

   Your changes are saved.

Additional WAN-Related Configuration Tasks

If you want the ability to manage the VPN firewall remotely, enable remote management (see *Configure Remote Management Access* on page 328). If you enable remote management, NETGEAR strongly recommends that you change your password (see *Change Passwords and Administrator and Guest Settings* on page 326).

You can also set up the traffic meter for the WAN interface. See *Enable the WAN Traffic Meter* on page 349.

Verify the Connection

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

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

What to Do Next

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

- *Chapter 3, LAN Configuration*
- *Configure Authentication Domains, Groups, and Users* on page 287
- *Manage Digital Certificates for VPN Connections* on page 308
- *Use the IPSec VPN Wizard for Client and Gateway Configurations* on page 213

LAN Configuration

3

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

Manage IPv4 Virtual LANs and DHCP Options

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 must 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 sets up the VLANs.

VLANs offer 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.

This section contains the following topics:

- *Port-Based VLANs*
- *Assign and Manage VLAN Profiles*
- *VLAN DHCP Options*
- *Configure a VLAN Profile*
- *Configure VLAN MAC Addresses and LAN Advanced Settings*

Port-Based VLANs

The VPN firewall supports port-based VLANs. Port-based VLANs help to confine broadcast traffic to the LAN ports. Even though a LAN port can be a member of more than one VLAN, the port can use only one VLAN ID as its port VLAN identifier (PVID). By default, all eight

LAN ports of the VPN firewall are assigned to the default VLAN, or VLAN 1. Therefore, by default, all eight LAN ports use the default PVID 1. However, you can assign another PVID to a LAN port by selecting a VLAN profile from the list on the LAN Setup screen.

After you create a VLAN profile and assign one or more ports to the profile, you must enable the profile to activate it.

The VPN firewall's default VLAN cannot be deleted. All untagged traffic is routed through the default VLAN (VLAN1), which you must 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 includes two Ethernet ports, one of which is connected to the VPN firewall, the other one to another device.

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

The configuration of the DHCP options for the default VLAN is described in *Configure the IPv4 Internet Connection and WAN Settings* on page 26. For information about how to add and edit a VLAN profile, including its DHCP options, see *Configure a VLAN Profile* on page 61.

Assign and Manage VLAN Profiles

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

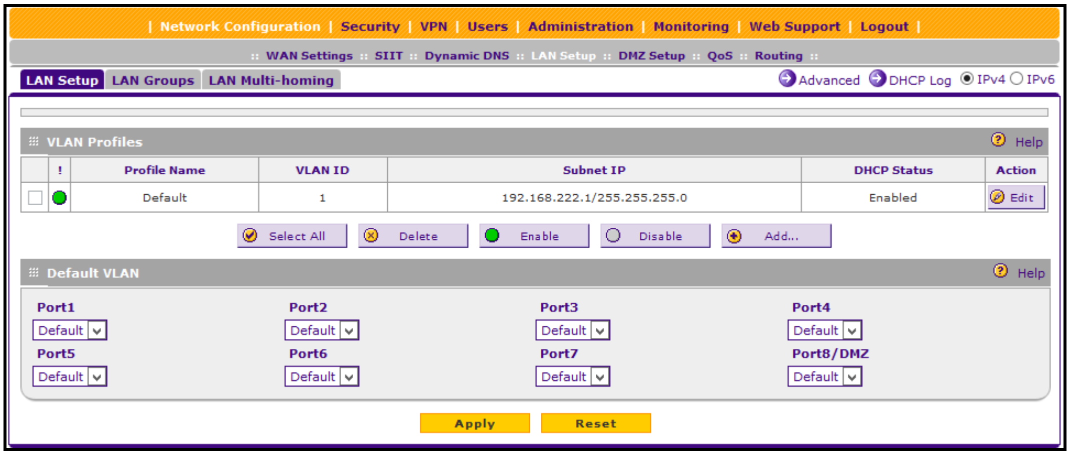
b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
Advanced
DHCP Log
● IPv4 ○ IPv6
VLAN Profiles
Help
Select All
Delete
Enable
Disable
Add...
Default VLAN
Help
Apply
Reset

	!	Profile Name	VLAN ID	Subnet IP	DHCP Status	Action
□	●	Default	1	192.168.222.1/255.255.255.0	Enabled	Edit

Port1	Port2	Port3	Port4
Default	Default	Default	Default
Port5	Port6	Port7	Port8/DMZ
Default	Default	Default	Default

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 Enabled or Disabled.
- **Action**. The **Edit** table button, which provides access to the Edit VLAN Profile screen.

3. Assign a VLAN profile to a LAN port by selecting a VLAN profile from the list.

The enabled VLAN profiles are displayed in the lists.

4. Click the **Apply** button.

Your settings are saved.

VLAN DHCP Options

For each VLAN, you must specify the Dynamic Host Configuration Protocol (DHCP) options. For more information, see *Configure a VLAN Profile* on page 61.

For more information about the configuration of the DHCP options for the VPN firewall's default VLAN, or VLAN 1, see *Configure the IPv4 Internet Connection and WAN Settings* on page 26. For information about the DHCP options, see the following sections:

- *DHCP Server*
- *DHCP Relay*
- *DNS Proxy*
- *LDAP Server*

DHCP Server

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

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

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

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

DHCP Relay

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

DNS Proxy

When the DNS proxy option is enabled for a VLAN, the 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 VPN firewall's LAN IP address). When the DNS proxy option is disabled for a VLAN, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address.

LDAP Server

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

Configure a VLAN Profile

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

After you complete the LAN setup, all outbound traffic is allowed and all inbound traffic is discarded except responses to requests from the LAN side.

➢ **To add a VLAN profile:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

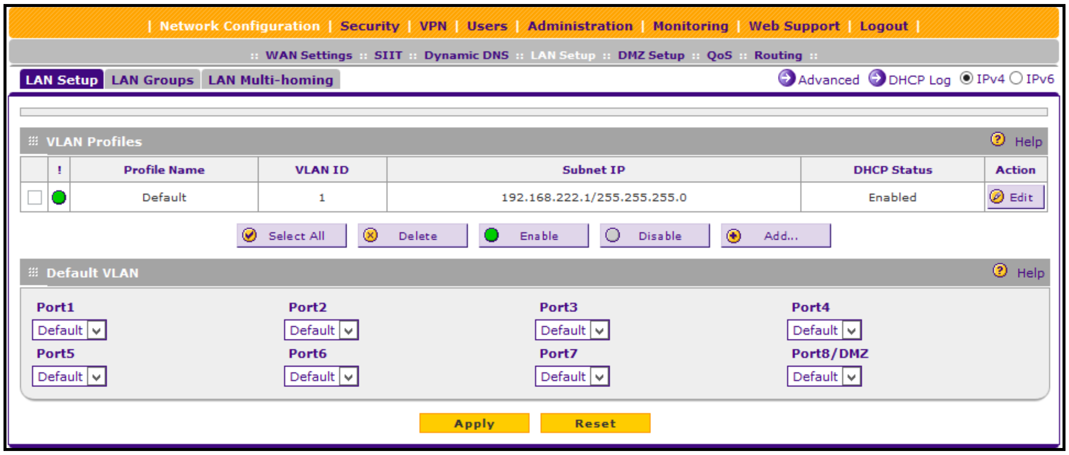
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
Advanced
DHCP Log
Help
Select All
Delete
Enable
Disable
Add...
Help
Apply
Reset

● IPv4 ○ IPv6

VLAN Profiles

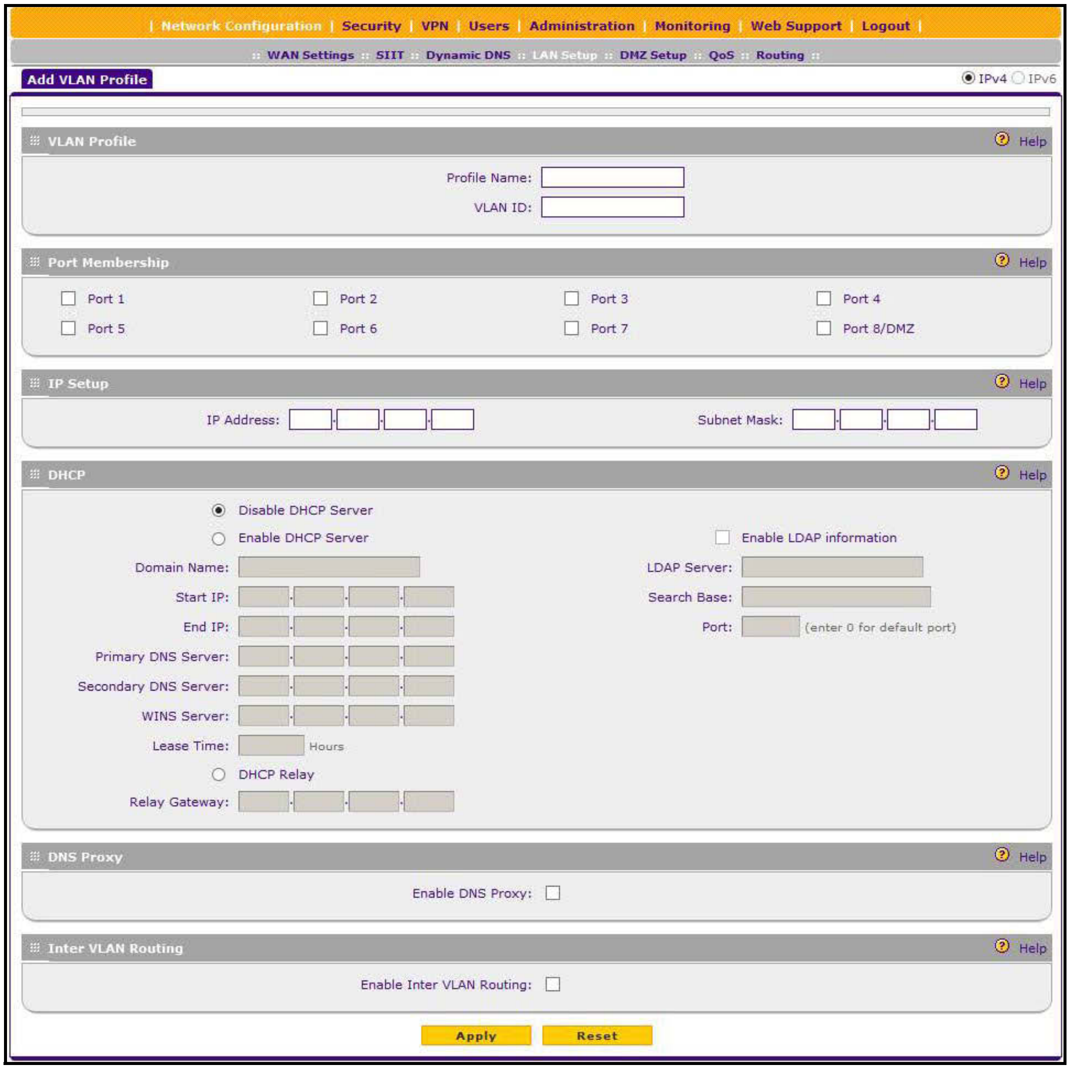
	!	Profile Name	VLAN ID	Subnet IP	DHCP Status	Action
□	●	Default	1	192.168.222.1/255.255.255.0	Enabled	Edit

Default VLAN

Port1	Port2	Port3	Port4
Default	Default	Default	Default
Port5	**Port6**	**Port7**	**Port8/DMZ**
Default	Default	Default	Default

For information about how to manage VLANs, see *Port-Based VLANs* on page 57. The following information describes how to configure a VLAN profile.

3. Under the VLAN Profiles table, click the **Add** table button.



4. 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 use the same VLAN ID number. **Note:** You can enter VLAN IDs from 2 to 4089. VLAN ID 1 is reserved for the default VLAN; VLAN ID 4094 is reserved for the DMZ interface.

Table 11. Add VLAN Profile screen settings (continued)

Setting	Description
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 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 must 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 must enter **https://10.0.0.1** in your browser to reconnect to the web management interface.
Subnet Mask	Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Based on the IP address that you assign, the VPN firewall automatically calculates the subnet mask. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the VPN firewall).
DHCP	
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you intend to manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. Except for the default VLAN for which the DHCP server is enabled, this is the default setting.

Table 11. Add VLAN Profile screen settings (continued)

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

Table 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 the following: • CN (for common name) • OU (for organizational unit) • O (for organization) • C (for country) • DC (for domain) For example, to search the Netgear.net domain for all last names of Johnson, you would enter cn=Johnson,dc=Netgear,dc=net
	Port	The port number for the LDAP server. The default setting is 0 (zero).
DNS Proxy		
Enable DNS Proxy	This setting is optional. To enable the VPN firewall to provide a LAN IP address for DNS address name resolution, select the **Enable DNS Proxy** check box. This feature 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 feature 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.	

5. Click the **Apply** button.

   Your settings are saved.

➤ To edit a VLAN profile:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

The LAN Setup screen displays.

3. For the VLAN profile that you want to modify, in the Action column, click the **Edit** button.

The Edit VLAN Profile screen displays. This screen is identical to the Add VLAN Profile screen.

4. Modify the settings as described in *Table 11* on page 63.
5. Click the **Apply** button.

Your settings are saved.

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

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

The LAN Setup screen displays.

3. 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.

4. 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.

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.

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 use a unique MAC address:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

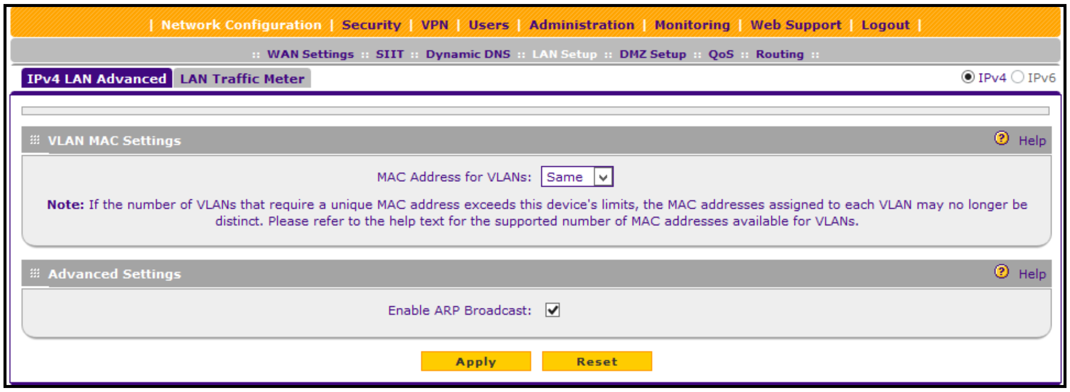
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. 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.

3. In the upper middle of the LAN Setup screen, click the **Advanced** option arrow.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
IPv4 LAN Advanced
LAN Traffic Meter
● IPv4 ○ IPv6
Help
Help
Apply
Reset

VLAN MAC Settings

MAC Address for VLANs: Same

Note: If the number of VLANs that require a unique MAC address exceeds this device's limits, the MAC addresses assigned to each VLAN may no longer be distinct. Please refer to the help text for the supported number of MAC addresses available for VLANs.

Advanced Settings

Enable ARP Broadcast: ☑

4. From the **MAC Address for VLANs** list, select **Unique**.

   The default is Same.

5. (Optional) 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.

6. Click the **Apply** button.

   Your settings are saved.

Configure IPv4 Multihome LAN IP Addresses on the Default VLAN

If computers on your LAN use different IPv4 networks (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 must be unique and cannot be assigned to a VLAN.

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

Make sure that any secondary LAN addresses are different from the primary LAN, WAN, and DMZ IP addresses and subnet addresses that are already configured on the VPN firewall. The following is an example of correctly configured IPv4 addresses:

- **WAN IP address**. 10.0.0.1 with subnet 255.0.0.0
- **DMZ IP address**. 176.16.2.1 with subnet 255.255.255.0
- **Primary LAN IP address**. 192.168.1.1 with subnet 255.255.255.0
- **Secondary LAN IP address**. 192.168.20.1 with subnet 255.255.255.0

➢ **To add a secondary LAN IPv4 address:**

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

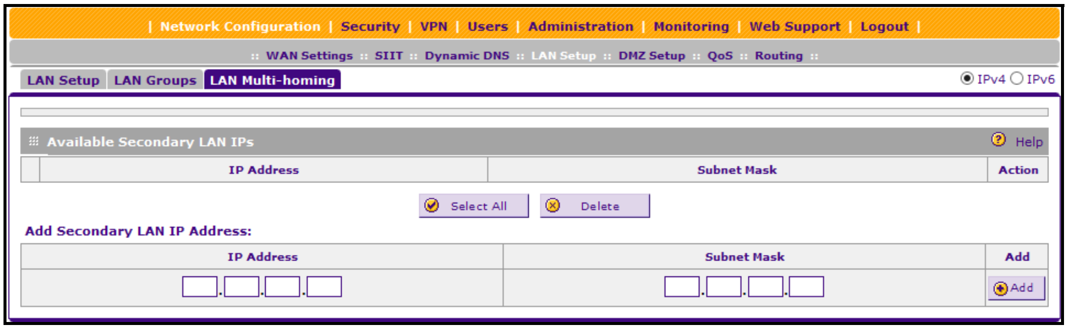
c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

d. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Multi-homing**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
● IPv4 ○ IPv6
Help
Select All
Delete
Add

Available Secondary LAN IPs

	IP Address	Subnet Mask	Action

Add Secondary LAN IP Address:

IP Address	Subnet Mask	Add
□.□.□.□	□.□.□.□	Add

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

3. In the Add Secondary LAN IP Address section, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the LAN ports.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.
4. To add the secondary IP address to the Available Secondary LAN IPs table, in the rightmost column, click the **Add** table button.
5. Repeat *Step 3* and *Step 4* for each secondary IP address that you want to add to the Available Secondary LAN IPs table.

➢ To edit a secondary LAN IP address:

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Multi-homing**.

   The LAN Multi-homing screen displays.

3. In the Action column for the secondary IP address that you want to modify, click the **Edit** button.

   The Edit LAN Multi-homing screen displays.

4. Modify the IP address or subnet mask or both.
5. Click the **Apply** button.

   Your settings are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Multi-homing**.

   The LAN Multi-homing screen displays.

3. 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 all secondary IP addresses.
4. Click the **Delete** table button.

   The information is deleted.

Manage IPv4 Groups and Hosts (IPv4 LAN Groups)

The Known PCs and Devices table on the LAN Groups (IPv4) screen lists all known computers and network devices that are assigned dynamic IP addresses by the VPN firewall, were discovered by other means, or were entered manually. Collectively, these entries make up the network database. For more information, see *Manage the Network Database* on page 73.

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.

  In large networks, scanning the network might generate unwanted traffic. When the VPN firewall receives a reply to an ARP request, it might not be able to determine the device name if the software firewall of the device blocks the name.
- **Manual entry**. You can manually enter information about a network device.

These are some advantages of the network database:

- Generally, you do not need to enter an IP address or a MAC address. Instead, you can select the name of the desired computer or device.
- 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 uses 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 127).
  - You can select groups that are allowed access to URLs that you blocked for other groups, or the other way around, block access to URLs that you allowed access to for groups (see *Configure Content Filtering* on page 189).
  - If necessary, you can also create firewall rules to apply to a single computer (see *Enable Source MAC Filtering* on page 196). Because the MAC address is used to identify each computer, users cannot avoid these restrictions by changing their IP address.

This section contains the following topics:

- *Manage the Network Database*
- *Change Group Names in the Network Database*

- *DHCPv6 Server Options*

Manage the Network Database

You can view the network database, manually add or remove database entries, and edit database entries. The Known PCs and Devices table lists the entries in the network database.

➢ To view the network database:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

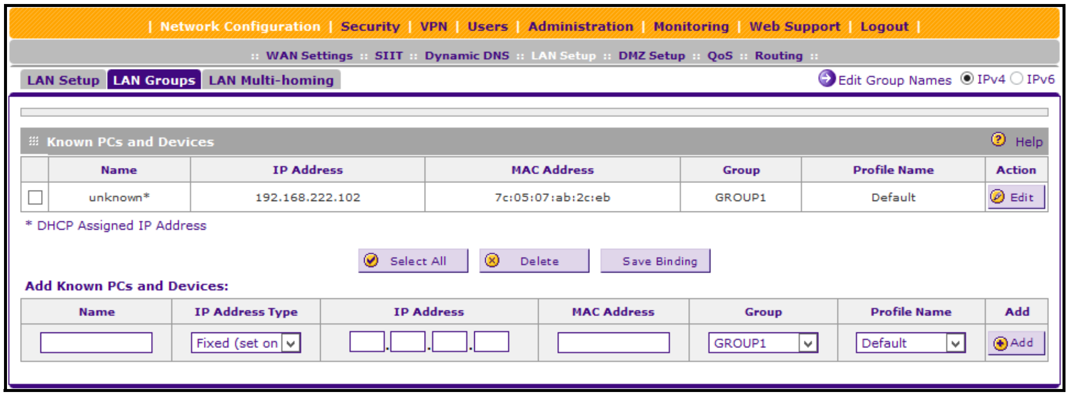
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Groups**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
Edit Group Names
● IPv4 ○ IPv6
Help
Select All
Delete
Save Binding
Add

Known PCs and Devices

	Name	IP Address	MAC Address	Group	Profile Name	Action
□	unknown*	192.168.222.102	7c:05:07:ab:2c:eb	GROUP1	Default	Edit

* DHCP Assigned IP Address

Add Known PCs and Devices:

Name	IP Address Type	IP Address	MAC Address	Group	Profile Name	Add
	Fixed (set on	. . .		GROUP1	Default	Add

3. For each computer or device, view the following fields:
   - **Check box**. Allows you to select the computer or device in the table.
   - **Name**. The name of the computer or device. For computers that do not support the NetBIOS protocol, the name is displayed as *Unknown* (you can edit the entry manually to add a meaningful name). If the computer or device was assigned an IP address by the DHCP server, the name is appended by an asterisk.
   - **IP Address**. The current IP address of the computer or device. For DHCP clients of the VPN firewall, this IP address does not change. If a computer or device is assigned a static IP address, you must update this entry manually after the IP address on the computer or device changes.
   - **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** 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** 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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Groups**.

   The LAN Groups screen displays.

3. In the Add Known PCs and Devices section, 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 list, select how the computer or device receives its IP address: • **Fixed (set on PC)**. The IP address is statically assigned on the computer or device. • **Reserved (DHCP Client)**. The DHCP server of the VPN firewall always assigns the specified IP address to this client during the DHCP negotiation (see *Set Up DHCP Address Reservation* on page 78). **Note:** For both types of IP addresses, the 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 must be outside 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** 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, a–f, and A–F), such as 01:23:d2:6f:89:ab.
Group	From the list, select the group to which the computer or device is assigned. (Group 1 is the default group.)
Profile Name	From the list, select the name of the VLAN profile to which the computer or device is assigned.

4. To add the computer or device to the Known PCs and Devices table, click the **Add** table button.
5. 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.

   The saved binding is also displayed on the IP/MAC Binding screen.

Edit Computers or Devices in the Network Database

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

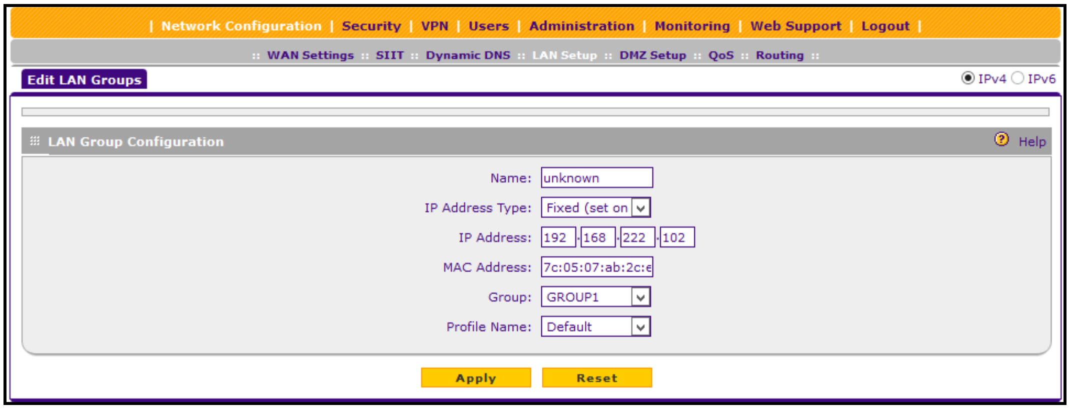
      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > LAN Setup > LAN Groups**.

   The LAN Groups screen displays.

3. In the **Known PCs and Devices** table, click the **Edit** table button of a table entry.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Edit LAN Groups
● IPv4 ○ IPv6
LAN Group Configuration
Help
Apply
Reset

Name:	unknown
IP Address Type:	Fixed (set on
IP Address:	192 . 168 . 222 . 102
MAC Address:	7c:05:07:ab:2c:e
Group:	GROUP1
Profile Name:	Default

4. Modify the settings.

   For more information, see *Table 12* on page 74.

5. Click the **Apply** button.

   Your changes are saved.

Deleting Computers or Devices from the Network Database

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Groups**.

   The LAN Groups screen displays.

3. 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.

4. Click the **Delete** table button.

   The information is deleted. 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.

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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

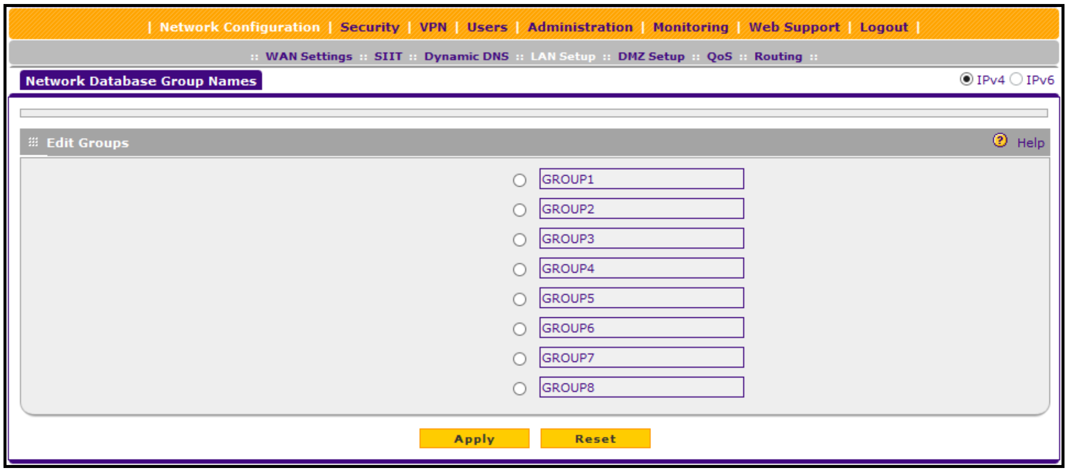
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Groups**.

   The LAN Groups screen displays.

3. To the right of the LAN submenu tabs, click the **Edit Group Names** option arrow.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Network Database Group Names
● IPv4 ○ IPv6
Edit Groups
Help
Apply
Reset

○ GROUP1
○ GROUP2
○ GROUP3
○ GROUP4
○ GROUP5
○ GROUP6
○ GROUP7
○ GROUP8

4. Select the radio button next to the group name that you want to edit.
5. 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.

6. Repeat *Step 4* and *Step 5* for any other group names.
7. Click the **Apply** button.

   Your changes are saved.

Set Up DHCP Address Reservation

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

To reserve and bind an IP address to a MAC address, select **Reserved (DHCP Client)** from the **IP Address Type** 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 74.

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

The saved binding is also displayed on the IP/MAC Binding screen.

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 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, are depreciated. However, NETGEAR implements 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.

This section contains the following topics:

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

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, three DHCPv6 options are available.

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 must configure the RADVD and advertisement prefixes. For more information, see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 88.

Stateless DHCPv6 Server with Prefix Delegation

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

Prefix delegation functions in the following way:

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

   You must select the **Prefix Delegation** check box on the ISP Broadband Settings screen for IPv6. For more information, see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection* on page 40.

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

   This prefix is automatically added to the List of Prefixes to Advertise table on the LAN RADVD screen for IPv6. For more information, see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 88.

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 then perform the following tasks:

   - Select the **Prefix Delegation** check box on the LAN Setup screen for IPv6.

     For more information, see *Configure the IPv6 LAN* on page 80.

- Configure the RADVD.

  For more information, see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 88.

- Optionally, manually add prefixes to the List of Prefixes for Prefix Delegation table on the LAN Setup screen for IPv6.

  For more information, see *IPv6 LAN Prefixes for Prefix Delegation* on page 86.

- Optionally, manually add prefixes to List of Prefixes to Advertise table on the RADVD screen.

  For more information, see *Advertisement Prefixes for the LAN* on page 90.

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 must configure IPv6 address pools. For more information, see *IPv6 LAN Address Pools* on page 83.

Configure the IPv6 LAN

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

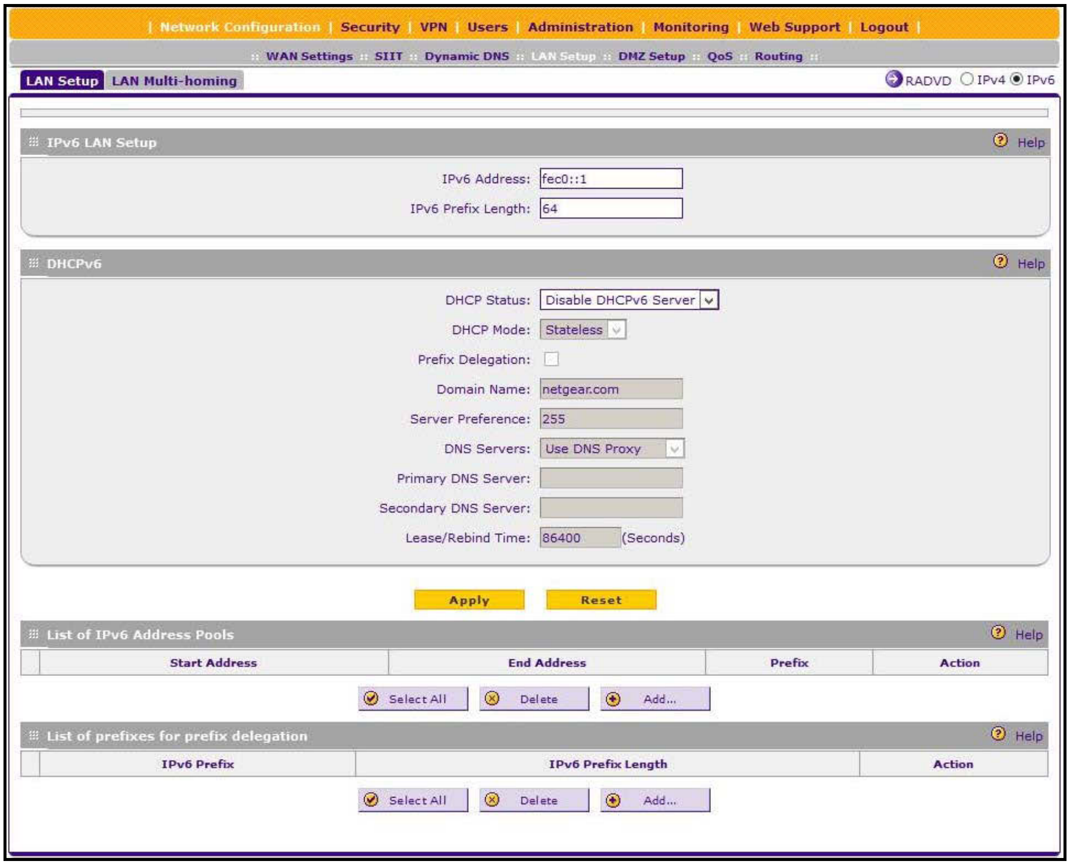
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Multi-homing
RADVD ○ IPv4 ● IPv6
Help
Apply
Reset
Select All
Delete
Add...

IPv6 LAN Setup

IPv6 Address: fec0::1

IPv6 Prefix Length: 64

DHCPv6

DHCP Status: Disable DHCPv6 Server

DHCP Mode: Stateless

Prefix Delegation: □

Domain Name: netgear.com

Server Preference: 255

DNS Servers: Use DNS Proxy

Primary DNS Server:

Secondary DNS Server:

Lease/Rebind Time: 86400 (Seconds)

List of IPv6 Address Pools

Start Address	End Address	Prefix	Action

List of prefixes for prefix delegation

IPv6 Prefix	IPv6 Prefix Length	Action

4. Enter the settings as described in the following 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 *Manage the IPv6 LAN* on page 78.)
IPv6 Prefix Length	Enter the IPv6 prefix length, for example, 10 or 64. The default prefix length is 64.

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

Setting	Description	
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 must complete the DHCPv6 fields.	
	DHCP Mode	Select one of the DHCPv6 modes from the 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 must configure the RADVD and advertisement prefixes (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the LAN* on page 88). As an option, you can enable prefix delegation (see the explanation later 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 must add IPv6 address pools to the List of IPv6 Address Pools table on the LAN Setup screen (see *IPv6 LAN Address Pools* on page 83).
	Prefix Delegation	If you 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 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 88). • **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 list: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers that you configured on the Broadband ISP Settings (IPv6) screen (see *Configure a Static IPv6 Internet Connection* on page 42). • **Use DNS from ISP**. The 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).	

The IPv6 address pools and prefixes for prefix delegation are described in the following sections:

- *IPv6 LAN Address Pools*
- *IPv6 LAN Prefixes for Prefix Delegation*

5. Click the **Apply** button.

   Your changes are saved.

IPv6 LAN Address Pools

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

➢ To add an IPv6 LAN address pool:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

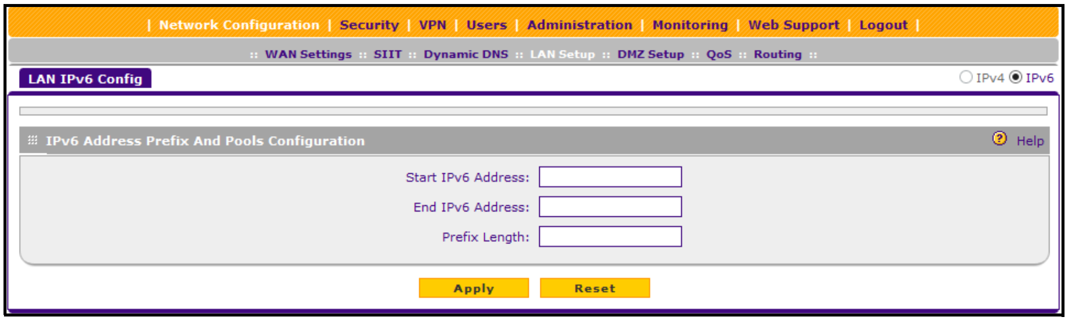
The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

The LAN Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.

4. Under the **List of IPv6 Address Pools** table, click the **Add** button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
LAN IPv6 Config
○ IPv4 ● IPv6
IPv6 Address Prefix And Pools Configuration
Help
Start IPv6 Address:
End IPv6 Address:
Prefix Length:
Apply
Reset

5. 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.

6. Click the **Apply** button.

Your changes are saved.

➢ To edit an IPv6 LAN address pool:

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.
4. Click the **Edit** button in the Action column for the address pool that you want to modify.

   The LAN IPv6 Config screen displays.

5. Modify the settings as described in *Table 14* on page 84.
6. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.
4. 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.
5. Click the **Delete** table button.

   The information is deleted.

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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

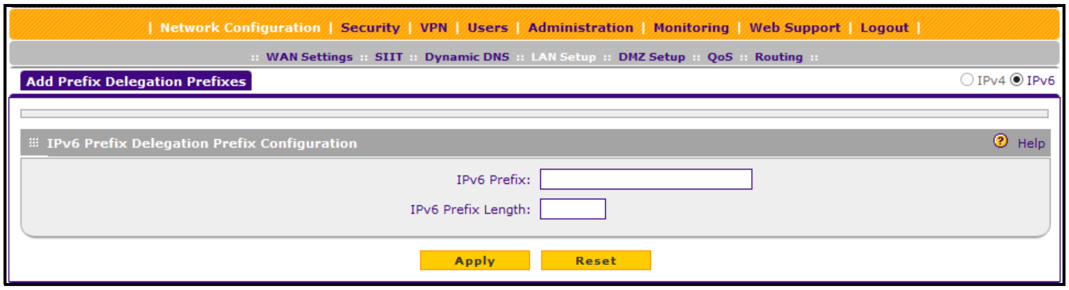
      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.

4. Under the List of Prefixes for Prefix Delegation table, click the **Add** button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Add Prefix Delegation Prefixes
○ IPv4 ● IPv6
IPv6 Prefix Delegation Prefix Configuration
Help
IPv6 Prefix:
IPv6 Prefix Length:
Apply
Reset

5. Enter the following settings:

   - **IPv6 Prefix**. Enter a prefix, for example, 2001:db8::.
   - **IPv6 Prefix Length**. Enter the IPv6 prefix length, for example, 64.

6. Click the **Apply** button.

   Your changes are saved.

➢ To edit a prefix:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

The LAN Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.
4. Click the **Edit** button in the Action column for the prefix that you want to modify.

The Edit Prefix Delegation Prefixes screen displays.

5. Modify the settings:.
   - **IPv6 Prefix**. Enter a prefix, for example, 2001:db8::.
   - **IPv6 Prefix Length**. Enter the IPv6 prefix length, for example, 64.
6. Click the **Apply** button.

Your changes are saved.

➤ **To delete one or more prefixes:**

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

The LAN Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.
4. 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.
5. Click the **Delete** table button.

The information is deleted.

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 must configure the Router Advertisement Deamon (RADVD) and advertisement prefixes.

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

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

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

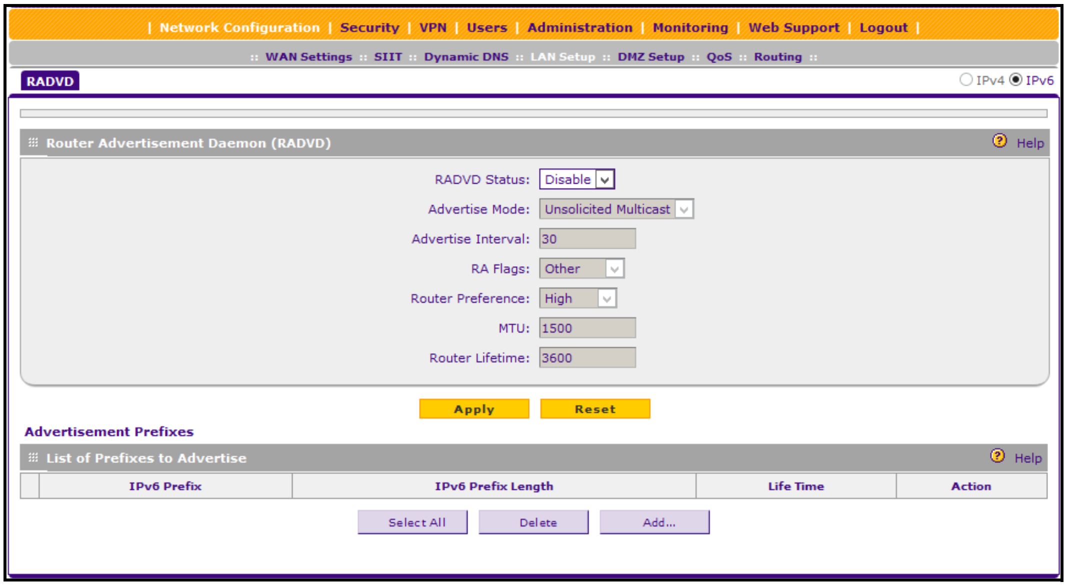
2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays.

3. Select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.

4. To the right of the **LAN Setup** tab, click the **RADVD** option arrow.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
RADVD
○ IPv4 ● IPv6
Help
Apply
Reset
Help
Select All
Delete
Add...

Router Advertisement Daemon (RADVD)

RADVD Status: Disable
Advertise Mode: Unsolicited Multicast
Advertise Interval: 30
RA Flags: Other
Router Preference: High
MTU: 1500
Router Lifetime: 3600

Advertisement Prefixes

List of Prefixes to Advertise

	IPv6 Prefix	IPv6 Prefix Length	Life Time	Action

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

Table 16. RADVD screen settings for the LAN

Setting	Description
RADVD Status	Select the RADVD status: • **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	Select the advertisement mode: • **Unsolicited Multicast**. The VPN firewall advertises unsolicited multicast packets at a rate that is specified by the advertisement interval. • **Unicast only**. The VPN firewall responds to unicast packet requests only. No unsolicited packets are advertised. Select this option for nonbroadcast multiple access (NBMA) links such as ISATAP.
Advertise Interval	Enter the advertisement interval of unsolicited multicast packets in seconds. The minimum value is 10 seconds; the maximum value is 1800 seconds.
RA Flags	Select what type of information the DHCPv6 server provides in the LAN: • **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	Select the VPN firewall's preference in relation to other hosts and routers in the LAN: • **Low**. The VPN firewall is treated as a nonpreferred router in the LAN. • **Medium**. The VPN firewall is treated as a neutral router in the LAN. • **High**. The VPN firewall is treated as a preferred router in the LAN.
MTU	The maximum transmission unit (MTU) size for a packet in one transmission over a link. The default setting is 1500.
Router Lifetime	The router lifetime specifies how long the default route that was created as a result of the router advertisement remains 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.

6. Click the **Apply** button.

   Your changes are saved.

Advertisement Prefixes for the LAN

You must configure the prefixes that are advertised in the LAN RAs, as follows:

- For a 6to4 address, you must specify only the site-level aggregation identifier (SLA ID) and the prefix lifetime.

- For a global, local, or ISATAP address, you must specify the prefix, prefix length, and prefix lifetime.

➢ To add an advertisement prefix for the LAN:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

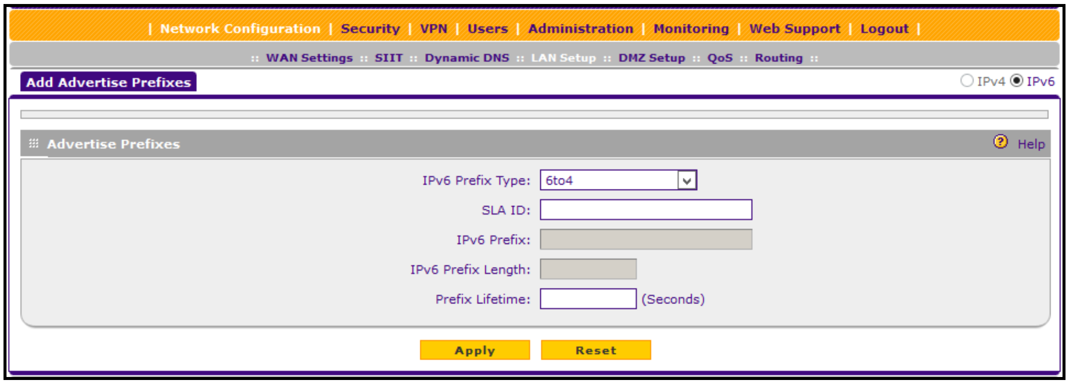
2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays.

3. Select the **IPv6** radio button.

4. To the right of the **LAN Setup** tab, click the **RADVD** option arrow.

5. Under the List of Prefixes to Advertise table, click the **Add** button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Add Advertise Prefixes
Advertise Prefixes
Help
Apply
Reset

○ IPv4 ● IPv6

IPv6 Prefix Type: 6to4

SLA ID:

IPv6 Prefix:

IPv6 Prefix Length:

Prefix Lifetime: (Seconds)

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

Table 17. Add Advertisement Prefix screen settings for the LAN

Setting	Description
IPv6 Prefix Type	Select the IPv6 prefix type: • **6to4**. The prefix is for a 6to4 address. You must 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 must be a global prefix or a site-local prefix; it cannot be a link-local prefix. You must 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 to be included in the advertisement.
IPv6 Prefix	Enter the IPv6 prefix for the VPN firewall's LAN to be included in the advertisement.
IPv6 Prefix Length	Enter the IPv6 prefix length (typically 64) to 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 remains valid. Enter the prefix lifetime in seconds to be included in the advertisement. The minimum period is 0 seconds; the maximum period is 65536 seconds.

7. Click the **Apply** button.

   Your changes are saved.

➤ To edit an advertisement prefix:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays.

3. Select the **IPv6** radio button.
4. Click the **RADVD** option arrow.
5. In the Action column for the advertisement prefix that you want to modify, click the **Edit** button.

The Add Advertisement Prefix screen displays.

6. Modify the settings as described in *Table 17* on page 92.
7. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays.

3. Select the **IPv6** radio button.
4. To the right of the **LAN Setup** tab, click the **RADVD** option arrow.
5. 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.
6. Click the **Delete** table button.

   The information is deleted.

Configure IPv6 Multihome LAN IP Addresses on the Default VLAN

If computers on your LAN use different IPv6 networks (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 must be unique and cannot be assigned to a VLAN. Secondary IP addresses cannot be configured in the DHCP server. The hosts on the secondary subnets must be manually configured with the IP addresses, gateway IP address, and DNS server IP addresses.

Make sure that any secondary LAN addresses are different from the primary LAN, WAN, and DMZ IP addresses and subnet addresses that are already configured on the VPN firewall. The following is an example of correctly configured IPv6 addresses:

- **WAN IP address**. 2000::e246:9aff:fe1d:1a9c with a prefix length of 64
- **DMZ IP address**. 176::e246:9aff:fe1d:a1bc with a prefix length of 64
- **Primary LAN IP address**. FEC0::1 with a prefix length of 10
- **Secondary LAN IP address**. 2001:db8:3000::2192 with a prefix length of 10

➢ To add a secondary LAN IPv6 address:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

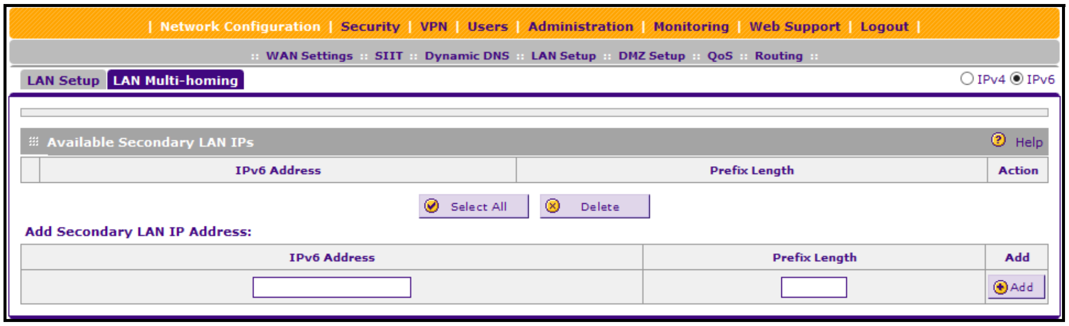
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Multi-homing**.

   The LAN Multi-homing screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Multi-homing
○ IPv4 ● IPv6
Available Secondary LAN IPs
Help
Select All
Delete
Add

	IPv6 Address	Prefix Length	Action

Add Secondary LAN IP Address:

IPv6 Address	Prefix Length	Add
		Add

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

4. In the Add Secondary LAN IP Address section, 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.
5. Click the **Add** table button.
6. Repeat *Step 3* and *Step 4* for each secondary IP address that you want to add to the Available Secondary LAN IPs table.

➢ To edit a secondary LAN IP address:

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Multi-homing**.

   The LAN Multi-homing screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.
4. In the Action column for the secondary IP address that you want to modify, click the **Edit** button.

   The Edit LAN Multi-homing screen displays.

5. Modify the IP address or prefix length, or both.
6. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup > LAN Multi-homing**.

   The LAN Multi-homing screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.
4. 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.
5. Click the **Delete** table button.

   The information is deleted.

Enable and Configure the DMZ Port for IPv4 and IPv6 Traffic

The demilitarized zone (DMZ) is a network that, by default, is configured with fewer firewall restrictions than the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. The rightmost LAN port on the VPN firewall can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN.

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

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

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. For information about how to define the DMZ WAN rules and LAN DMZ rules, see *Configure DMZ WAN Rules* on page 144 and *Configure LAN DMZ Rules* on page 153, respectively.

When you enable the DMZ port for IPv4 traffic, IPv6 traffic, or both, the DMZ LED next to LAN port 8 lights green to indicate that the DMZ port is enabled. For more information, see *Front Panel* on page 13.

This section contains the following topics:

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

DMZ Port for IPv4 Traffic

You can 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 13) and configure an IPv4 address and subnet mask for the DMZ port.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

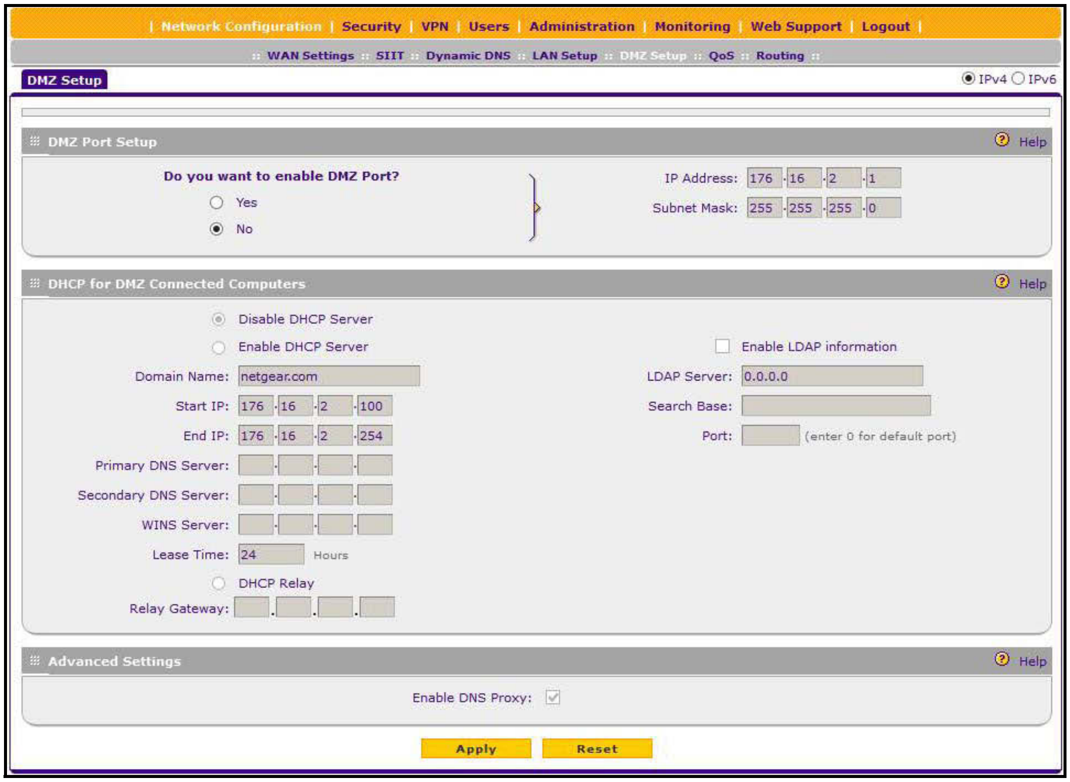
c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

d. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > DMZ Setup**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Help
Help
Help
Apply
Reset

DMZ Setup ● IPv4 ○ IPv6

DMZ Port Setup

Do you want to enable DMZ Port?
○ Yes
● No

IP Address: 176 . 16 . 2 . 1
Subnet Mask: 255 . 255 . 255 . 0

DHCP for DMZ Connected Computers

● Disable DHCP Server
○ Enable DHCP Server
Domain Name: netgear.com
Start IP: 176 . 16 . 2 . 100
End IP: 176 . 16 . 2 . 254
Primary DNS Server:
Secondary DNS Server:
WINS Server:
Lease Time: 24 Hours
○ DHCP Relay
Relay Gateway:

☐ Enable LDAP information
LDAP Server: 0.0.0.0
Search Base:
Port: (enter 0 for default port)

Advanced Settings

Enable DNS Proxy: ☑

3. 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. Complete the **IP Address** and **Subnet Mask** fields. • **No**. Allows you to disable the DMZ port after you configure it.	
	IP Address	Enter the IP address of the DMZ port. Make sure that the DMZ port IP address and LAN port IP address are in different subnets (for example, an address outside the LAN DHCP address pool, such as 192.168.1.101 when the LAN DHCP pool is 192.168.1.2–192.168.1.100). The default IP address for the DMZ port 176.16.2.1.
	Subnet Mask	Enter the IP subnet mask of the DMZ port. The subnet mask specifies the network number portion of an IP address. The subnet mask for the DMZ port is 255.255.255.0.
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.	

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

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

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

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td rowspan="4">Enable LDAP information</td><td colspan="2">To enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information, select the <b>Enable LDAP information</b> check box. Enter the following settings.</td></tr>
<tr><td>LDAP Server</td><td>The IP address or name of the LDAP server.</td></tr>
<tr><td>Search Base</td><td>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 the following:
• 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</td></tr>
<tr><td>Port</td><td>The port number for the LDAP server. The default setting is 0 (zero).</td></tr>
<tr><td colspan="3"><b>DNS Proxy</b></td></tr>
<tr><td>Enable DNS Proxy</td><td colspan="2">This setting is optional. To enable the VPN firewall to provide a LAN IP address for DNS address name resolution, select the <b>Enable DNS Proxy</b> check box. This check box is selected by default.
<b>Note:</b> 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.</td></tr>
</table>

4. Click the **Apply** button.

   Your changes are saved.

DMZ Port for IPv6 Traffic

You can 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 13) 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, two DHCPv6 server options are available:

- **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 must configure the RADVD and advertisement prefixes. For more information, see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the DMZ* on page 106.

- **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 must configure IPv6 address pools. For more information, see *IPv6 DMZ Address Pools* on page 104.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

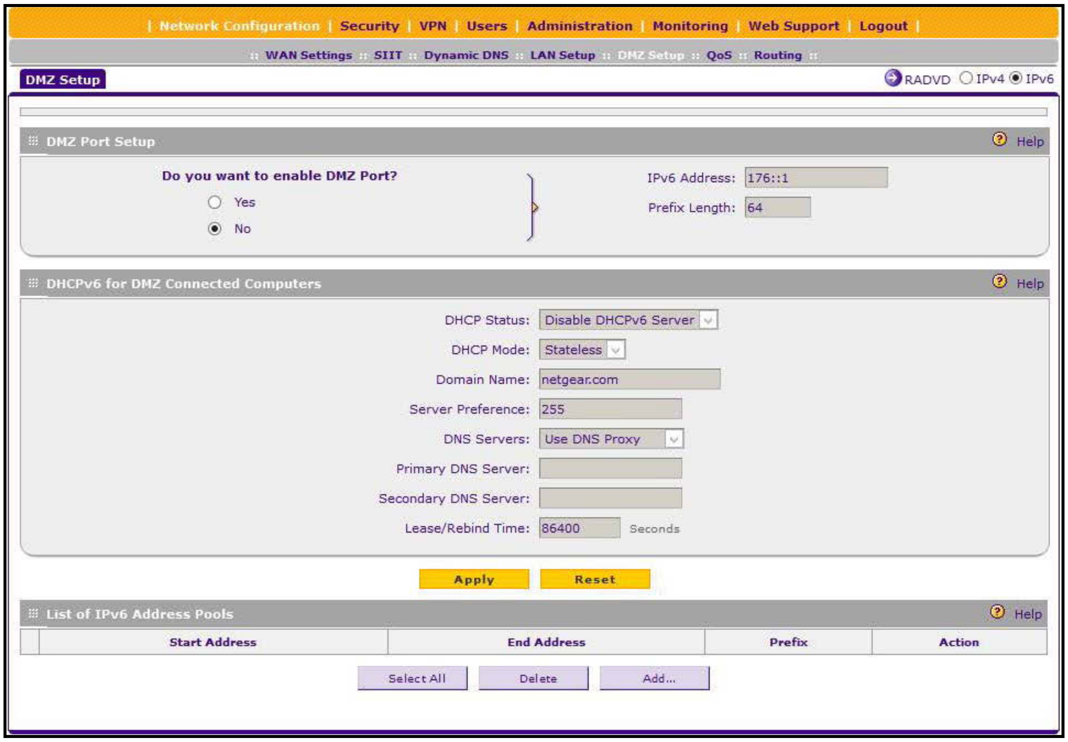
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
DMZ Setup
RADVD ○ IPv4 ● IPv6
Help
Apply
Reset
Select All
Delete
Add...

DMZ Port Setup

Do you want to enable DMZ Port?
○ Yes
● No

IPv6 Address: 176::1
Prefix Length: 64

DHCPv6 for DMZ Connected Computers

DHCP Status: Disable DHCPv6 Server
DHCP Mode: Stateless
Domain Name: netgear.com
Server Preference: 255
DNS Servers: Use DNS Proxy
Primary DNS Server:
Secondary DNS Server:
Lease/Rebind Time: 86400 Seconds

List of IPv6 Address Pools

	Start Address	End Address	Prefix	Action

4. 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. Complete the **IP Address** and **Subnet Mask** fields. • **No**. Allows you to disable the DMZ port after you configure 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.

Table 19. DMZ Setup screen settings for IPv6 (continued)

Setting	Description	
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 must complete the DHCPv6 fields.	
	DHCP Mode	Select a DHCPv6 mode: • **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 must configure the RADVD and advertisement prefixes (see *Configure the IPv6 Router Advertisement Daemon and Advertisement Prefixes for the DMZ* on page 106). • **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 104).
	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 lists: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers that you configured on the Broadband ISP Settings (IPv6) screen (see *Configure a Static IPv6 Internet Connection* on page 42). • **Use DNS from ISP**. The 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).	

5. Click the **Apply** button.

   Your changes are saved.

IPv6 DMZ Address Pools

If you configure a stateful DHCPv6 server for the DMZ, you must 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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.
4. Under the List of IPv6 Address Pools table, click the **Add** button.
5. 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.

6. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.
4. In the Action column for the address pool that you want to modify, click the **Edit** button.

   The DMZ IPv6 Config screen displays.

5. Modify the settings as described in *Table 20* on page 105.
6. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays.
3. In the upper right of the screen, select the **IPv6** radio button.
4. 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.
5. Click the **Delete** table button.

   The information is deleted.

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 must configure the Router Advertisement Deamon (RADVD) and advertisement prefixes.

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

Hosts and routers in the LAN use NDP to determine the link-layer addresses and related information of neighbors in the LAN that can forward packets on their behalf. The VPN firewall periodically distributes router advertisements (RAs) throughout the DMZ to provide such information to the hosts and routers in the DMZ. RAs include IPv6 addresses, types of prefixes, prefix addresses, prefix lifetimes, the maximum transmission unit (MTU), and so on. In addition to configuring the RADVD, you also must 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 configure 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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays.

3. Select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings.

4. Click the **RADVD** option arrow.
5. Enter the settings as described in the following table:

Table 22. RADVD screen settings for the DMZ

Setting	Description
RADVD Status	Select the RADVD status: • **Enable**. The RADVD is enabled, and the RADVD fields become available. • **Disable**. The RADVD is disabled, and the RADVD fields are masked out. This is the default setting.
Advertise Mode	Select the advertisement mode: • **Unsolicited Multicast**. The VPN firewall advertises unsolicited multicast packets at a rate that is specified by the advertisement interval. • **Unicast only**. The VPN firewall responds to unicast packet requests only. No unsolicited packets are advertised. Select this option for nonbroadcast multiple access (NBMA) links such as ISATAP.
Advertise Interval	Enter the advertisement interval of unsolicited multicast packets in seconds. The minimum value is 10 seconds; the maximum value is 1800 seconds.
RA Flags	Select what type of information the DHCPv6 server provides in the DMZ: • **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	Select the VPN firewall’s preference in relation to other hosts and routers in the DMZ: • **Low**. The VPN firewall is treated as a nonpreferred router in the DMZ. • **Medium**. The VPN firewall is treated as a neutral router in the DMZ. • **High**. The VPN firewall is treated as a preferred router in the DMZ.
MTU	The maximum transmission unit (MTU) size for a packet in one transmission over a link. The default setting is 1500.
Router Lifetime	The router lifetime specifies how long the default route that was created as a result of the router advertisement remains 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.

6. Click the **Apply** button.

   Your changes are saved.

Advertisement Prefixes for the DMZ

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

➢ To add an advertisement prefix for the DMZ:

1. Log in to the unit:
    a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

       The NETGEAR Configuration Manager Login screen displays.

    b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

       Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

    c. Click the **Login** button.

       The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays.

3. Select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings.

4. Click the **RADVD** option arrow.
5. Under the List of Prefixes to Advertise table, click the **Add** button.
6. Enter the settings as described in the following table:

Table 23. Add Advertisement Prefix screen settings for the DMZ

Setting	Description
IPv6 Prefix Type	Select the IPv6 prefix type: • **6to4**. The prefix is for a 6to4 address. You must 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 must be a global prefix or a site-local prefix; it cannot be a link-local prefix. You must 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 to be included in the advertisement.
IPv6 Prefix	Enter the IPv6 prefix for the VPN firewall's DMZ to be included in the advertisement.
IPv6 Prefix Length	Enter the IPv6 prefix length (typically 64) to 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 remains valid. Enter the prefix lifetime in seconds to be included in the advertisement. The minimum period is 0 seconds; the maximum period is 65536 seconds.

7. Click the **Apply** button.

   Your changes are saved.

➢ **To edit an advertisement prefix:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays.
3. Select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings.
4. Click the **RADVD** option arrow.
5. In the Action column for the advertisement prefix that you want to modify, click the **Edit** button.

   The Add Advertisement Prefix screen displays.
6. Modify the settings as described in *Table 23* on page 109.
7. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays.

3. Select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings.

4. Click the **RADVD** option arrow.
5. 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.
6. Click the **Delete** table button.

   The information is deleted.

Manage Static IPv4 Routing

Static routes provide additional routing information to your VPN firewall. Under normal circumstances, the VPN firewall is provided with adequate routing information after it is configured for Internet access, and you do not need to configure additional static routes. Configure static routes only for unusual cases such as multiple firewalls or multiple IP subnets on your network.

The VPN firewall automatically sets up routes between VLANs and secondary IPv4 addresses that you configured on the LAN Multi-homing (IPv4) screen. For more information, see *Configure IPv4 Multihome LAN IP Addresses on the Default VLAN* on page 69. Therefore, you do not need to manually add an IPv4 static route between a VLAN and a secondary IPv4 address.

This section contains the following topics:

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

Configure Static IPv4 Routes

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

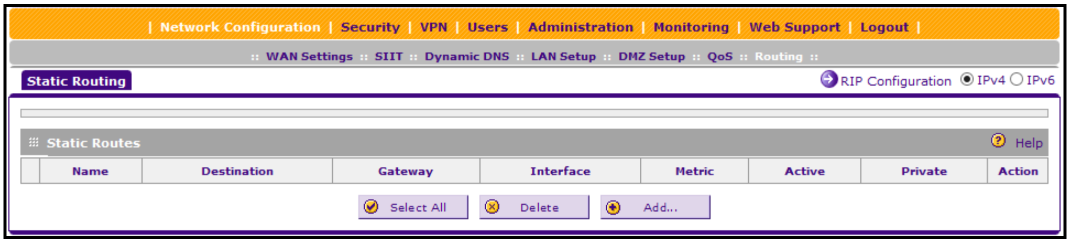
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

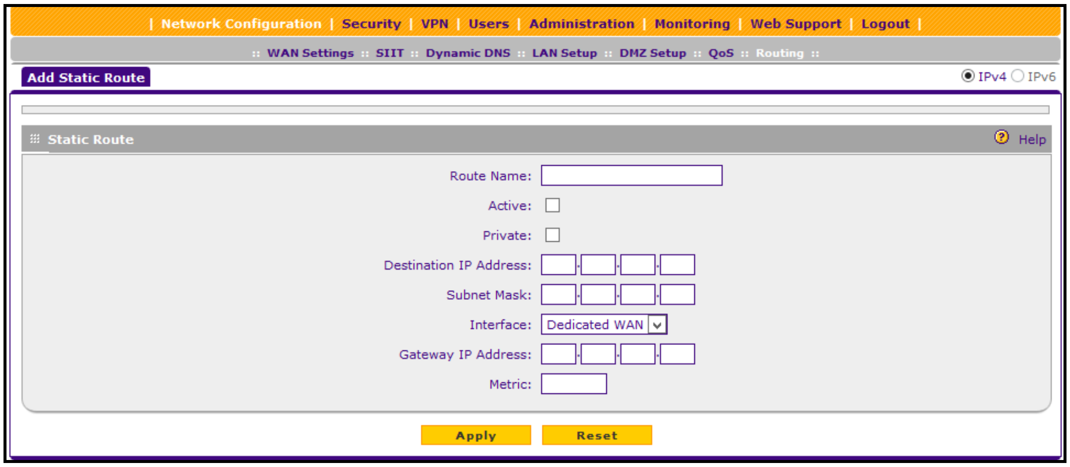
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > Routing**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Static Routing
RIP Configuration ● IPv4 ○ IPv6
Static Routes
Help
Name
Destination
Gateway
Interface
Metric
Active
Private
Action
Select All
Delete
Add...

3. Click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Add Static Route
● IPv4 ○ IPv6
Static Route
Help
Route Name:
Active: □
Private: □
Destination IP Address:
Subnet Mask:
Interface: Dedicated WAN
Gateway IP Address:
Metric:
Apply
Reset

4. 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 entries. 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	Select the physical or virtual network interface (WAN, VLAN, or DMZ interface) through which the route is accessible.

Table 24. Add Static Route screen settings for IPv4 (continued)

Setting	Description
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.

5. Click the **Apply** button.

   Your changes are saved.

➢ To edit an IPv4 static route:

1. Log in to the unit:
   - a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - c. Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > Routing**.

   The Static Routing screen displays.
3. In the Action column for the route that you want to modify, click the **Edit** button.

   The Edit Static Route screen displays. This screen is identical to the Add Static Route screen.
4. Modify the settings as described in *Table 24* on page 112.
5. Click the **Apply** button.

   Your changes are saved.

➢ To delete one or more routes:

1. Log in to the unit:
   - a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > Routing**.

The Static Routing screen displays.

3. 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.
4. Click the **Delete** table button.

The information is deleted.

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. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

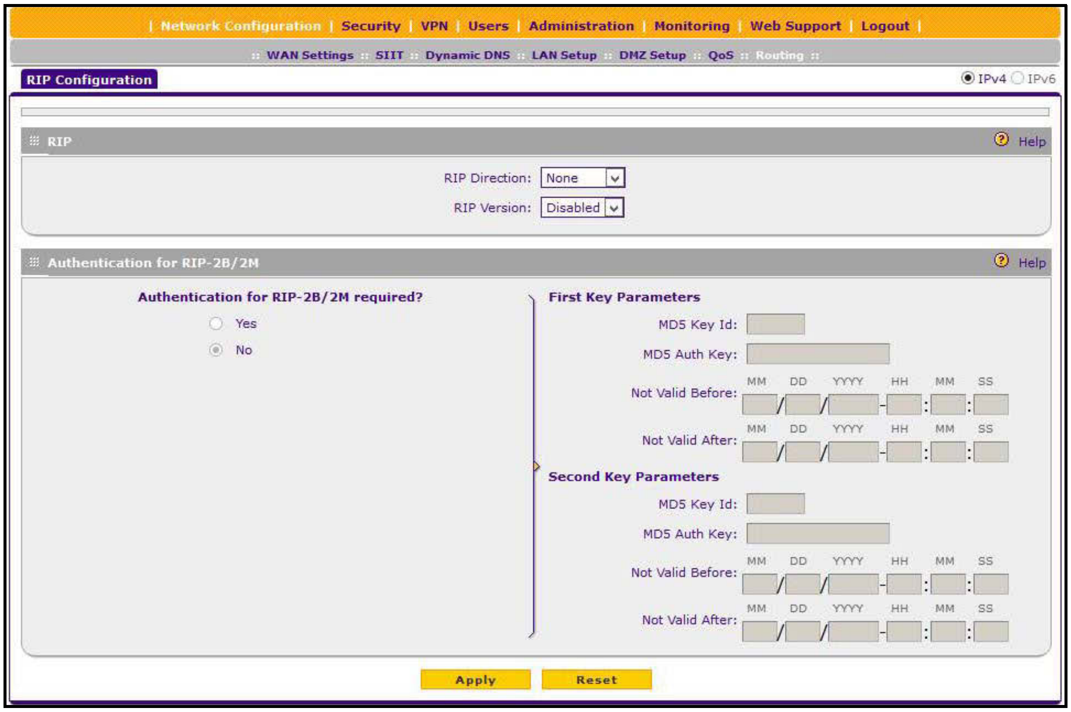
c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > Routing**.

The Static Routing screen displays.

3. Click the **RIP Configuration** option arrow.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
RIP Configuration
Help
Help
Apply
Reset

● IPv4 ○ IPv6

RIP

RIP Direction: None

RIP Version: Disabled

Authentication for RIP-2B/2M

Authentication for RIP-2B/2M required?

○ Yes

● No

First Key Parameters

MD5 Key Id:

MD5 Auth Key:

Not Valid Before: MM / DD / YYYY - HH : MM : SS

Not Valid After: MM / DD / YYYY - HH : MM : SS

Second Key Parameters

MD5 Key Id:

MD5 Auth Key:

Not Valid Before: MM / DD / YYYY - HH : MM : SS

Not Valid After: MM / DD / YYYY - HH : MM : SS

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

Table 25. RIP Configuration screen settings

Setting	Description
RIP	
RIP Direction	Select the direction in which the VPN firewall sends and receives RIP packets: • **None**. The VPN firewall neither advertises its routing table nor accepts any RIP packets from other routers. This effectively disables RIP and is the default setting. • **In Only**. The VPN firewall accepts RIP information from other routers but does not advertise its routing table. • **Out Only**. The VPN firewall advertises its routing table but does not accept RIP information from other routers. • **Both**. The VPN firewall advertises its routing table and also processes RIP information received from other routers.
RIP Version	By default, the RIP version is set to **Disabled**. From the RIP Version 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.

Table 25. RIP Configuration screen settings (continued)

Setting	Description	
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.

5. Click the **Apply** button.

   Your changes are saved.

IPv4 Static Route Example

In this example, assume the following:

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

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

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

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

In this case, you must define a static route, informing the VPN firewall that the 134.177.0.0 IP address is to be accessed through the local LAN IP address (192.168.1.100).

The static route on the VPN firewall must be defined as follows:

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

Manage Static IPv6 Routing

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

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

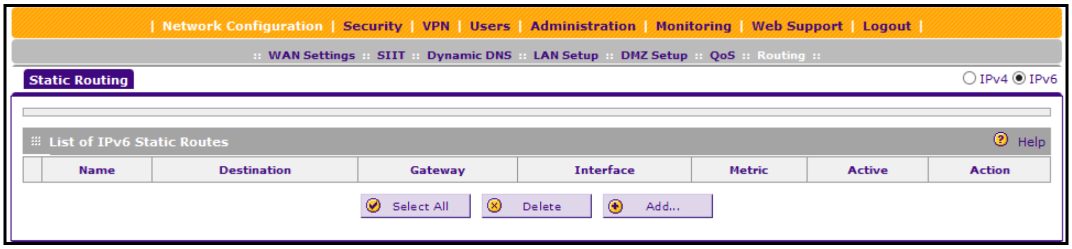
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > Routing**.

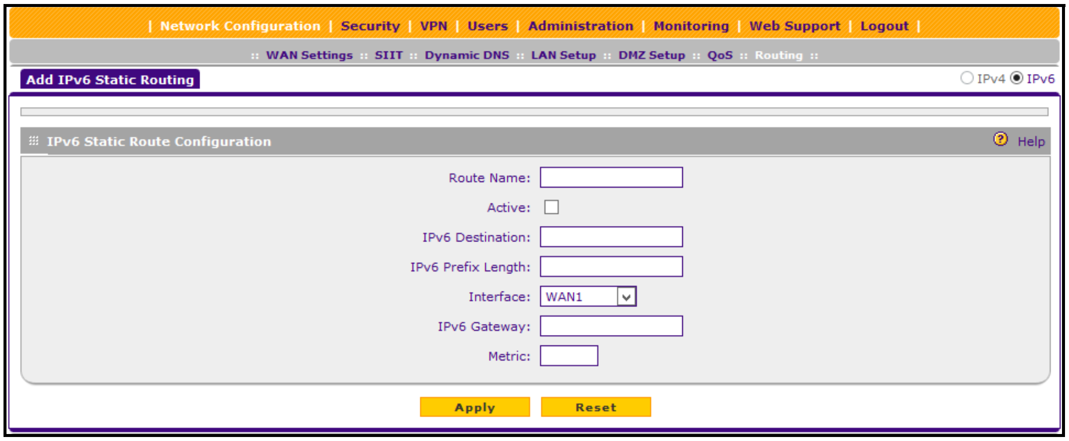
   The Static Routing screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Static Routing
○ IPv4 ● IPv6
List of IPv6 Static Routes
Help
Select All
Delete
Add...

	Name	Destination	Gateway	Interface	Metric	Active	Action

4. Click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Add IPv6 Static Routing
○ IPv4 ● IPv6
IPv6 Static Route Configuration
Help
Apply
Reset

Route Name:

Active: □

IPv6 Destination:

IPv6 Prefix Length:

Interface: WAN1

IPv6 Gateway:

Metric:

5. 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 entries.
IPv6 Destination	The destination IPv6 address of the host or network to which the route leads.
IPv6 Prefix Length	The destination IPv6 prefix length of the host or network to which the route leads.
Interface	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.

6. Click the **Apply** button.

Your changes are saved.

➢ To edit an IPv6 static route:

1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > Routing**.

   The Static Routing screen displays.
3. Select the **IPv6** radio button.
4. In the Action column for the route that you want to modify, click the **Edit** button.

   The Edit IPv6 Static Routing screen displays. This screen is identical to the Add IPv6 Static Routing screen.
5. Modify the settings as described in *Table 26* on page 118.
6. Click the **Apply** button.

   Your changes are saved.

➢ To delete one or more routes:

1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > Routing**.

   The Static Routing screen displays.
3. Select the **IPv6** radio button.

4. 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.
5. Click the **Delete** table button.

   The information is deleted.

Configure Quality of Service

QoS refers to the capability of providing better service to selected network traffic. Bandwidth allocation or priority can be assigned for individual traffic to ensure service quality. The router provides the following two types of QoS functionality for transmitting packets through the WAN ports:

- **Rate Control**. Guarantees both minimum bandwidth and maximum bandwidth through each WAN port.
- **Priority**. Sets a priority for each different service.

The QoS screen also displays the configured Network QoS profiles in the router. A QoS profile is active if the QoS type of the profile matches the Global QoS type for the network.

➤ **To enable or disable quality of service:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

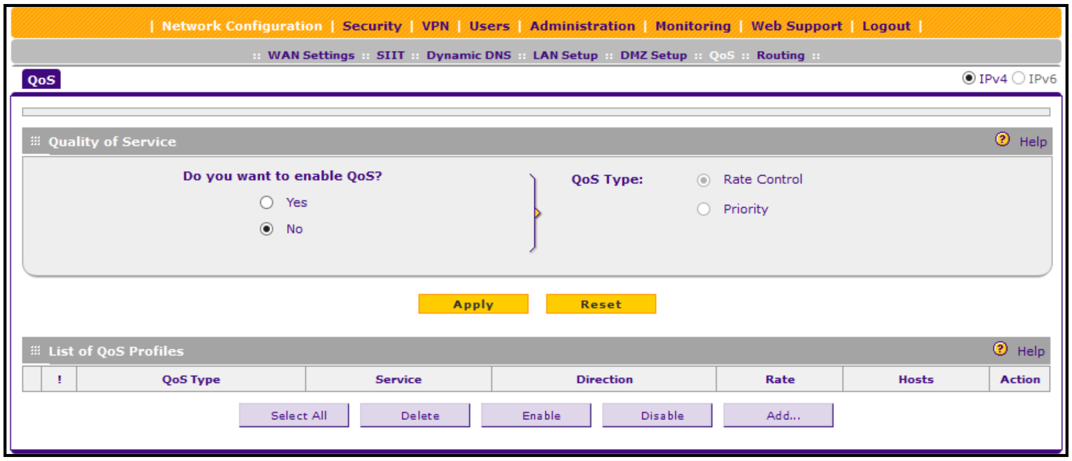
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > QoS**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
QoS
● IPv4 ○ IPv6
Quality of Service
Help
Apply
Reset
List of QoS Profiles
Help
Select All
Delete
Enable
Disable
Add...

Do you want to enable QoS?
○ Yes
● No

QoS Type: ● Rate Control ○ Priority

	!	QoS Type	Service	Direction	Rate	Hosts	Action

3. To enable QoS, under Do you want to enable QoS, select the **Yes** radio button.
4. To select the QoS type, next to **QoS Type**, select either the **Rate Control** or the **Priority** radio button.

   If **Rate Control** is selected as the the QoS type, then only rate control QoS profiles are active.

   If **Priority** is selected as the QoS type, then only priority QoS profiles are active.
5. Under the List of QoS Profiles table, select the QoS profiles that you want to enable or disable and click either the **Enable** button or the **Disable** button.
6. Click the **Apply** button.

   Your changes are saved.

➢ To add a QoS profile:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

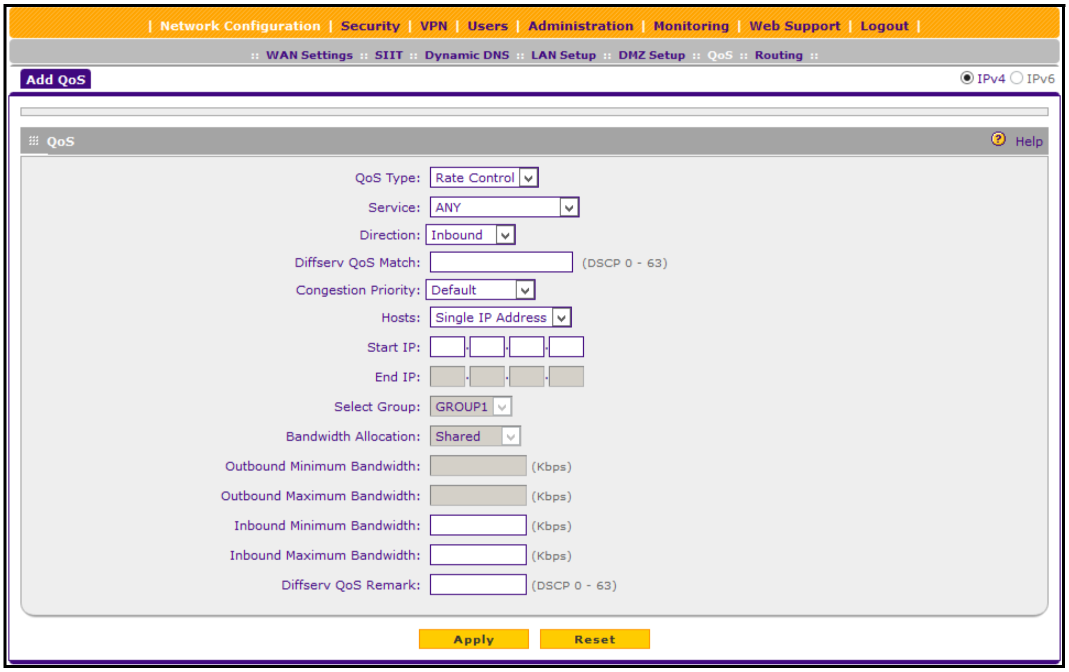
   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > QoS**.

   The QoS screen displays.

3. Under the List of QoS Profiles table, click the **Add** button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
Add QoS
● IPv4 ○ IPv6
QoS
Help
Apply
Reset

QoS Type: Rate Control
Service: ANY
Direction: Inbound
Diffserv QoS Match: (DSCP 0 - 63)
Congestion Priority: Default
Hosts: Single IP Address
Start IP:
End IP:
Select Group: GROUP1
Bandwidth Allocation: Shared
Outbound Minimum Bandwidth: (Kbps)
Outbound Maximum Bandwidth: (Kbps)
Inbound Minimum Bandwidth: (Kbps)
Inbound Maximum Bandwidth: (Kbps)
Diffserv QoS Remark: (DSCP 0 - 63)

Enter the settings as described in the following table.

Table 27. QoS profile configuration settings

Setting	Description
QoS Type	Select either **Rate Control** or **Priority**.
Service	Select the type of traffic for you want to perform rate control.
Direction	Select the direction of traffic: • **Outbound**. Controls the LAN client’s upstream bandwidth. • **Outbound**. Controls the LAN client’s upstream bandwidth. • **Both**. Controls the LAN client’s upstream and downstream bandwidth.
Diffserv QoS Match	The VPN firewall configures the QoS packet when the packet matches the selected option. For DSCP the value must be between 0 and 63. DSCP match is disabled if the value is 0. Leave the field blank if the match is not required.
Congestion priority (Rate control)	This affects how the excess bandwidth is distributed among rules. The rules with higher priority are offered excess bandwidth first, and rules about minimum and maximum rates are still met.
Priority (Priority)	Select the level of priority, either **High (60%)** or **Low (10%)**.
Hosts	Specifies whether a group or one or more IP addresses on the LAN is affected by the rule. This rule affects packets for the selected service from the defined group or range of IP addresses on the LAN side.
Single Address	A single LAN IP address is affected by the rule.
Address Range	A range of LAN IP addresses is affected by the rule.

Table 27. QoS profile configuration settings (continued)

Setting	Description
Group	Computers that are part of the group defined in the network database are affected by the rule.
Start	Enter the starting address for a single address or a range of IP addresses.
End	Enter the end address for a range of IP addresses. This field is not active for a single address.
Select Group	Predefined group of network clients.
Bandwidth allocation	Two modes are available: • **Shared**. All clients share this bandwidth for the particular service. • **Individual**. This bandwidth is allotted for each client for the particular service.
Outbound Minimum Bandwidth	Specify the minimum bandwidth value in Kbps for the profile for the outbound direction.
Outbound Maximum Bandwidth	Specify the maximum bandwidth value in Kbps for the profile for the outbound direction.
Inbound Minimum Bandwidth	Specify the minimum bandwidth value in Kbps for the profile for the inbound direction.
Inbound Maximum Bandwidth	Specify the maximum bandwidth value in Kbps for the profile for the inbound direction.
Diffserv QoS Remark	Enter a remark to be added to the QoS packet when the packet matches the option you specified in the **Diffserv QoS Match** field. Leave the field blank if no DSCP marking is to be done.

4. Click the **Apply** button.

   Your changes are saved.

➤ To edit a QoS profile:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > QoS**.

   The QoS screen displays.

3. Select the QoS profile that you want to modify and click the **Edit** button.
4. Modify the settings as described in *Table 27* on page 122.
5. Click the **Apply** button.S

   Your changes are saved.

➢ To delete a QoS profile:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > QoS**.

   The QoS screen displays.

3. Under the List of QoS Profiles table, select the QoS profile that you want to delete or click the **Select All** table button to select all routes.
4. Click the **Delete** table button.

   The information is deleted.

Firewall Protection

4

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

About Firewall Protection

A firewall protects one network (the trusted network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. You can further segment keyword blocking to certain known groups. For information about how to set up LAN groups, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 71.

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 must manage distant sites from a central location.

   For more information, see *Configure Authentication Domains, Groups, and Users* on page 287 and *Configure Remote Management Access* on page 328.

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 127), you can further refine your control using the following features and capabilities of the VPN firewall:
   - **Groups and hosts**. See *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 71.
   - **Services**. See *Outbound Rules* on page 128 and *Inbound Rules* on page 130.
   - **Schedules**. See *Set a Schedule to Block or Allow Specific Traffic* on page 195.
   - **Allowing or blocking sites**. See *Configure Content Filtering* on page 189.
   - **Source MAC filtering**. See *Enable Source MAC Filtering* on page 196.
   - **Port triggering**. See *Configure Port Triggering* on page 206.

3. Some firewall settings might affect the performance of the VPN firewall.

   For more information, see *Performance Management* on page 320.

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 353.

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 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 access.

A firewall is configured with two default rules, one for inbound traffic and one for outbound. The default rules of the VPN firewall are as follows:

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

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

Table 28. 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 176).
- **Quality of Service (QoS) priorities**. Each service is assigned 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 183).
- **Bandwidth profiles**. After you configure a bandwidth profile (see *Create Bandwidth Profiles* on page 180), you can assign it to a rule.

This section contains the following topics:

- *Outbound Rules*

- *Inbound Rules*
- *Order of Precedence for Rules*

Outbound Rules

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

The following table describes the fields that define the rules for outbound traffic and that are common to most Outbound Service screens.

Table 29. 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 must define it using the Services screen (see *Add Customized Services* on page 176).	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
Select Schedule	The time schedule (that is, **Schedule1**, **Schedule2**, or **Schedule3**) that is used by this rule. • This 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 195).	All rules when **BLOCK by schedule, otherwise allow** or **ALLOW by schedule, otherwise block** is selected as the action.
LAN Users	Select which computers on your network are affected by this rule: • **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 73). Groups are applicable only to IPv4 rules.	LAN WAN rules LAN DMZ rules

Table 29. Outbound rules overview (continued)

Setting	Description	Outbound Rules
WAN Users	Select which Internet locations are covered by the rule, based on their IP address: • **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	Select which DMZ computers on the DMZ network are affected by this rule: • **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 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 183. **Note:** The VPN firewall is preconfigured with 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
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 180. 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

Table 29. Outbound rules overview (continued)

Setting	Description	Outbound Rules
Log	Select whether packets covered by this rule are logged: • **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	Select whether the source address of the outgoing packets on the WAN are assigned the address of the WAN interface or the address of a different interface. You can specify the following settings only for outbound traffic of the WAN interface: • **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 configured. **Note:** The **NAT IP** list is available only when the WAN mode is NAT. If you select **Single Address**, the IP address specified must fall under the WAN subnet.	IPv4 LAN WAN rules IPv4 DMZ WAN rules

For yet another way to block outbound traffic from selected computers that would otherwise be allowed by the firewall, see *Enable Source MAC Filtering* on page 196.

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

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

Inbound Rules

If you 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 27.

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. Enable only 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. For more information, see *Configure Dynamic DNS* on page 35.

- 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. For more information, see *Set Up DHCP Address Reservation* on page 78.

- Local computers must 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.
- For yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall. For more information, see *Configure Port Triggering* on page 206.
- The VPN firewall always blocks denial of service (DoS) attacks. A DoS attack does not attempt to steal data or damage your computers, but overloads your Internet connection so that you cannot use it (that is, the service becomes unavailable).
- 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 169), multiple concurrent connections of the same application from one host or IP address (such as multiple DNS queries from one computer) trigger the VPN firewall's DoS protection.

The following table describes the fields that define the rules for inbound traffic and that are common to most Inbound Service screens.

Table 30. 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 must define it using the Services screen (see *Add Customized Services* on page 176).	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

Table 30. Inbound rules overview (continued)

Setting	Description	Inbound Rules
Select Schedule	The **time** schedule (that is, **Schedule1**, **Schedule2**, or Schedule3) that is used by this rule. • This 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 195).	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.) Select an option: • **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 specify this setting and specify a port number. If the service is using the default port, you do not need to enable this feature.	IPv4 LAN WAN rules IPv4 DMZ WAN rules
WAN Destination IP Address	The setting that determines the destination IP address applicable to incoming traffic. This is the public IP address that maps to the internal LAN server. This can be either the address of the WAN interface or another public IP address. You can also enter an address range. Enter the required addresses in the **Start** and **Finish** fields to apply the rule to a range of devices.	IPv4 LAN WAN rules IPv4 DMZ WAN rules
LAN Users	This setting applies to a LAN WAN inbound rule when the WAN mode is classical routing and determines which computers on your network are affected by this rule. Select an option: • **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 73). 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

Table 30. Inbound rules overview (continued)

Setting	Description	Inbound Rules
WAN Users	Select which Internet locations are covered by the rule, based on their IP address: • **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	Select which DMZ computers on the DMZ network are affected by this rule: • **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	Select whether packets covered by this rule are logged: • **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
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 180. 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

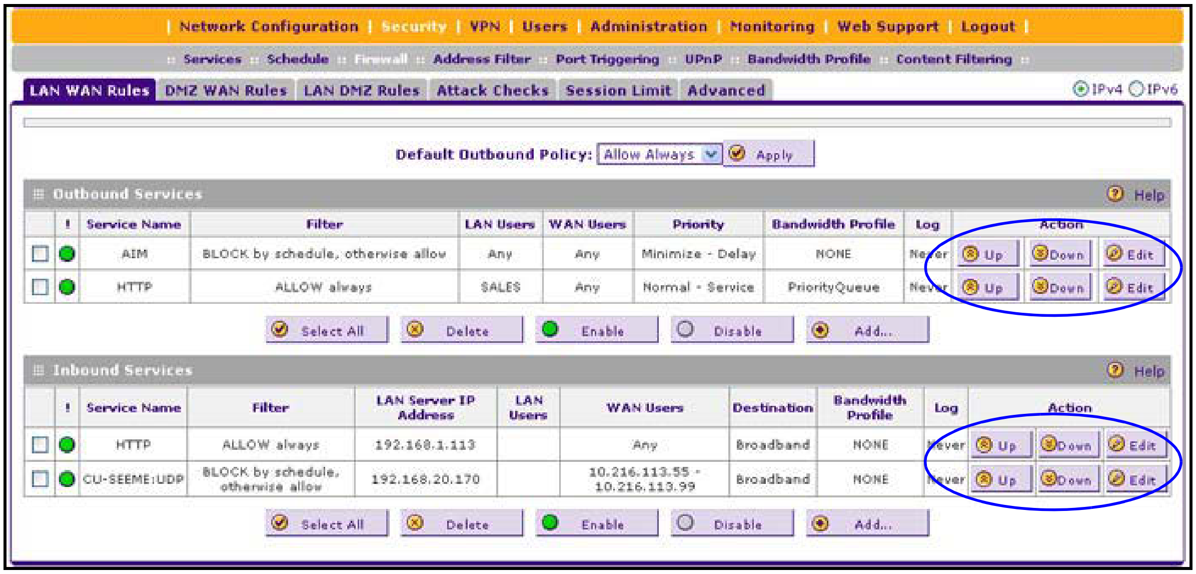
Note: Some residential broadband ISPs do not allow you to run any server processes (such as a web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active servers at your location. If you are unsure, see the acceptable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

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

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

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:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
● IPv4 ○ IPv6
Apply
Help
Select All
Delete
Enable
Disable
Add...

Default Outbound Policy: Allow Always

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Bandwidth Profile	Log	Action
□	●	AIM	BLOCK by schedule, otherwise allow	Any	Any	Minimize - Delay	NONE	Never	Up Down Edit
□	●	HTTP	ALLOW always	SALES	Any	Normal - Service	PriorityQueue	Never	Up Down Edit

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Bandwidth Profile	Log	Action
□	●	HTTP	ALLOW always	192.168.1.113		Any	Broadband	NONE	Never	Up Down Edit
□	●	CU-SEEME:UDP	BLOCK by schedule, otherwise allow	192.168.20.170		10.216.113.55 - 10.216.113.99	Broadband	NONE	Never	Up Down Edit

Figure 9. Order of preference

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

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

This section contains the following topics:

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

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

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

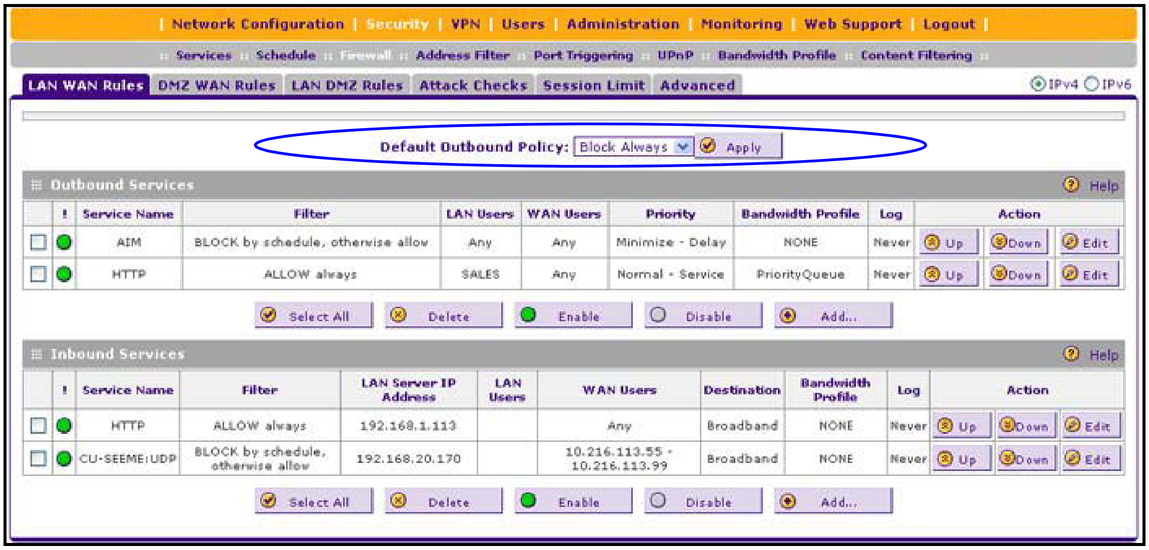
b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
⦿ IPv4 ○ IPv6
Apply
Help
Select All
Delete
Enable
Disable
Add...

Default Outbound Policy: Block Always

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Bandwidth Profile	Log	Action		
□	●	AIM	BLOCK by schedule, otherwise allow	Any	Any	Minimize - Delay	NONE	Never	Up	Down	Edit
□	●	HTTP	ALLOW always	SALES	Any	Normal - Service	PriorityQueue	Never	Up	Down	Edit

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Bandwidth Profile	Log	Action		
□	●	HTTP	ALLOW always	192.168.1.113		Any	Broadband	NONE	Never	Up	Down	Edit
□	●	CU-SEEME:UDP	BLOCK by schedule, otherwise allow	192.168.20.170		10.216.113.55 - 10.216.113.99	Broadband	NONE	Never	Up	Down	Edit

3. From the **Default Outbound Policy** list, select **Block Always**.

   By default, **Allow Always** is selected.

4. Click the **Apply** button.

   Your changes are saved.

5. 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
     - Edit LAN WAN Inbound Service screen for IPv4

6. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

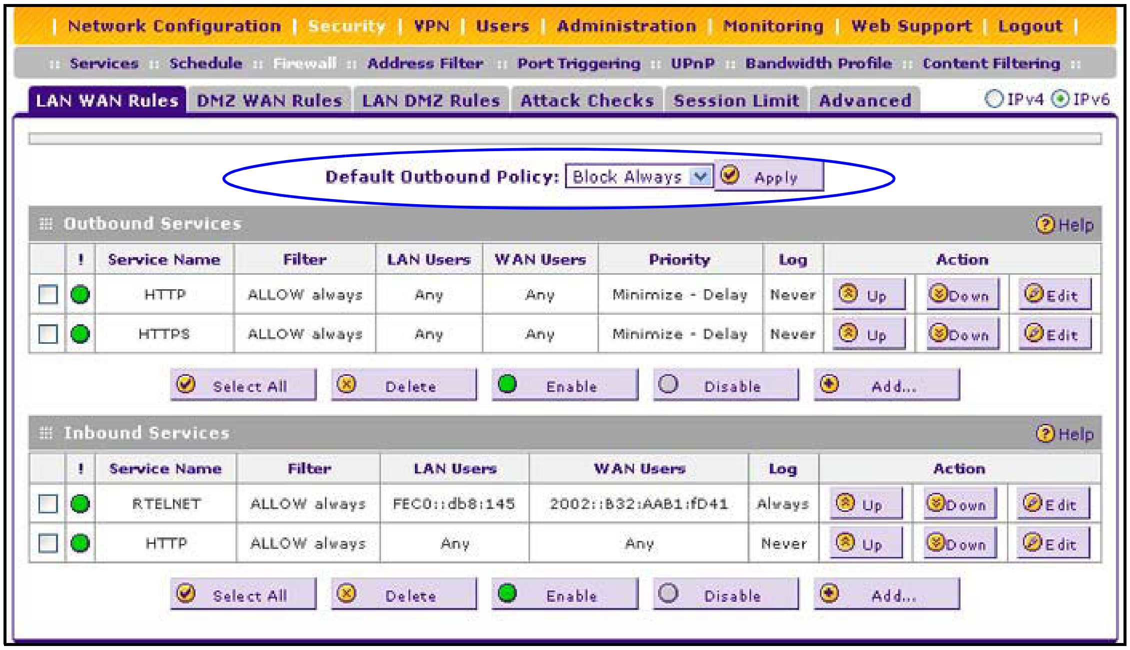
   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen for IPv4 in view.

3. In the upper right of the screen, select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
○ IPv4 ● IPv6
Apply
Help
Select All
Delete
Enable
Disable
Add...

Default Outbound Policy: Block Always

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action		
□	●	HTTP	ALLOW always	Any	Any	Minimize - Delay	Never	Up	Down	Edit
□	●	HTTPS	ALLOW always	Any	Any	Minimize - Delay	Never	Up	Down	Edit

Inbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Log	Action		
□	●	RTELNET	ALLOW always	FEC0::db8:145	2002::B32:AAB1:fD41	Always	Up	Down	Edit
□	●	HTTP	ALLOW always	Any	Any	Never	Up	Down	Edit

4. From the **Default Outbound Policy** list, select **Block Always**.

   By default, **Allow Always** is selected.

5. Click the **Apply** button.

   Your changes are saved.

6. 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
  - Edit LAN WAN Inbound Service screen for IPv6

7. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall**.

   The LAN WAN Rules screen displays.

3. 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.
4. 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.
5. Click the **Apply** button.

   Your changes are saved.

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 126).

IPv4 LAN WAN Outbound Rules

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

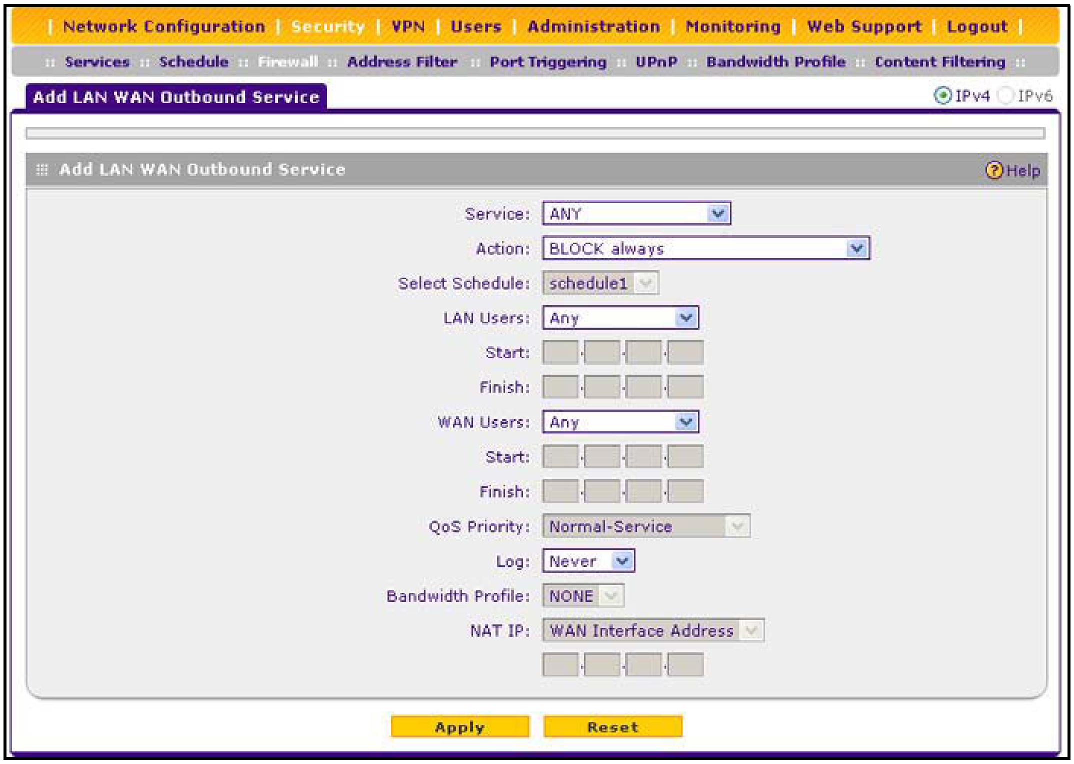
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall**.

   The LAN WAN Rules screen displays. In the upper right of the LAN WAN Rules screen, the **IPv4** radio button is selected by default. The screen displays the IPv4 settings.

3. Click the **Add** table button under the Outbound Services table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Outbound Service
● IPv4 ○ IPv6
Help
Apply
Reset

Add LAN WAN Outbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	schedule1
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
QoS Priority:	Normal-Service
Log:	Never
Bandwidth Profile:	NONE
NAT IP:	WAN Interface Address

4. Enter the settings as described in *Table 29* on page 128.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **LAN Users**
   - **WAN Users**

   Unless your selection from the **Action** list is **BLOCK always**, you also must make selections from the following lists:

   - **Select Schedule**
   - **QoS Priority**
   - **Bandwidth Profile**
   - **NAT IP** (This ist is available only when the WAN mode is NAT. If you select **Single Address**, the IP address specified must fall under the WAN subnet.)

5. Click the **Apply** button.

   Your changes are saved.

IPv6 LAN WAN Outbound Rules

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

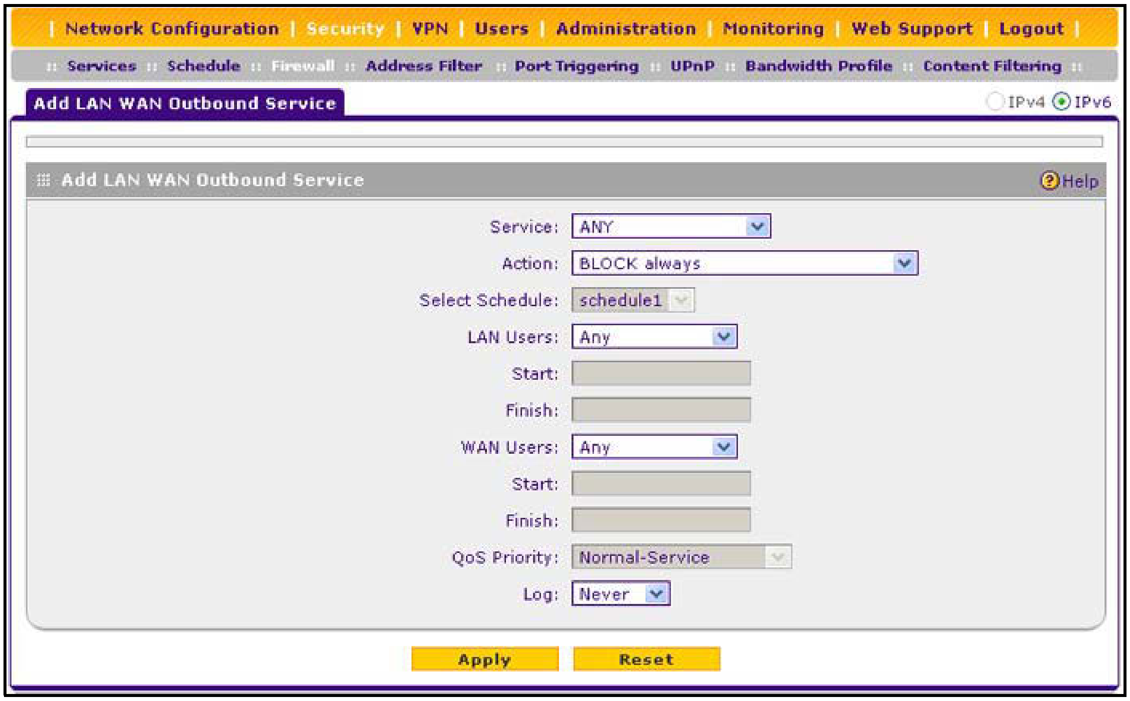
2. Select **Security > Firewall**.

The LAN WAN Rules screen displays.

3. In the upper right of the LAN WAN Rules screen, select the **IPv6** radio button.

The screen displays the IPv6 settings.

4. Click the **Add** table button under the Outbound Services table.



Add LAN WAN Outbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	schedule1
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
QoS Priority:	Normal-Service
Log:	Never

5. Enter the settings as described in *Table 29* on page 128. In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:
   - **LAN Users**
   - **WAN Users**

   Unless your selection from the **Action** list is **BLOCK always**, you also must make a selection from the following lists:

   - **Select Schedule**
   - **QoS Priority**

6. Click the **Apply** button.

   Your changes are saved.

Create LAN WAN Inbound Service Rules

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

⚠ **WARNING:**

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

IPv4 LAN WAN Inbound Service Rules

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

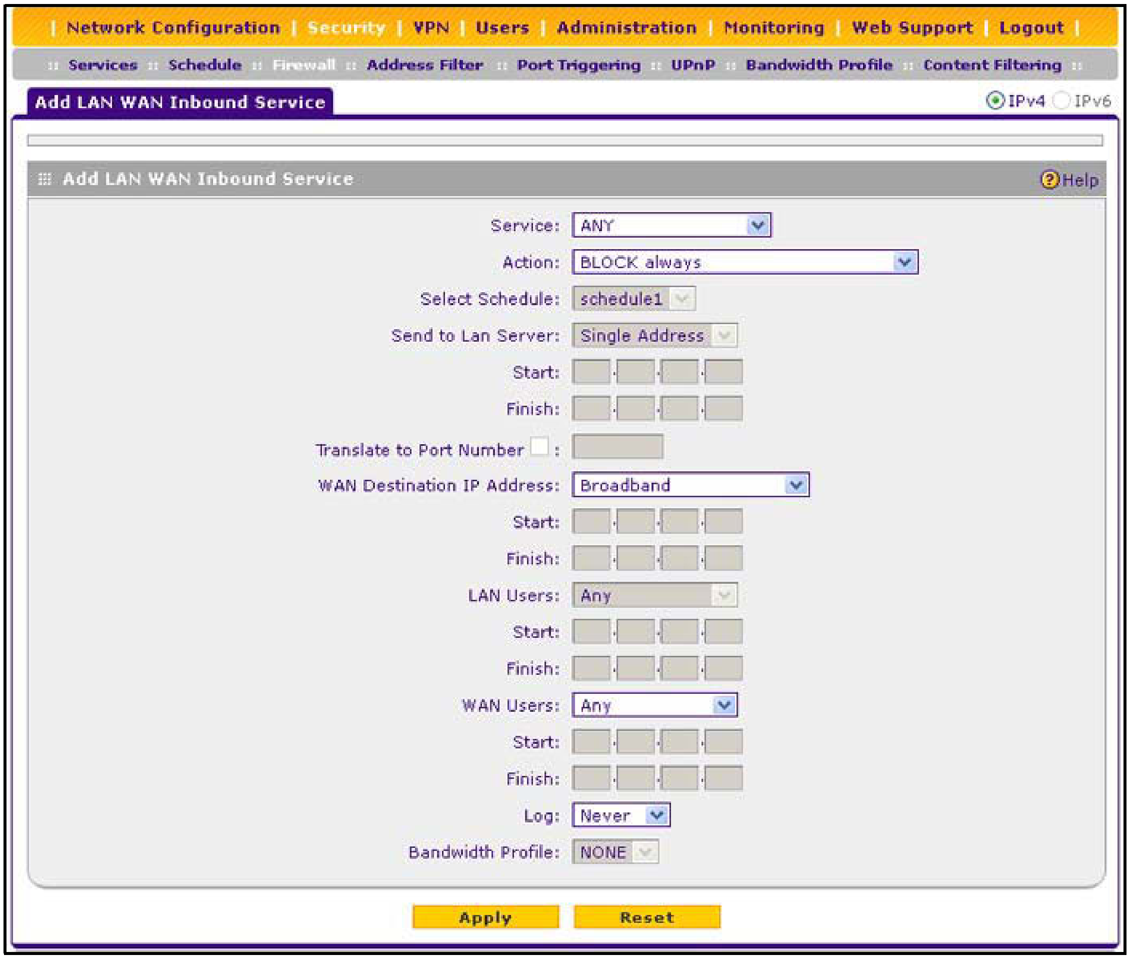
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall**.

   The LAN WAN Rules screen displays. In the upper right of the LAN WAN Rules screen, the **IPv4** radio button is selected by default. The screen displays the IPv4 settings.

3. Under the Inbound Services table, click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
● IPv4 ○ IPv6
Help
Apply
Reset

Add LAN WAN Inbound Service

Add LAN WAN Inbound Service

Service: ANY

Action: BLOCK always

Select Schedule: schedule1

Send to Lan Server: Single Address

Start:

Finish:

Translate to Port Number □ :

WAN Destination IP Address: Broadband

Start:

Finish:

LAN Users: Any

Start:

Finish:

WAN Users: Any

Start:

Finish:

Log: Never

Bandwidth Profile: NONE

4. Enter the settings as described in *Table 30* on page 131.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **WAN Destination IP Address**
   - **LAN Users** (This 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** list is **BLOCK always**, you also must make selections from the following lists:

   - **Select Schedule**
   - **Send to Lan Server**

   The following configuration is optional:

   - **Translate to Port Number**
   - **Bandwidth Profile**

5. Click the **Apply** button.

   Your changes are saved.

IPv6 LAN WAN Inbound Rules

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

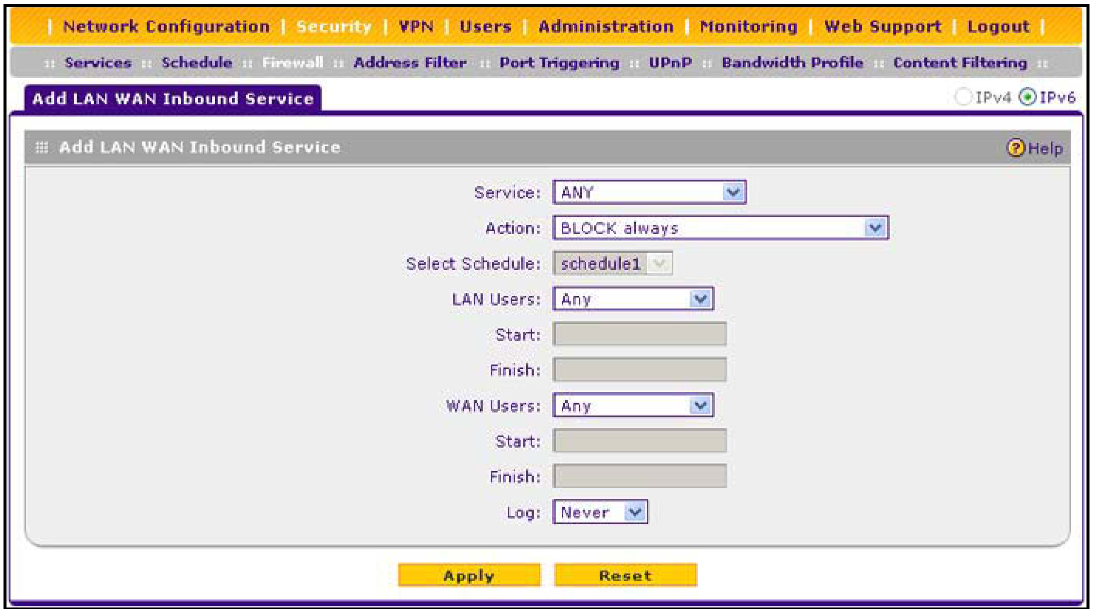
2. Select **Security > Firewall**.

   The LAN WAN Rules screen displays.

3. In the upper right of the LAN WAN Rules screen, select the **IPv6** radio button.

   The screen displays the IPv6 settings.

4. Under the Inbound Services table, click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Inbound Service
○ IPv4 ● IPv6
Help
Apply
Reset

Add LAN WAN Inbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	schedule1
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
Log:	Never

5. Enter the settings as described in *Table 30* on page 131.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

- **LAN Users**
- **WAN Users**

Unless your selection from the **Action** list is **BLOCK always**, you also must make a selection from the **Select Schedule** list.

6. Click the **Apply** button.

   Your changes are saved.

Configure DMZ WAN Rules

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

The DMZ WAN Rules screen does not provide a list that lets you set the default outbound policy as the LAN WAN Rules screen does. You can change the default outbound policy by enabling all outbound traffic and then blocking only specific services from passing through the VPN firewall. You do so by adding outbound services rules. For more information, see *Create DMZ WAN Outbound Service Rules* on page 147.

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.

This section contains the following topics:

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

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

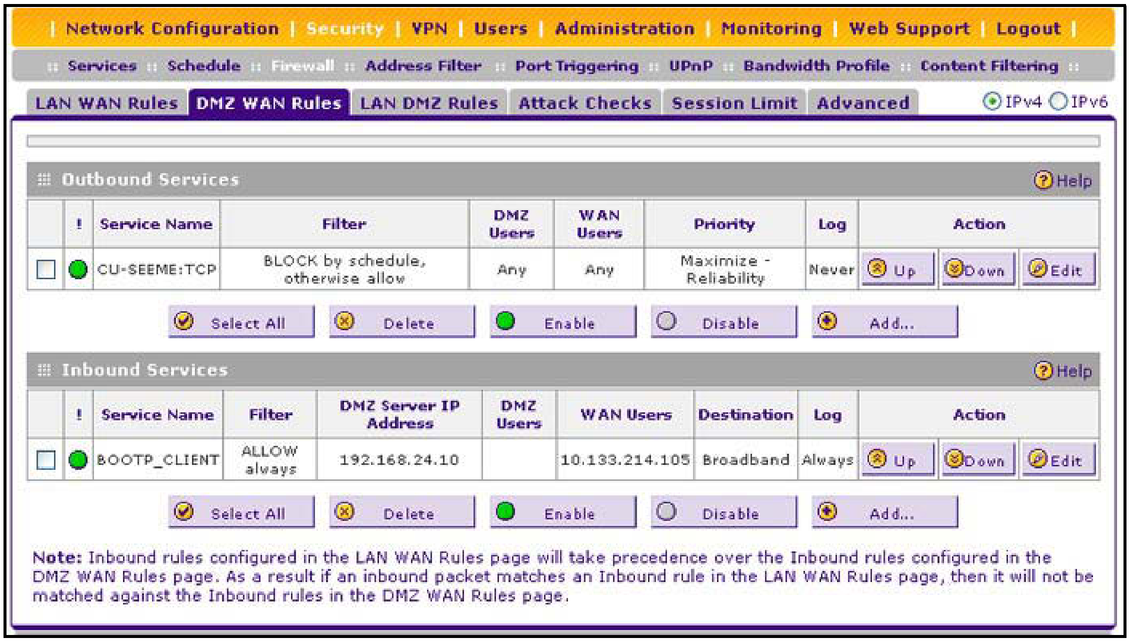
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > DMZ WAN Rules**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
● IPv4 ○ IPv6
Outbound Services
Help
Select All
Delete
Enable
Disable
Add...
Inbound Services
Help
Select All
Delete
Enable
Disable
Add...

Outbound Services

	!	Service Name	Filter	DMZ Users	WAN Users	Priority	Log	Action
☐	●	CU-SEEME:TCP	BLOCK by schedule, otherwise allow	Any	Any	Maximize - Reliability	Never	Up Down Edit

Inbound Services

	!	Service Name	Filter	DMZ Server IP Address	DMZ Users	WAN Users	Destination	Log	Action
☐	●	BOOTP_CLIENT	ALLOW always	192.168.24.10		10.133.214.105	Broadband	Always	Up Down Edit

Note: Inbound rules configured in the LAN WAN Rules page will take precedence over the Inbound rules configured in the DMZ WAN Rules page. As a result if an inbound packet matches an Inbound rule in the LAN WAN Rules page, then it will not be matched against the Inbound rules in the DMZ WAN Rules page.

3. 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
     - Edit DMZ WAN Inbound Service screen for IPv4
4. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

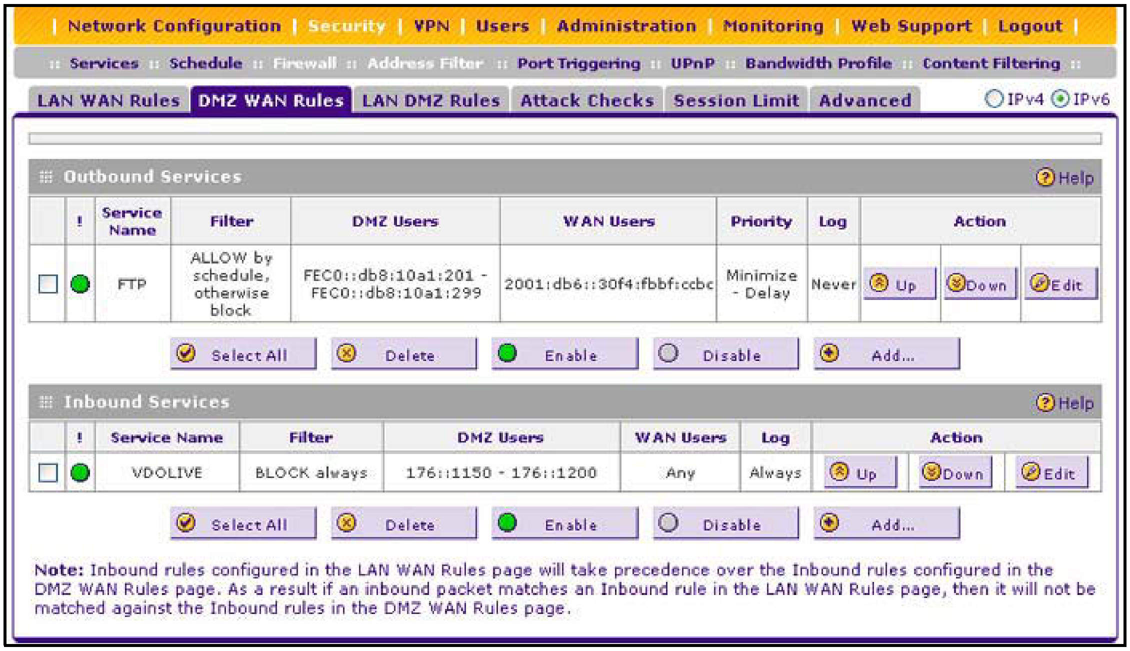
   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > DMZ WAN Rules**.

   The Firewall submenu tabs display with the DMZ WAN Rules screen for IPv4 in view.

3. In the upper right of the screen, select the **IPv6** radio button.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
LAN WAN Rules | DMZ WAN Rules | LAN DMZ Rules | Attack Checks | Session Limit | Advanced
○ IPv4 ● IPv6
Help

Outbound Services

	!	Service Name	Filter	DMZ Users	WAN Users	Priority	Log	Action		
□	●	FTP	ALLOW by schedule, otherwise block	FEC0::db8:10a1:201 - FEC0::db8:10a1:299	2001:db6::30f4:fbbf:ccbc	Minimize - Delay	Never	Up	Down	Edit

Select All
Delete
Enable
Disable
Add...

Inbound Services

	!	Service Name	Filter	DMZ Users	WAN Users	Log	Action		
□	●	VDOLIVE	BLOCK always	176::1150 - 176::1200	Any	Always	Up	Down	Edit

Select All
Delete
Enable
Disable
Add...

Note: Inbound rules configured in the LAN WAN Rules page will take precedence over the Inbound rules configured in the DMZ WAN Rules page. As a result if an inbound packet matches an Inbound rule in the LAN WAN Rules page, then it will not be matched against the Inbound rules in the DMZ WAN Rules page.

4. 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
     - Edit DMZ WAN Inbound Service screen for IPv6

5. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > DMZ WAN Rules**.

   The Firewall submenu tabs display with the DMZ WAN Rules screen for IPv4 in view.

3. To view the DMZ WAN Rules screen for IPv6 rules, in the upper right of the screen, select the **IPv6** radio button.
4. 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.
5. 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.
6. Click the **Apply** button.

   Your changes are saved.

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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

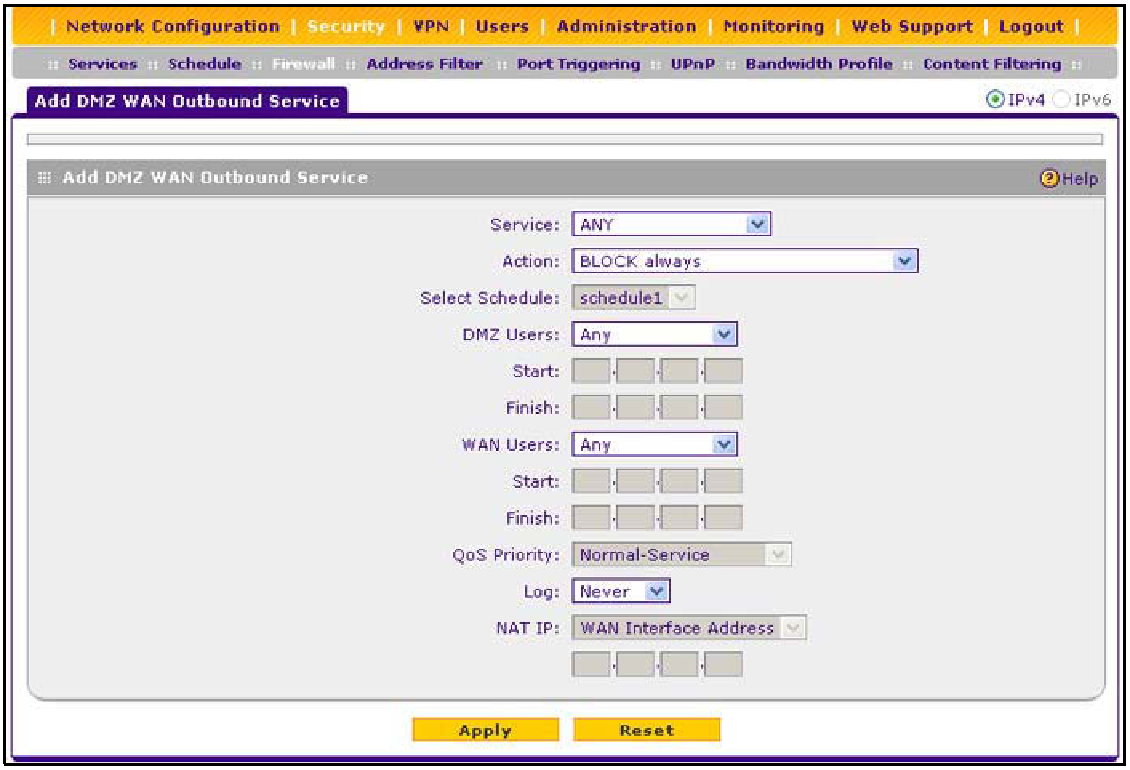
   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > DMZ WAN Rules**.

The DMZ WAN Rules screen displays. The **IPv4** radio button is selected by default. The screen displays the IPv4 settings.

3. Click the **Add** table button under the Outbound Services table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add DMZ WAN Outbound Service
● IPv4 ○ IPv6
Help
Apply
Reset

Add DMZ WAN Outbound Service

Service: ANY
Action: BLOCK always
Select Schedule: schedule1
DMZ Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
QoS Priority: Normal-Service
Log: Never
NAT IP: WAN Interface Address

4. Enter the settings as described in *Table 29* on page 128.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **DMZ Users**
   - **WAN Users**

   Unless your selection from the **Action** list is **BLOCK always**, you also must make selections from the following lists:

   - **Select Schedule**
   - **QoS Priority**
   - **NAT IP** (This list is available only when the WAN mode is NAT. If you select **Single Address**, the IP address specified must fall under the WAN subnet.)

5. Click the **Apply** button.

   Your changes are saved.

IPv6 DMZ WAN Outbound Service Rules

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

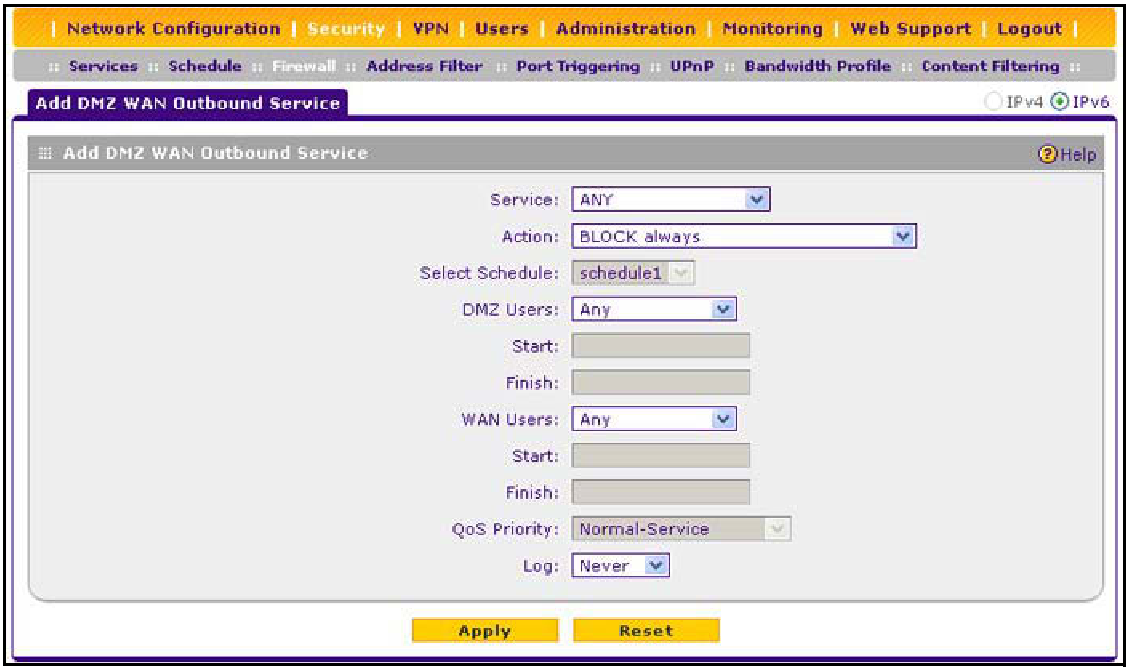
2. Select **Security > Firewall > DMZ WAN Rules**.

   The DMZ WAN Rules screen displays.

3. Select the **IPv6** radio button.

   The screen displays the IPv6 settings.

4. Click the **Add** table button under the Outbound Services table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add DMZ WAN Outbound Service
○ IPv4 ● IPv6
Help
Apply
Reset

Add DMZ WAN Outbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	schedule1
DMZ Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
QoS Priority:	Normal-Service
Log:	Never

5. Enter the settings as described in *Table 29* on page 128.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **DMZ Users**

- **WAN Users**

Unless your selection from the **Action** list is **BLOCK always**, you also must make selections from the following lists:

- **Select Schedule**
- **QoS Priority**

6. Click the **Apply** button.

   Your changes are saved.

Create DMZ WAN Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you did not define 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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

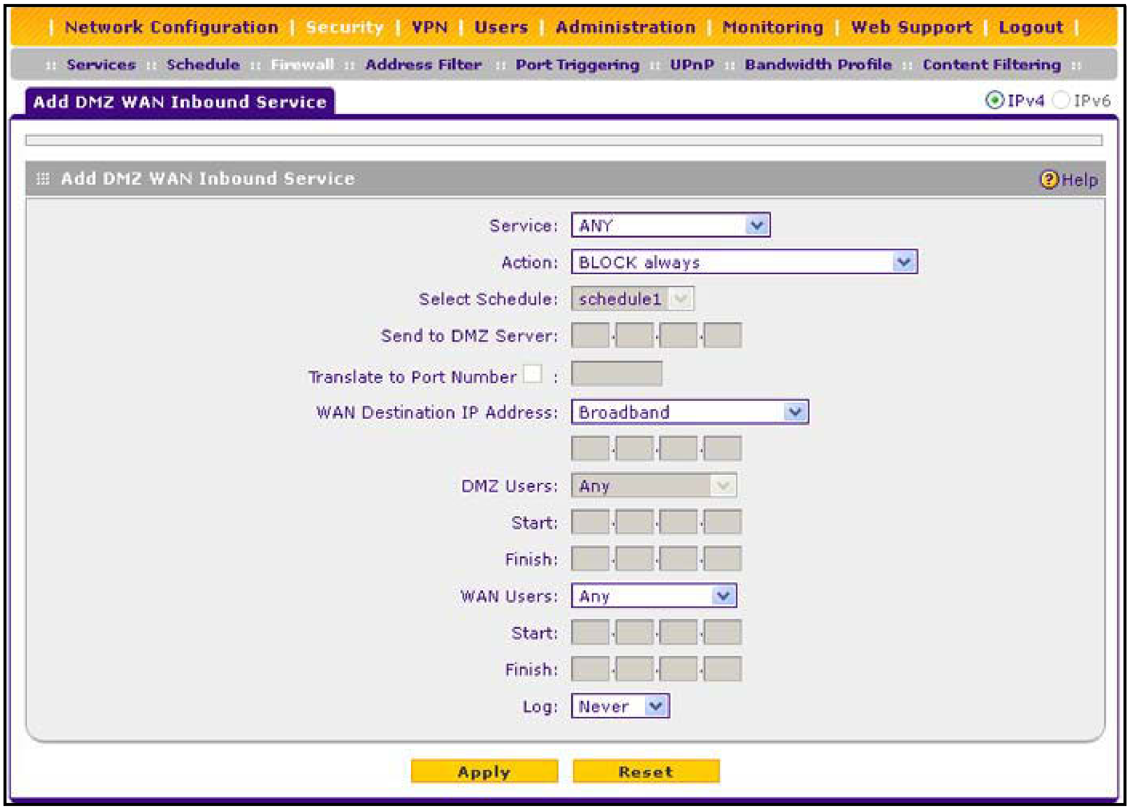
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > DMZ WAN Rules**.

   The DMZ WAN Rules screen displays. The **IPv4** radio button is selected by default. The screen displays the IPv4 settings.

3. Click the **Add** table button under the Inbound Services table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add DMZ WAN Inbound Service
● IPv4 ○ IPv6
Help
Apply
Reset

Add DMZ WAN Inbound Service

Service: ANY
Action: BLOCK always
Select Schedule: schedule1
Send to DMZ Server: . . .
Translate to Port Number □ :
WAN Destination IP Address: Broadband
. . .
DMZ Users: Any
Start: . . .
Finish: . . .
WAN Users: Any
Start: . . .
Finish: . . .
Log: Never

4. Enter the settings as described in *Table 30* on page 131.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **WAN Destination IP Address**
   - **DMZ Users** (This 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** list is **BLOCK always**, you also must make selections from the following lists:

   - **Select Schedule**
   - **Send to DMZ Server**

   The **Translate to Port Number** field is optional.

5. Click the **Apply** button.

   Your changes are saved.

IPv6 DMZ WAN Inbound Service Rules

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

1. Log in to the unit:
    a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

       The NETGEAR Configuration Manager Login screen displays.

    b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

       Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

    c. Click the **Login** button.

       The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

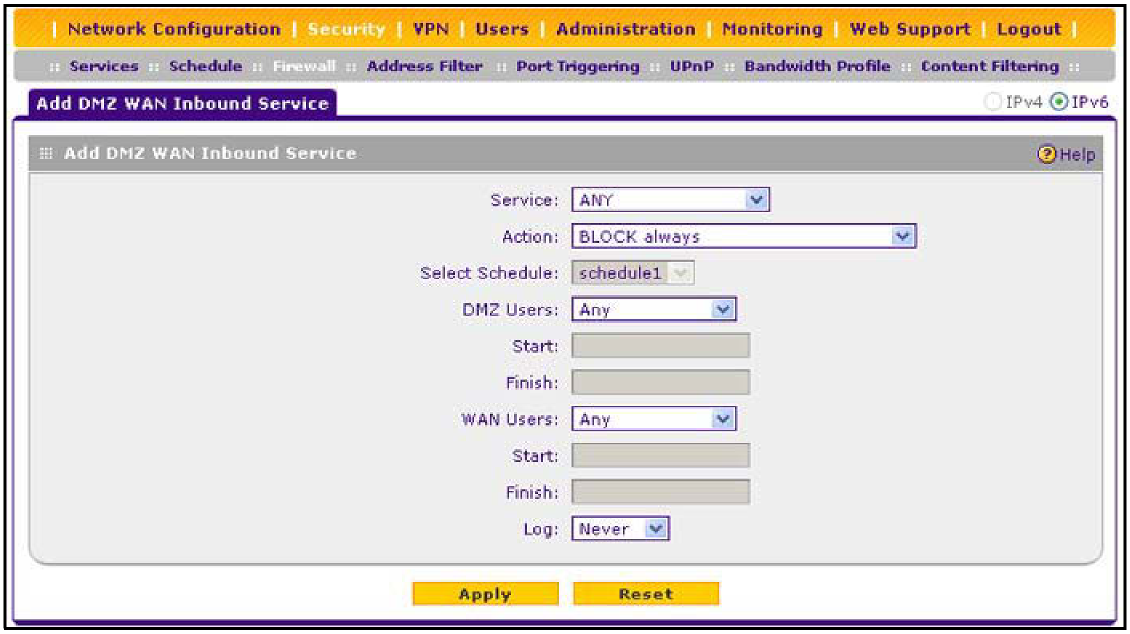
2. Select **Security > Firewall > DMZ WAN Rules**.

   The DMZ WAN Rules screen displays.

3. Select the **IPv6** radio button.

   The screen displays the IPv6 settings.

4. Click the **Add** table button under the Inbound Services table.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add DMZ WAN Inbound Service
○ IPv4 ● IPv6
Help
Apply
Reset

Add DMZ WAN Inbound Service

Service: ANY

Action: BLOCK always

Select Schedule: schedule1

DMZ Users: Any

Start:

Finish:

WAN Users: Any

Start:

Finish:

Log: Never

5. Enter the settings as described in *Table 30* on page 131.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **DMZ Users**

- **WAN Users**

  Unless your selection from the **Action** list is **BLOCK always**, you also must make selections from the **Select Schedule** list.

6. Click the **Apply** button.

   Your changes are saved.

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).

The LAN DMZ Rules screen does not provide a list that lets you set the default outbound policy as the LAN WAN Rules screen does. You can change the default outbound policy by allowing all outbound traffic and then blocking specific services from passing through the VPN firewall. You do so by adding outbound service rules (see *Create LAN DMZ Outbound Service Rules* on page 156).

This section contains the following topics:

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

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

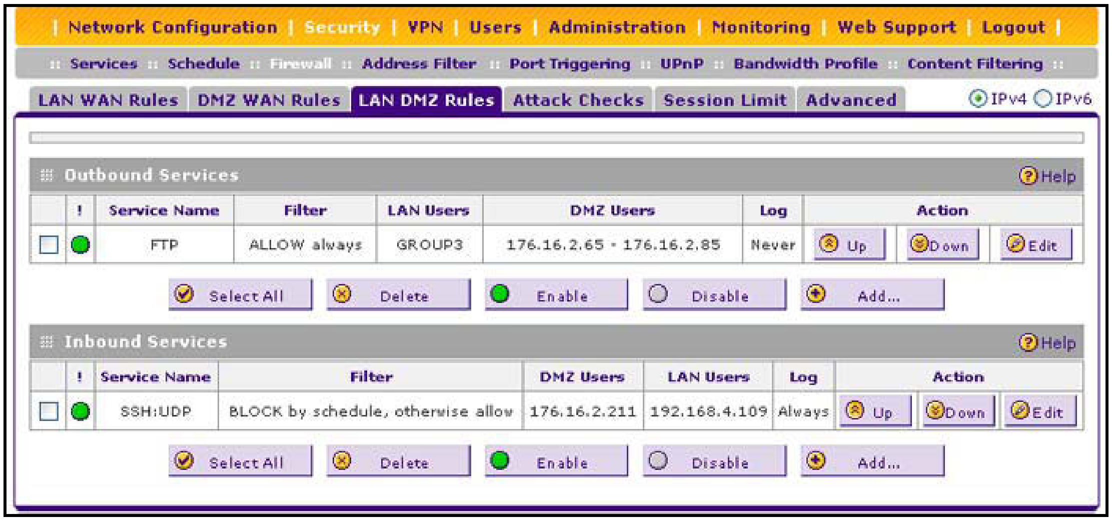
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > LAN DMZ Rules**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
● IPv4 ○ IPv6
Help
Select All
Delete
Enable
Disable
Add...

Outbound Services

	!	Service Name	Filter	LAN Users	DMZ Users	Log	Action		
□	●	FTP	ALLOW always	GROUP3	176.16.2.65 - 176.16.2.85	Never	Up	Down	Edit

Inbound Services

	!	Service Name	Filter	DMZ Users	LAN Users	Log	Action		
□	●	SSH:UDP	BLOCK by schedule, otherwise allow	176.16.2.211	192.168.4.109	Always	Up	Down	Edit

3. 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
     - Edit LAN DMZ Inbound Service screen for IPv4
4. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

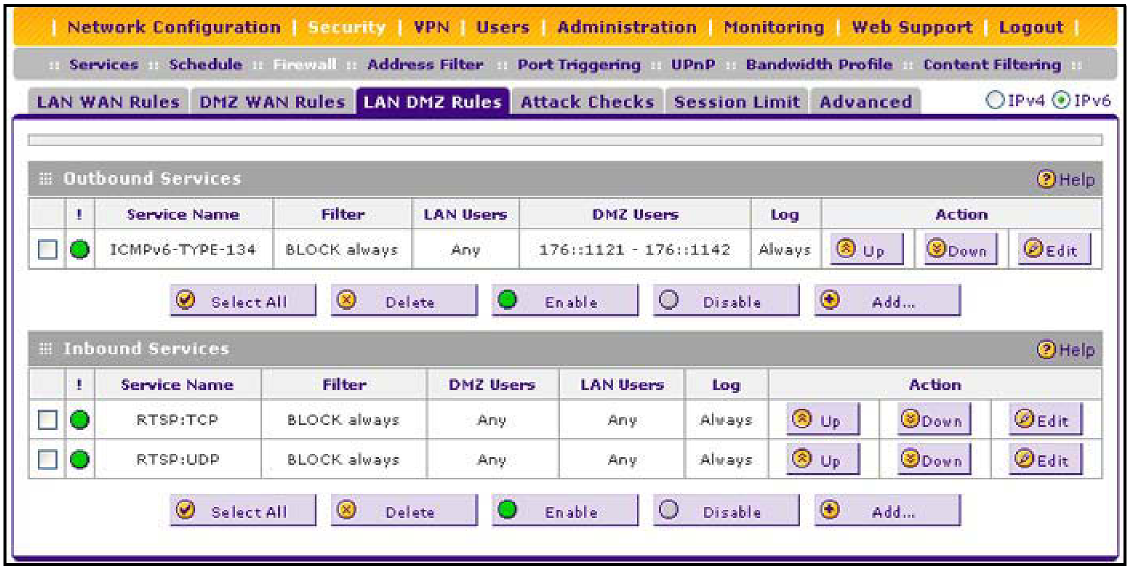
   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > LAN DMZ Rules**.

   The Firewall submenu tabs display with the LAN DMZ Rules screen for IPv4 in view.

3. In the upper right of the screen, select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
○ IPv4 ● IPv6
Help
Select All
Delete
Enable
Disable
Add...

Outbound Services

	!	Service Name	Filter	LAN Users	DMZ Users	Log	Action		
□	●	ICMPv6-TYPE-134	BLOCK always	Any	176::1121 - 176::1142	Always	Up	Down	Edit

Inbound Services

	!	Service Name	Filter	DMZ Users	LAN Users	Log	Action		
□	●	RTSP:TCP	BLOCK always	Any	Any	Always	Up	Down	Edit
□	●	RTSP:UDP	BLOCK always	Any	Any	Always	Up	Down	Edit

4. 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
     - Edit LAN DMZ Inbound Service screen for IPv6
5. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > LAN DMZ Rules**.

   The Firewall submenu tabs display with the DMZ WAN Rules screen for IPv4 in view.

3. To view the DMZ WAN Rules screen for IPv6 rules, in the upper right of the screen, select the **IPv6** radio button.
4. 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.
5. 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.
6. Click the **Apply** button.

   Your changes are saved.

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. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

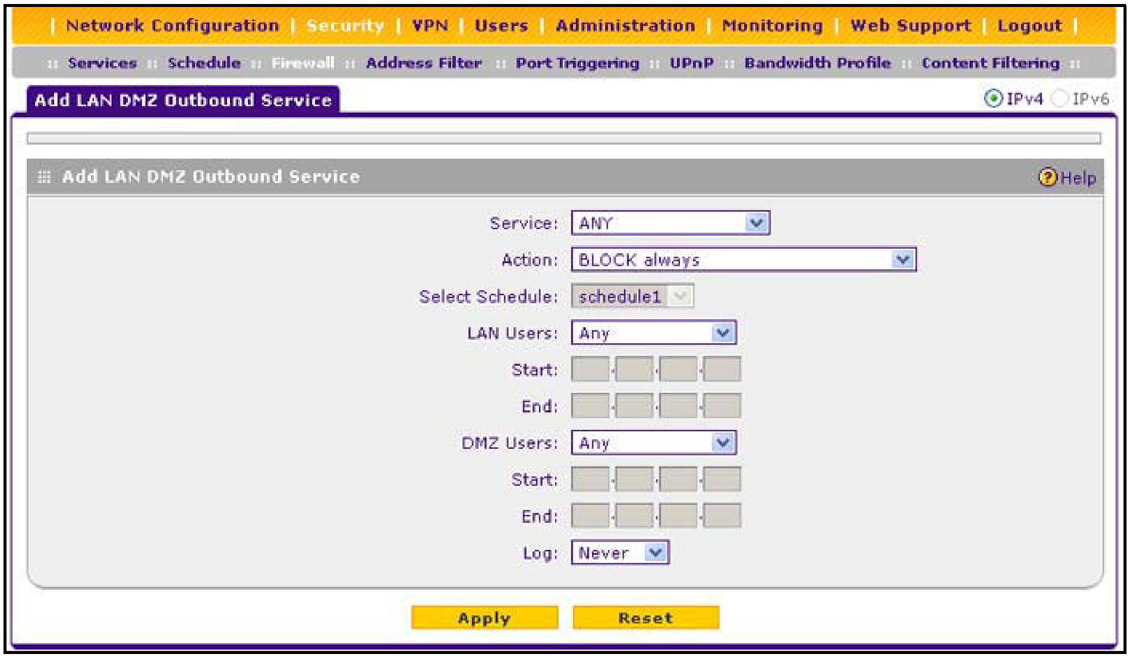
     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Security > Firewall > LAN DMZ Rules**.

   In the upper right of the LAN DMZ Rules screen, the **IPv4** radio button is selected by default. The screen displays the IPv4 settings.

3. Click the **Add** table button under the Outbound Services table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN DMZ Outbound Service
● IPv4 ○ IPv6
Help
Apply
Reset

Add LAN DMZ Outbound Service

Service: ANY
Action: BLOCK always
Select Schedule: schedule1
LAN Users: Any
Start:
End:
DMZ Users: Any
Start:
End:
Log: Never

4. Enter the settings as described in *Table 29* on page 128.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **LAN Users**
   - **DMZ Users**

   Unless your selection from the **Action** list is **BLOCK always**, you also must make a selection from the **Select Schedule** list.

5. Click the **Apply** button.

   Your changes are saved.

IPv6 LAN DMZ Outbound Service Rules

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

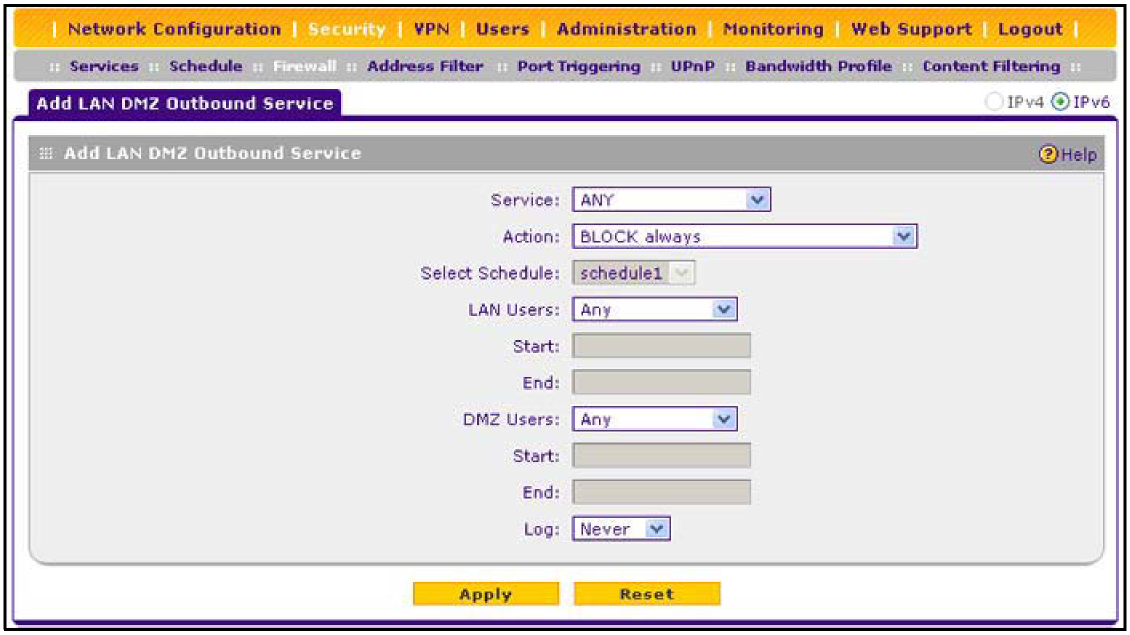
2. Select **Security > Firewall > LAN DMZ Rules**.

   The LAN DMZ Rules screen displays.

3. Select the **IPv6** radio button.

   The screen displays the IPv6 settings.

4. Click the **Add** table button under the Outbound Services table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
○ IPv4 ● IPv6
?Help
Apply
Reset

Add LAN DMZ Outbound Service

Add LAN DMZ Outbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	schedule1
LAN Users:	Any
Start:	
End:	
DMZ Users:	Any
Start:	
End:	
Log:	Never

5. Enter the settings as described in *Table 29* on page 128.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **LAN Users**
   - **DMZ Users**

   Unless your selection from the **Action** list is **BLOCK always**, you also must make a selection from the **Select Schedule** list.

6. Click the **Apply** button.

   Your changes are saved.

Create LAN DMZ Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you did not define 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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

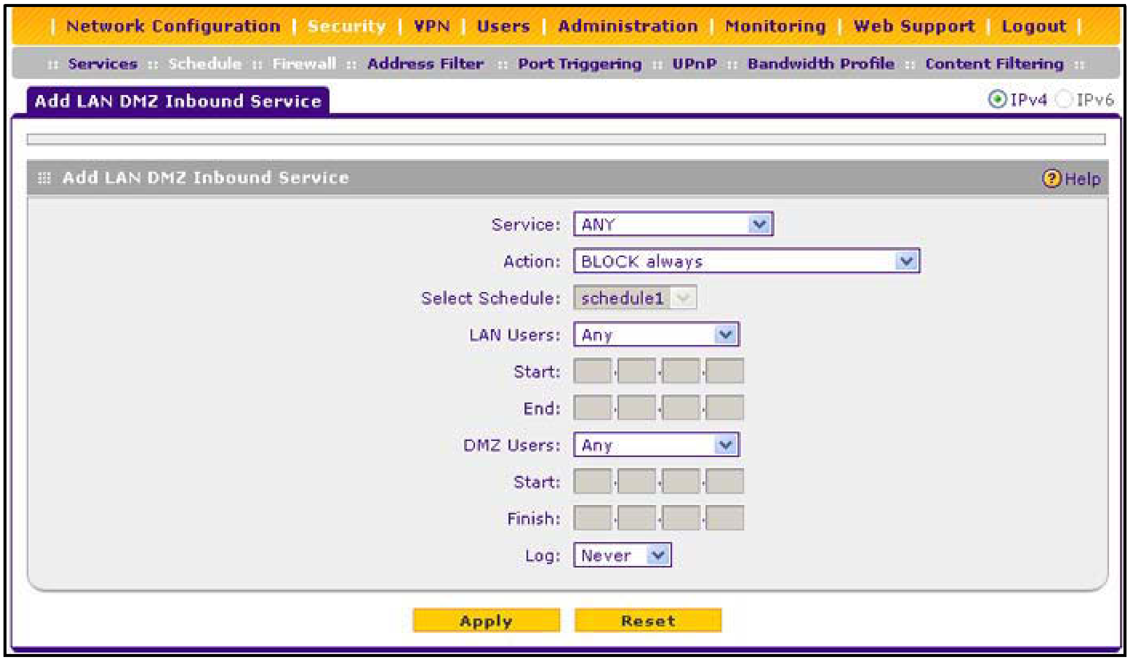
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > LAN DMZ Rules**.

   The LAN DMZ Rules screen displays. The **IPv4** radio button is selected by default. The screen displays the IPv4 settings.

3. Click the **Add** table button under the Inbound Services table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN DMZ Inbound Service
● IPv4 ○ IPv6
Add LAN DMZ Inbound Service
Help
Apply
Reset

Service: ANY
Action: BLOCK always
Select Schedule: schedule1
LAN Users: Any
Start:
End:
DMZ Users: Any
Start:
Finish:
Log: Never

4. Enter the settings as described in *Table 30* on page 131.

   In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

   - **LAN Users**
   - **DMZ Users**

Unless your selection from the **Action** list is **BLOCK always**, you also must make a selection from the **Select Schedule** list.

5. Click the **Apply** button.

   Your changes are saved.

IPv6 LAN DMZ Inbound Service Rules

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

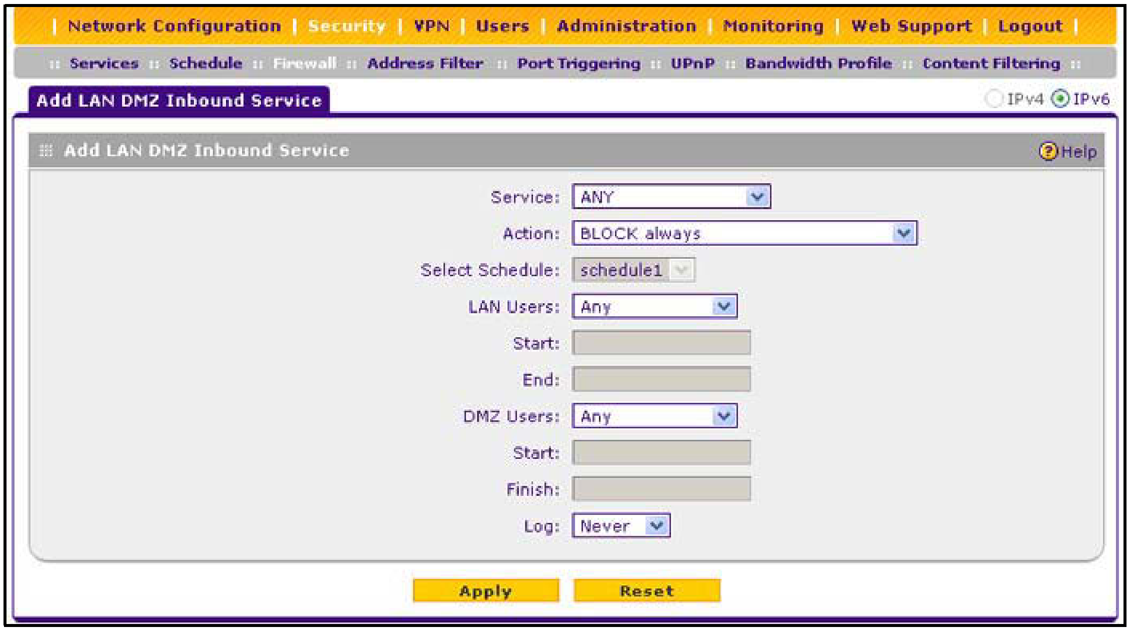
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > LAN DMZ Rules**.

   The LAN DMZ Rules screen displays. Select the **IPv6** radio button. The screen displays the IPv6 settings.

3. Click the **Add** table button under the Inbound Services table.



Add LAN DMZ Inbound Service ○ IPv4 ● IPv6

Add LAN DMZ Inbound Service

Service: ANY

Action: BLOCK always

Select Schedule: schedule1

LAN Users: Any

Start:

End:

DMZ Users: Any

Start:

Finish:

Log: Never

4. Enter the settings as described in *Table 30* on page 131.

In addition to selections from the **Service**, **Action**, and **Log** lists, you must make selections from the following lists:

- **LAN Users**
- **DMZ Users**

Unless your selection from the **Action** list is **BLOCK always**, you also must make a selection from the **Select Schedule** list.

5. Click the **Apply** button.

   Your changes are saved.

Examples of Firewall Rules

This section contains the following topics:

- *Examples of Inbound Firewall Rules*
- *Examples of Outbound Firewall Rules*

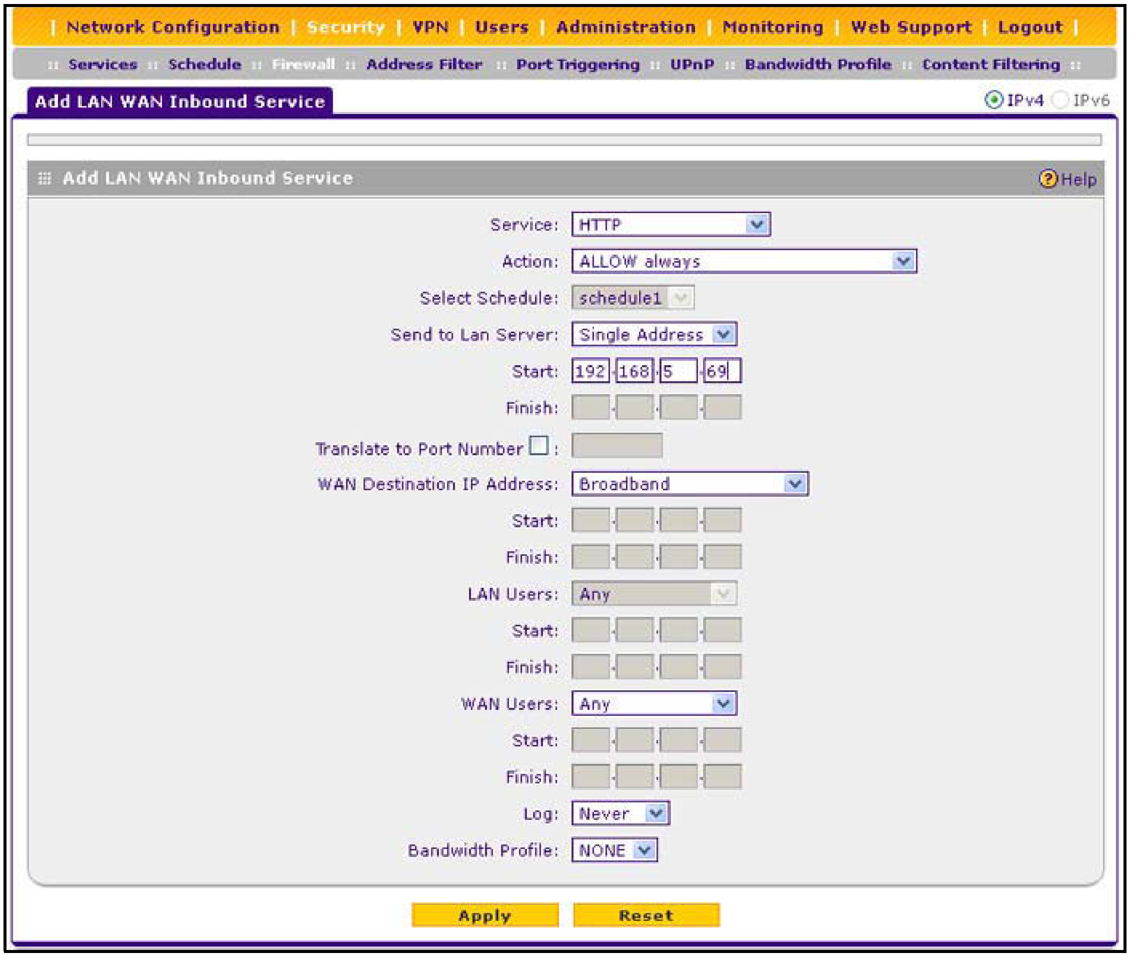
Examples of Inbound Firewall Rules

This section contains the following topics:

- *IPv4 LAN WAN Inbound Rule: Host a Local Public Web Server*
- *IPv4 LAN WAN Inbound Rule: Allow a Videoconference from Restricted Addresses*
- *IPv4 LAN WAN or IPv4 DMZ WAN Inbound Rule: Set Up One-to-One NAT Mapping*
- *IPv4 LAN WAN or IPv4 DMZ WAN Inbound Rule: Specifying an Exposed Host*
- *IPv6 LAN WAN Inbound Rule: Restrict RTelnet from a Single WAN User to a Single LAN User*

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.

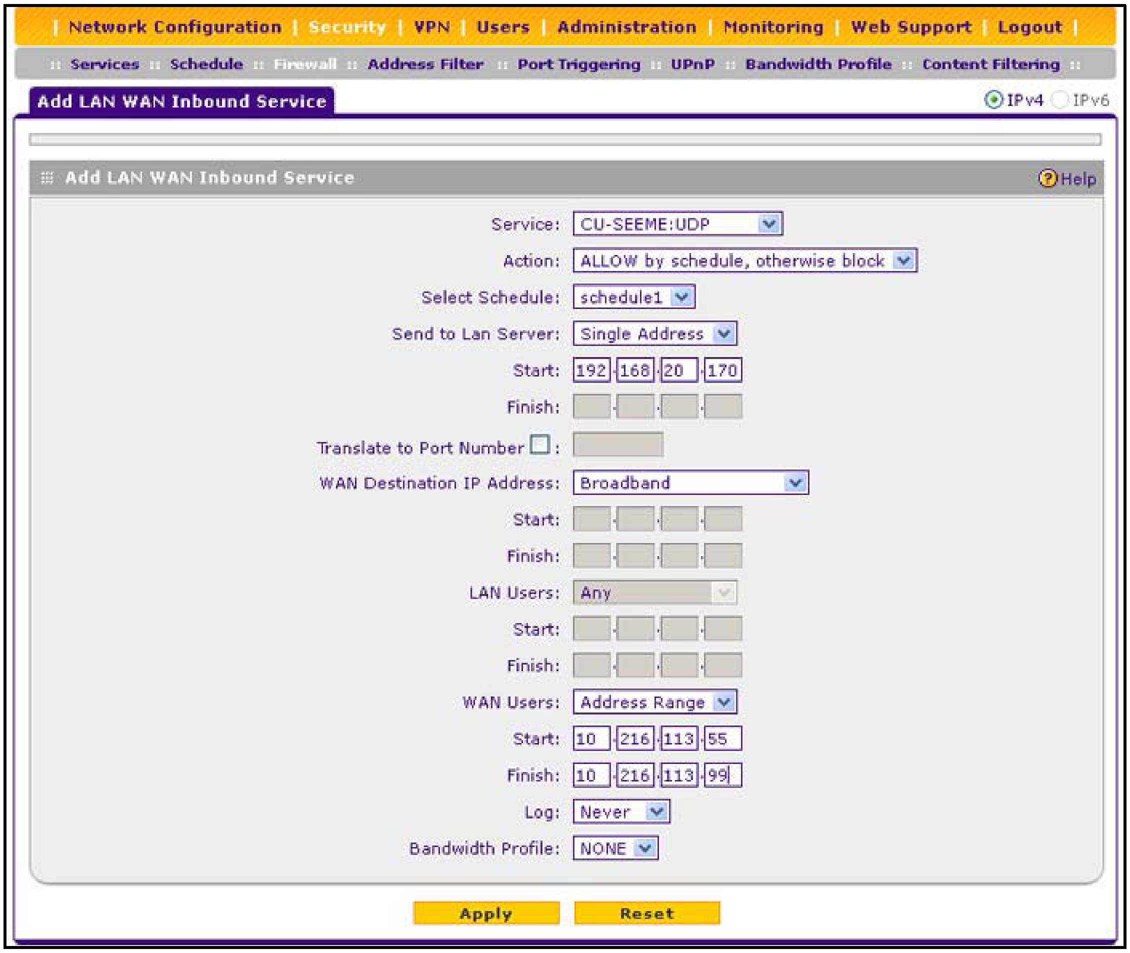

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Inbound Service
● IPv4 ○ IPv6
Add LAN WAN Inbound Service
Help
Apply
Reset

Service:	HTTP
Action:	ALLOW always
Select Schedule:	schedule1
Send to Lan Server:	Single Address
Start:	192.168.5.69
Finish:	
Translate to Port Number □ :	
WAN Destination IP Address:	Broadband
Start:	
Finish:	
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
Log:	Never
Bandwidth Profile:	NONE

Figure 10. Example of inbound firewall rule

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.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Help
Apply
Reset

Add LAN WAN Inbound Service

● IPv4 ○ IPv6

Add LAN WAN Inbound Service

Service: CU-SEEME:UDP

Action: ALLOW by schedule, otherwise block

Select Schedule: schedule1

Send to Lan Server: Single Address

Start: 192.168.20.170

Finish:

Translate to Port Number □ :

WAN Destination IP Address: Broadband

Start:

Finish:

LAN Users: Any

Start:

Finish:

WAN Users: Address Range

Start: 10.216.113.55

Finish: 10.216.113.99

Log: Never

Bandwidth Profile: NONE

Figure 11. Example of inbound firewall rule

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

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

The following addressing scheme is used to illustrate this procedure:

- NETGEAR VPN firewall:
  - **WAN IP address**. 10.1.0.118
  - **LAN IP address subnet**. 192.168.1.1 with subnet 255.255.255.0
  - **DMZ IP address subnet**. 192.168.10.1 with subnet 255.255.255.0
- Web server computer on the VPN firewall’s LAN:
  - **LAN IP address**. 192.168.1.2
  - **DMZ IP address**. 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 use more than one public IP address, you can use the additional public IP addresses to map to servers on your LAN or DMZ. One of these public IP addresses is used as the primary IP address of the router that provides Internet access to your LAN computers through NAT. The other addresses are available to map to your servers.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

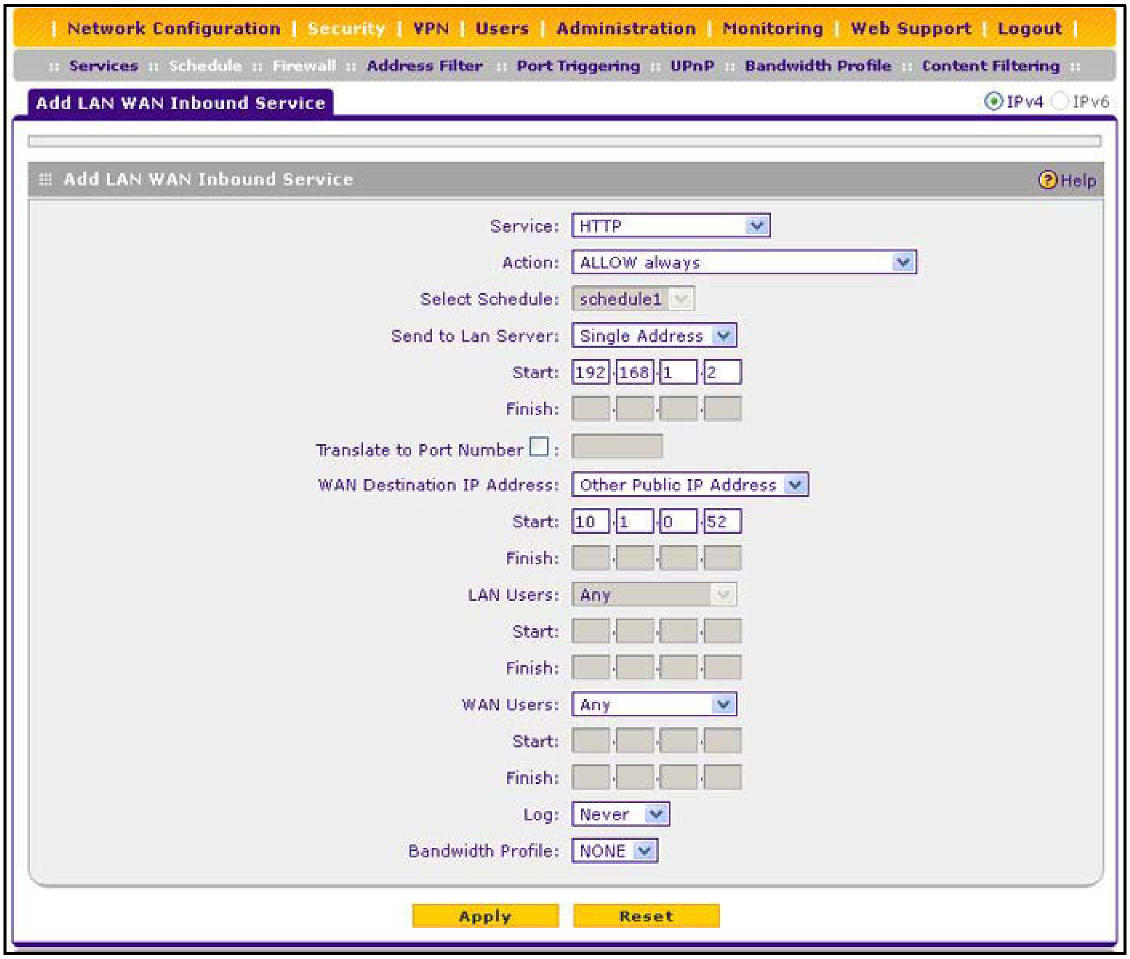
2. Select **Security > Firewall**.

   The Firewall submenu tabs display.

3. Choose one of the following:
   - 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.

   The **IPv4** radio button is selected by default. The screen displays the IPv4 settings.

4. Under the Inbound Services table, click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Inbound Service
● IPv4 ○ IPv6
Add LAN WAN Inbound Service
? Help
Apply
Reset

Service:	HTTP
Action:	ALLOW always
Select Schedule:	schedule1
Send to Lan Server:	Single Address
Start:	192.168.1.2
Finish:	
Translate to Port Number □:	
WAN Destination IP Address:	Other Public IP Address
Start:	10.1.0.52
Finish:	
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
Log:	Never
Bandwidth Profile:	NONE

5. From the **Service** list, select **HTTP** for a web server.
6. From the **Action** list, select **ALLOW always**.
7. In the **Send to LAN Server** field, enter the local IP address of your web server computer.

   The IP address is 192.168.1.2 in this example.

8. In the **WAN Destination IP Address** fields, enter **10.1.0.52**.
9. Click the **Apply** button.

   Your changes are saved.

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 mapped to your web server in *Step 8*. You 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 did not yet define.

WARNING:

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

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

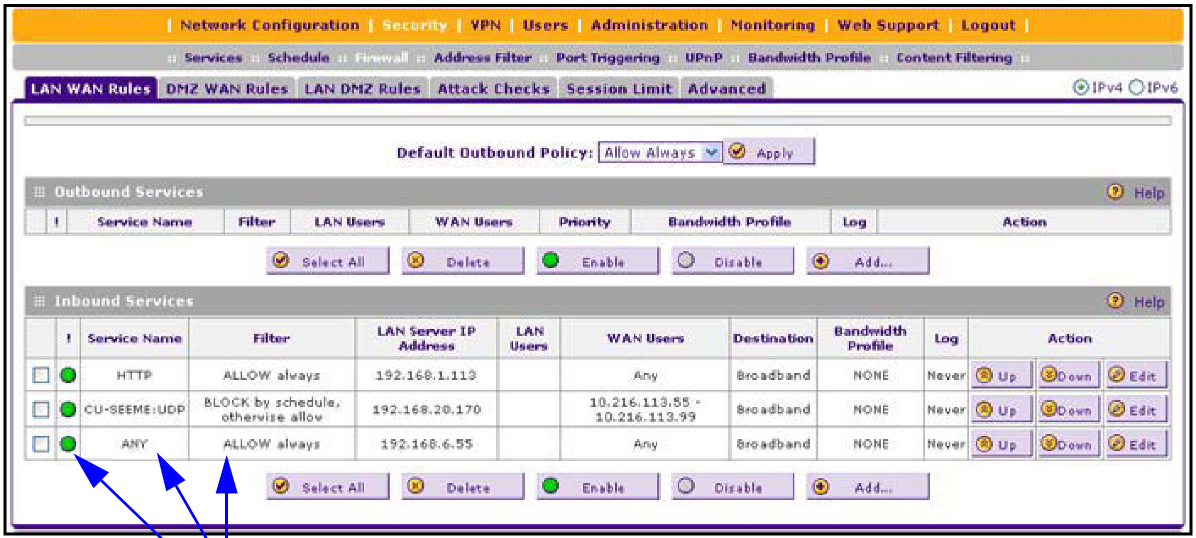
      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall** > **LAN WAN Rules**.

   The LAN WAN Rules screen displays.

3. Create an inbound rule that allows all protocols.
4. Place the rule below all other inbound rules.

See the example in the following figure.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
◉ IPv4 ○ IPv6
Apply
Outbound Services
Help
Select All
Delete
Enable
Disable
Add...
Inbound Services
Help
Select All
Delete
Enable
Disable
Add...

Default Outbound Policy: Allow Always

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Bandwidth Profile	Log	Action

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Bandwidth Profile	Log	Action
□	●	HTTP	ALLOW always	192.168.1.113		Any	Broadband	NONE	Never	Up Down Edit
□	●	CU-SEEME:UDP	BLOCK by schedule, otherwise allow	192.168.20.170		10.216.113.55 - 10.216.113.99	Broadband	NONE	Never	Up Down Edit
□	●	ANY	ALLOW always	192.168.6.55		Any	Broadband	NONE	Never	Up Down Edit

1. Select Any and Allow Always (or Allow by Schedule).
2. Place the rule below all other inbound rules.

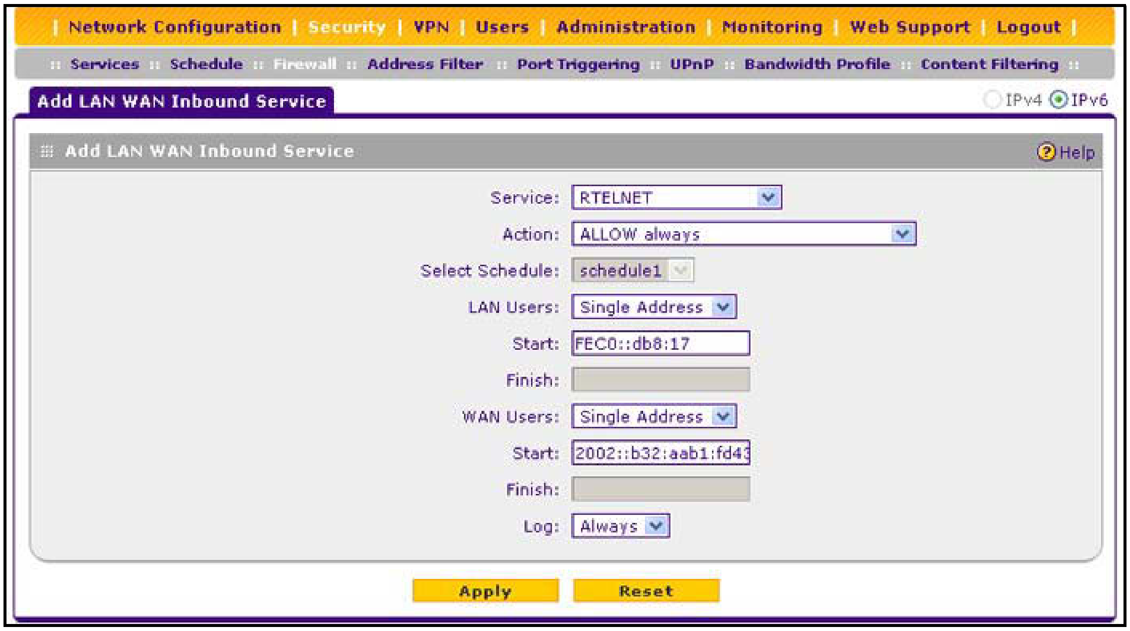
Figure 12. Example of inbound firewall rule

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 the example in the following figure.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Inbound Service
○ IPv4 ● IPv6
Add LAN WAN Inbound Service
Help
Apply
Reset

Service: RTELNET

Action: ALLOW always

Select Schedule: schedule1

LAN Users: Single Address

Start: FEC0::db8:17

Finish:

WAN Users: Single Address

Start: 2002::b32:aab1:fd43

Finish:

Log: Always

Figure 13. Example of inbound firewall rule

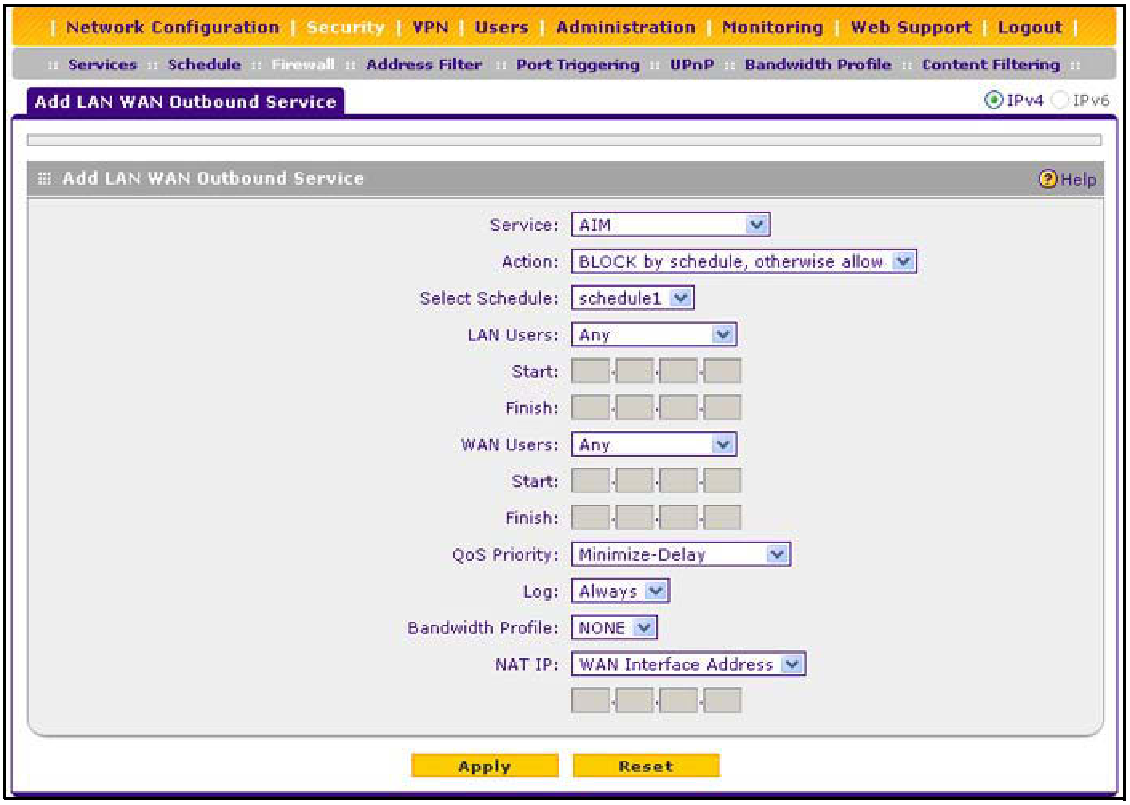
Examples of Outbound Firewall Rules

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 create on the Schedule screen. The schedule should specify working hours.

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


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Outbound Service
● IPv4 ○ IPv6
Add LAN WAN Outbound Service
Help
Apply
Reset

Service: AIM

Action: BLOCK by schedule, otherwise allow

Select Schedule: schedule1

LAN Users: Any

Start:

Finish:

WAN Users: Any

Start:

Finish:

QoS Priority: Minimize-Delay

Log: Always

Bandwidth Profile: NONE

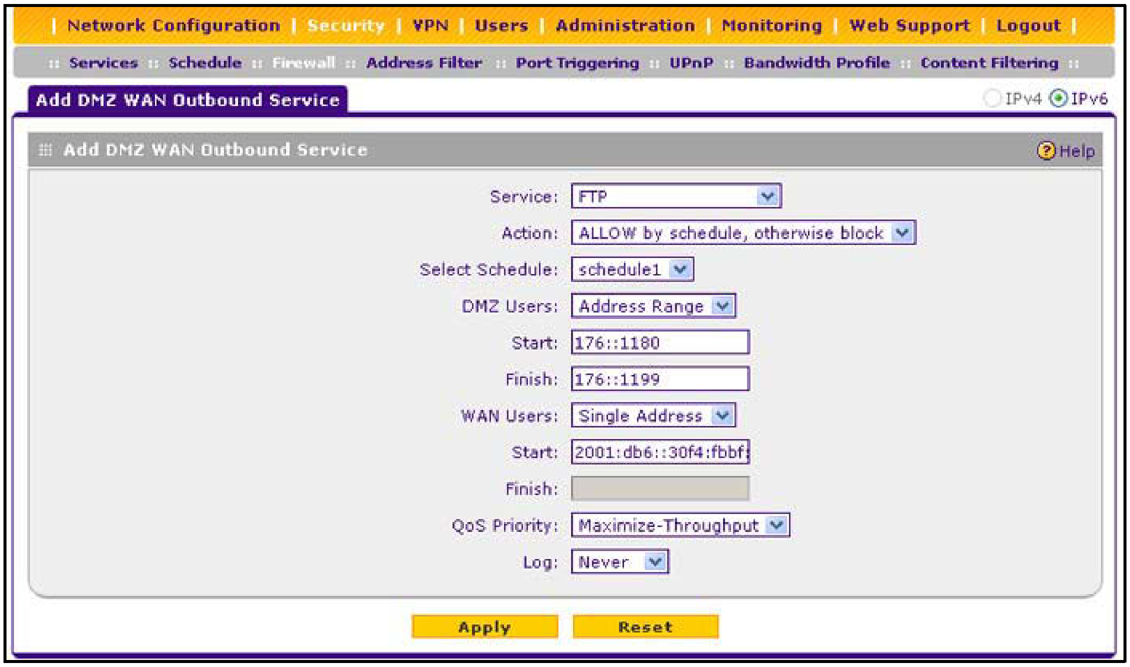
NAT IP: WAN Interface Address

Figure 14. Example of outbound firewall rule

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 the example in the following figure.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Help
Apply
Reset

Add DMZ WAN Outbound Service ○ IPv4 ● IPv6

Add DMZ WAN Outbound Service

Service: FTP
Action: ALLOW by schedule, otherwise block
Select Schedule: schedule1
DMZ Users: Address Range
Start: 176::1180
Finish: 176::1199
WAN Users: Single Address
Start: 2001:db6::30f4:fbbf
Finish:
QoS Priority: Maximize-Throughput
Log: Never

Figure 15. Example of outbound firewall rule

Configure Other Firewall Features

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

This section contains the following topics:

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

Attack Checks

You can specify whether the VPN firewall is 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 31* on page 170. 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. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

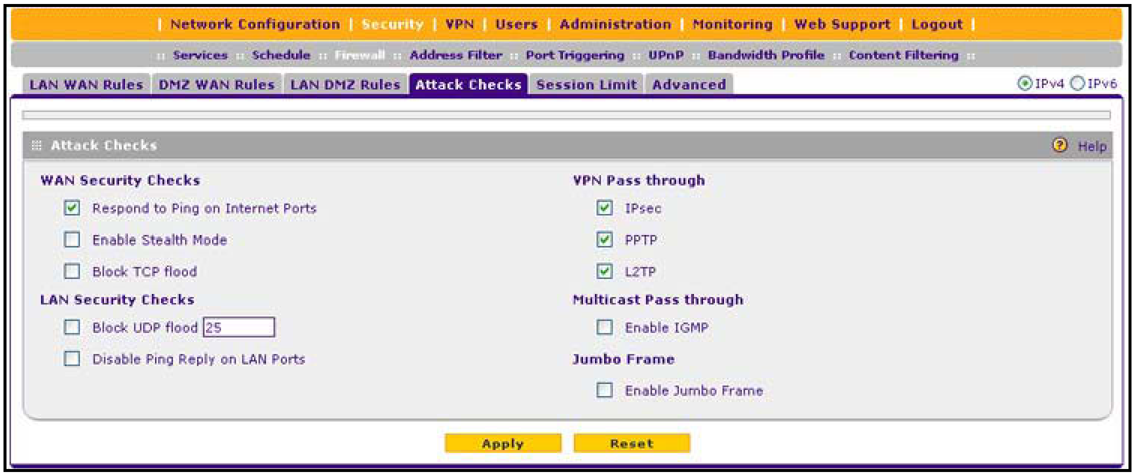
b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > Attack Checks**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Help
Apply
Reset

● IPv4 ○ IPv6

Attack Checks

WAN Security Checks
☑ Respond to Ping on Internet Ports
☐ Enable Stealth Mode
☐ Block TCP flood

LAN Security Checks
☐ Block UDP flood 25
☐ Disable Ping Reply on LAN Ports

VPN Pass through
☑ IPsec
☑ PPTP
☑ L2TP

Multicast Pass through
☐ Enable IGMP

Jumbo Frame
☐ Enable Jumbo Frame

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

Table 31. Attack Checks screen settings for IPv4

Setting	Description
WAN Security Checks	
Respond to Ping on Internet Ports	Select the **Respond to Ping on Internet Ports** check box to enable the VPN firewall to respond to a ping from the Internet to its IPv4 address. A ping can be used as a diagnostic tool. Keep this check box cleared unless a specific reason exists to enable the VPN firewall to respond to a ping from the Internet.
Enable Stealth Mode	Select the **Enable Stealth Mode** check box (which is the default setting) to prevent the VPN firewall from responding to port scans from the WAN, thus making it less susceptible to discovery and attacks.
Block TCP flood	Select the **Block TCP flood** check box (which is the default setting) to enable the VPN firewall to drop all invalid TCP packets and to protect the VPN firewall from a SYN flood attack. A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN (synchronize) requests to a target system. When the system responds, the attacker does not complete the connections, thus leaving the connection half open and flooding the server with SYN messages. No legitimate connections can then be made.

Table 31. 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 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 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 that the number of simultaneous, active UDP connections from a single device on the LAN is not restricted. A UDP flood is a form of denial of service attack that can be initiated when one device sends many UDP packets to random ports on a remote host. As a result, the distant host does the following: 1. Checks for the application listening at that port. 2. Sees that no application is listening at that port. 3. Replies with an ICMP Destination Unreachable packet. When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker might also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach the attacker, thus making the attacker’s network location anonymous.
Disable Ping Reply on LAN Ports	Select the **Disable Ping Reply on LAN Ports** check box to prevent the VPN firewall from responding to a ping on a LAN port. A ping can be used as a diagnostic tool. Keep this check box cleared unless a specific reason exists to prevent the VPN firewall from responding to a ping on a LAN port.
VPN Pass through	
IPSec PPTP L2TP	When the VPN firewall functions in NAT mode, all packets going to the remote VPN gateway are first filtered through NAT and then encrypted according to the VPN policy. For example, if a VPN client or gateway on the LAN side of the VPN firewall wants to connect to another VPN endpoint on the WAN side (placing the VPN firewall between two VPN endpoints), encrypted packets are sent to the VPN firewall. Because the VPN firewall filters the encrypted packets through NAT, the packets become invalid unless you enable the VPN Pass through feature. To enable the VPN tunnel to pass the VPN traffic without any filtering, select any or all of the following check boxes: • **IPSec**. Disables NAT filtering for IPSec tunnels. • **PPTP**. Disables NAT filtering for PPTP tunnels. • **L2TP**. Disables NAT filtering for L2TP tunnels. By default, all three check boxes are selected.
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.

Table 31. Attack Checks screen settings for IPv4 (continued)

Setting	Description
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.

4. Click the **Apply** button.

   Your changes are saved.

IPv6 Attack Checks

➤ **To enable IPv6 attack checks for your network environment:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

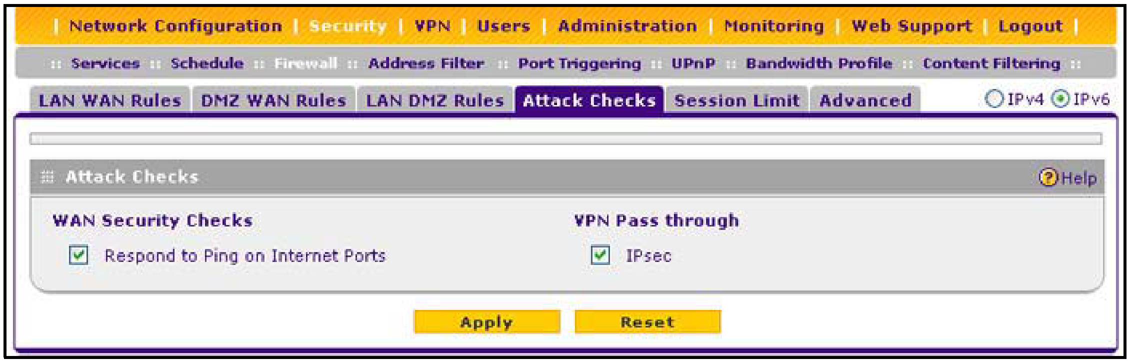
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > Attack Checks**.

   The Attack Checks screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
○ IPv4 ● IPv6
Attack Checks
Help
Apply
Reset

WAN Security Checks

☑ Respond to Ping on Internet Ports

VPN Pass through

☑ IPsec

4. Configure the following settings:

- **Respond to Ping on Internet Ports**. Select this check box to enable the VPN firewall to respond to a ping from the Internet to its IPv6 address. A ping can be used as a diagnostic tool. Keep this check box cleared unless a specific reason exists to enable the VPN firewall to respond to a ping from the Internet.
- **IPsec**. Select this 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.

5. Click the **Apply** button.

   Your changes are saved.

Set Limits for IPv4 Sessions

You can specify the total number of sessions that are allowed, per user, over an IPv4 connection across the VPN firewall. The session limits feature is disabled by default.

➢ **To enable and configure session limits:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

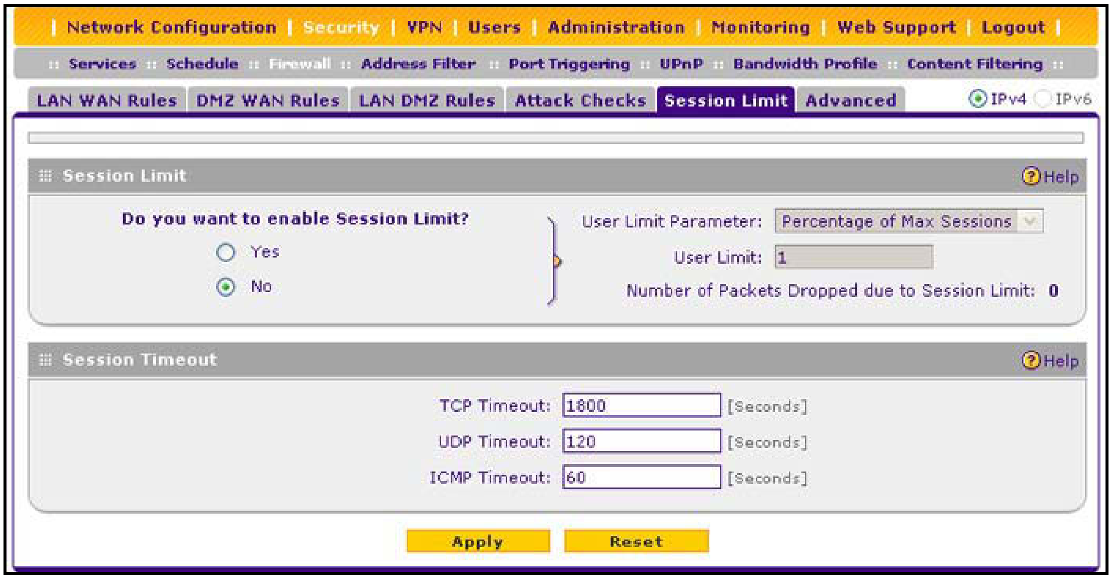
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > Session Limit**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
● IPv4 ○ IPv6
Help
Help
Apply
Reset

Session Limit

Do you want to enable Session Limit?
○ Yes
● No

User Limit Parameter: Percentage of Max Sessions

User Limit: 1

Number of Packets Dropped due to Session Limit: 0

Session Timeout

TCP Timeout: 1800 [Seconds]

UDP Timeout: 120 [Seconds]

ICMP Timeout: 60 [Seconds]

3. Select the **Yes** radio button under Do you want to enable Session Limit?
4. Enter the settings as described in the following table:

Table 32. Session Limit screen settings

Setting	Description
Session Limit	
User Limit Parameter	Select a user limit option: • **Percentage of Max Sessions**. A percentage of the total session connection capacity of the VPN firewall. • **Number of Sessions**. An absolute number of maximum sessions.
User Limit	Enter a number to indicate the user limit. Note the following: • If the user limit parameter is set to **Percentage of Max Sessions**, the number specifies the maximum number of sessions that are allowed from a single-source device as a percentage of the total session connection capacity of the VPN firewall. (The session limit is per-device based.) • If the user limit parameter is set to **Number of Sessions**, the number specifies an absolute value. **Note:** Some protocols such as FTP and RSTP create two sessions per connection. Consider this 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.

Table 32. Session Limit screen settings (continued)

Setting	Description
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	

5. Click the **Apply** button.

   Your changes are saved.

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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

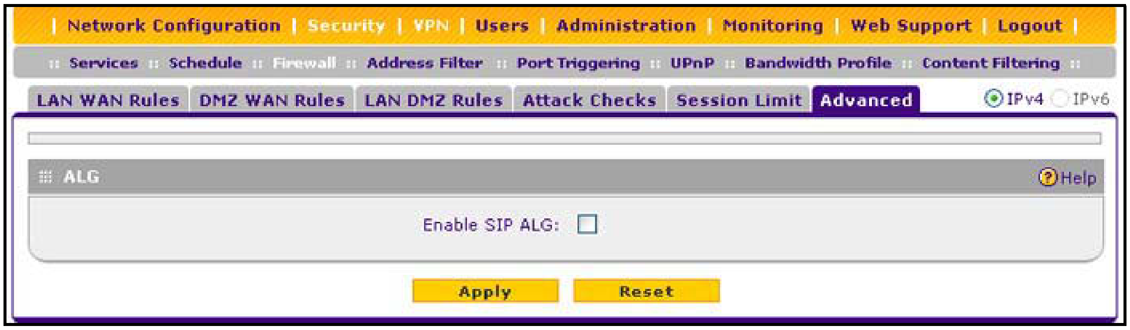
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Firewall > Advanced**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
LAN WAN Rules | DMZ WAN Rules | LAN DMZ Rules | Attack Checks | Session Limit | Advanced
● IPv4 ○ IPv6
ALG
Help
Apply
Reset

Enable SIP ALG: □

3. Select the **Enable SIP ALG** check box.
4. Click the **Apply** button.

Your changes are saved.

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 176.
- **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 180.
- **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 183.

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 195.

This section contains the following topics:

- *Add Customized Services*
- *Create Bandwidth Profiles*
- *Preconfigured Quality of Service Profiles*
- *Configure Service Groups*
- *Configure IP Groups*

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 players’ moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC 1700, *Assigned Numbers*. Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. However, on the VPN firewall you can select service numbers in the range from 1 to 65535.

Although the VPN firewall already holds a list of many service port numbers, you are not limited to these choices. Use the Services screen to add additional services and applications to the list for use in defining firewall rules. The Services screen shows a list of services that you defined.

To define a new service, you must 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 know the port number information, you can enter it on the Services screen.

The following ports are used internally:

- **TCP ports**. 11, 23, 53, 113, 443, 7911, 49152
- **UDP ports**. 53, 67, 161, 500, 520, 1028, 1029, 1030, 1900, 4500

➤ To add a customized service:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

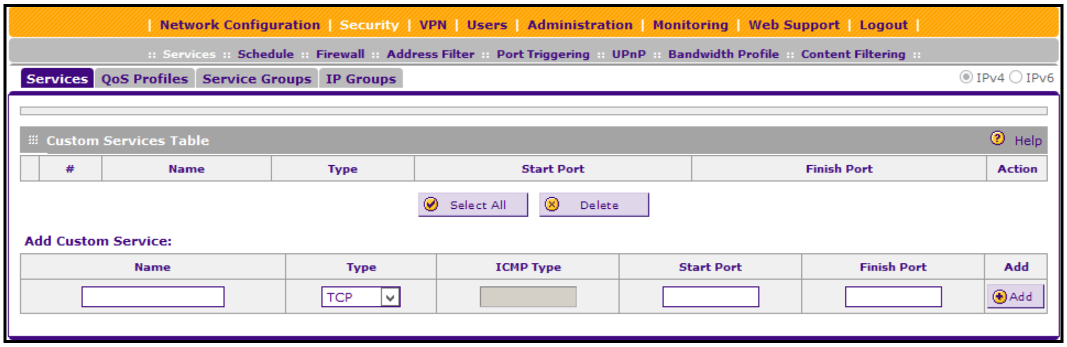
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Services**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Services
QoS Profiles
Service Groups
IP Groups
● IPv4 ○ IPv6
Help
Select All
Delete
Add

Custom Services Table

#	Name	Type	Start Port	Finish Port	Action

Add Custom Service:

Name	Type	ICMP Type	Start Port	Finish Port	Add
	TCP				Add

3. In the Add Customer Service section, enter the settings as described in the following table:

Table 33. Services screen settings

Setting	Description
Name	A descriptive name of the service for identification and management purposes.
Type	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, visit *http://www.iana.org/assignments/icmp-parameters*. **Note:** This field is enabled only when you select **ICMP** or **ICMPv6** from the Type list.
Start Port	The first TCP or UDP port of a range that the service uses. **Note:** This field is enabled only when you select **TCP** or **UDP** from the **Type** 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** list.
Default QoS Priority	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 183.

4. Click the **Apply** button.

   Your changes are saved.

➤ To edit a service:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

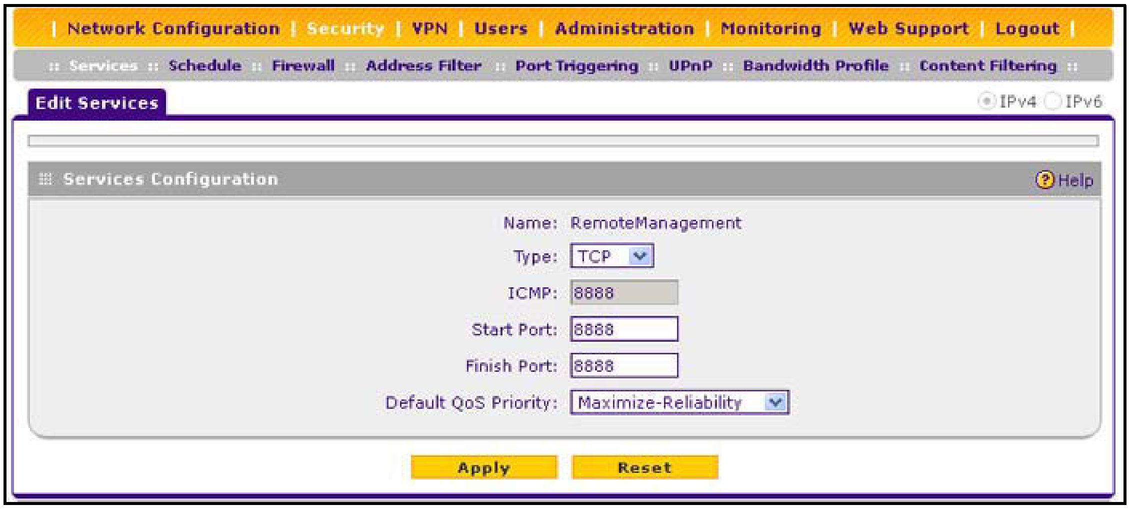
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Services**.

   The Services screen displays.

3. In the Custom Services table to the right of the service that you want to edit, click the **Edit** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Edit Services
● IPv4 ○ IPv6
Services Configuration
Help
Apply
Reset

Name: RemoteManagement
Type: TCP
ICMP: 8888
Start Port: 8888
Finish Port: 8888
Default QoS Priority: Maximize-Reliability

4. Modify the settings that you wish to change.

   See *Table 33* on page 178.

5. Click the **Apply** button.

   Your changes are saved.

➢ **To delete one or more services:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Services**.

   The Services screen displays.

3. 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.

4. Click the **Delete** table button.

   The information is deleted.

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 and allocates the traffic a bandwidth class as follows:

- If the rule includes 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 create a bandwidth profile, you can assign the bandwidth profile to firewall rules on the following screens:

- Add LAN WAN Outbound Services screen for IPv4
- Add LAN WAN Inbound Services screen for IPv4

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

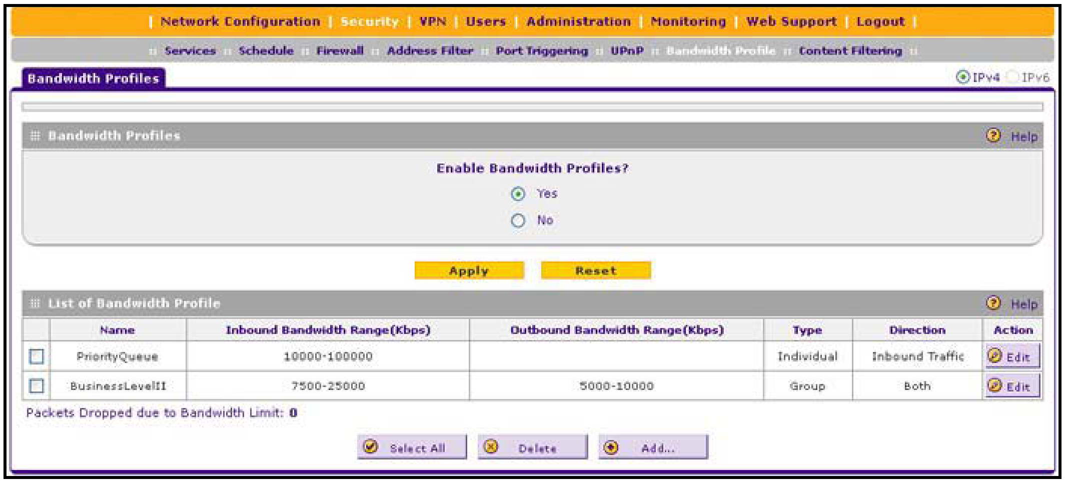
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Bandwidth Profiles**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Bandwidth Profiles
● IPv4 ○ IPv6
Help
Apply
Reset
Select All
Delete
Add...

Bandwidth Profiles

Enable Bandwidth Profiles?

● Yes

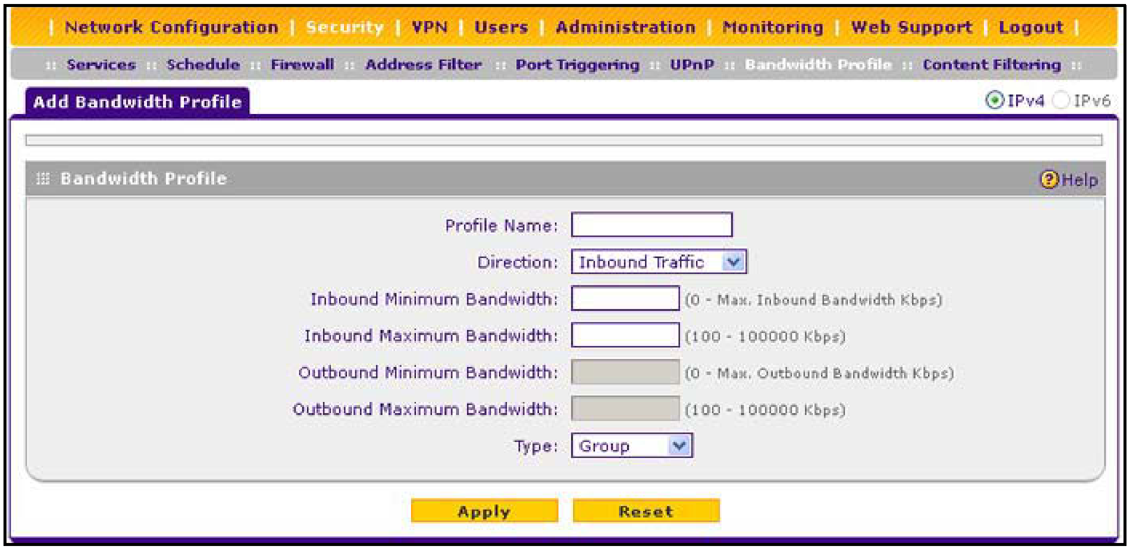
○ No

List of Bandwidth Profile

	Name	Inbound Bandwidth Range(Kbps)	Outbound Bandwidth Range(Kbps)	Type	Direction	Action
□	PriorityQueue	10000-100000		Individual	Inbound Traffic	Edit
□	BusinessLevelII	7500-25000	5000-10000	Group	Both	Edit

Packets Dropped due to Bandwidth Limit: 0

3. Under the List of Bandwidth Profiles table, click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add Bandwidth Profile
● IPv4 ○ IPv6
Help
Apply
Reset

Bandwidth Profile

Profile Name:		
Direction:	Inbound Traffic	
Inbound Minimum Bandwidth:		(0 - Max. Inbound Bandwidth Kbps)
Inbound Maximum Bandwidth:		(100 - 100000 Kbps)
Outbound Minimum Bandwidth:		(0 - Max. Outbound Bandwidth Kbps)
Outbound Maximum Bandwidth:		(100 - 100000 Kbps)
Type:	Group	

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

Table 34. Add Bandwidth Profile screen settings

Setting	Description
Profile Name	A descriptive name of the bandwidth profile for identification and management purposes.
Direction	Select the traffic direction for the bandwidth profile: • **Inbound Traffic**. The bandwidth profile is applied only to inbound traffic. Specify the inbound minimum and maximum bandwidths. • **Outbound Traffic**. The bandwidth profile is applied only to outbound traffic. Specify the outbound minimum and maximum bandwidths. • **Both**. The bandwidth profile is applied to both outbound and inbound traffic. Specify both the outbound and inbound minimum and maximum bandwidths.

Table 34. Add Bandwidth Profile screen settings (continued)

Setting	Description
Inbound Minimum Bandwidth	The inbound minimum allocated bandwidth in Kbps. No default setting is specified.
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. No default setting is specified.
Outbound Minimum Bandwidth	The outbound minimum allocated bandwidth in Kbps. No default setting is specified.
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. No default setting is specified.
Type	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.

5. Click the **Apply** button.

   Your changes are saved.

6. In the Bandwidth Profiles section, under Enable Bandwidth Profiles, select the **Yes** radio button

   By default, the **No** radio button is selected.

7. Click the **Apply** button.

   Your changes are saved.

➢ **To edit a bandwidth profile:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Bandwidth Profiles**.

   The Bandwidth Profiles screen displays.

3. In the List of Bandwidth Profiles table to the right of the bandwidth profile that you want to edit, click the **Edit** table button.

   The Edit Bandwidth Profile screen displays.

4. Modify the settings that you wish to change.

   See *Table 34* on page 181.

5. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Bandwidth Profiles**.

   The Bandwidth Profiles screen displays.

3. 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.

4. To delete the selected profile or profiles, click the **Delete** table button.

   The information is deleted.

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 VPN firewall. A QoS profile becomes active only when it is associated with a nonblocking inbound or outbound firewall rule or service, and traffic matching the firewall rule or service is processed by the VPN firewall. Priorities are defined by 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
- Add LAN WAN Outbound Services screen for IPv6
- Add DMZ WAN Outbound Services screen for IPv4

- Add DMZ WAN Outbound Services screen for IPv6
- Services screen

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 must be transferred over a link with a lower cost. IP packets are marked with a ToS value of 2.
- **Maximize-Reliability**. Used when data must 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 must be low. IP packets are marked with a ToS value of 16.

Configure Service Groups

A firewall is a security mechanism that lets network administrators selectively block or allow certain types of traffic in accordance with rules that they specify.

When you create a firewall rule, you select a service to which the firewall rule applies. Use the Service Group screen to create custom service groups for which firewall rules can be defined. Once defined, the new service group appears in the Service list of the screens you use to add or edit firewall rules.

➤ **To add a custom service group:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

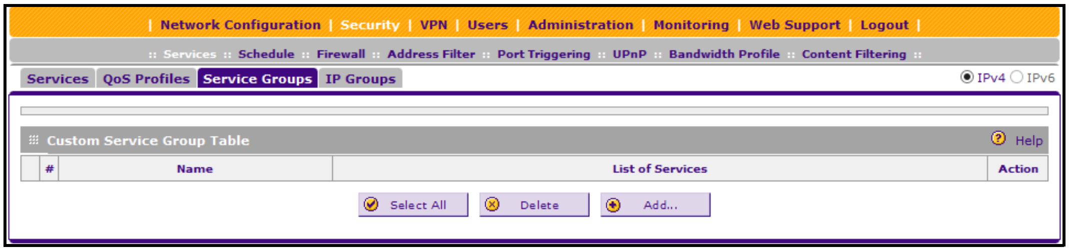
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Service Groups**.

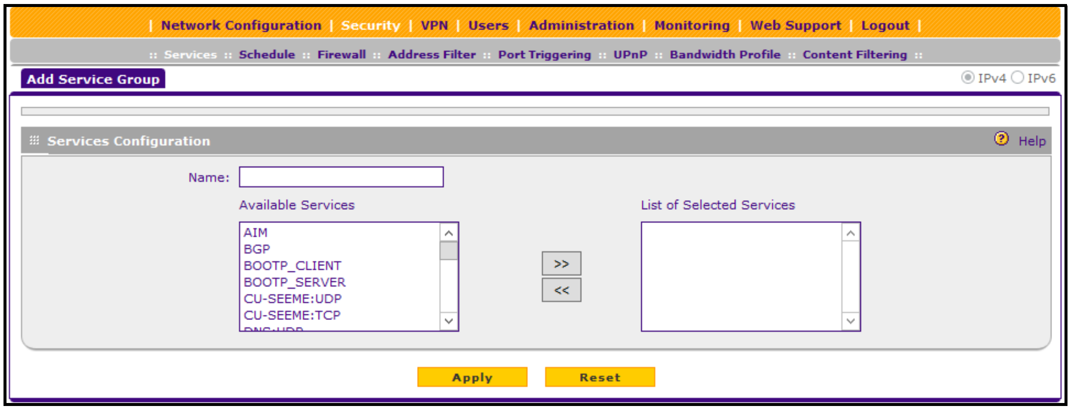

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Services
QoS Profiles
Service Groups
IP Groups
● IPv4 ○ IPv6
Custom Service Group Table
Help
#
Name
List of Services
Action
Select All
Delete
Add...

The following table lists all the custom service groups and their settings.

Table 35. Custom service group settings

Setting	Description
#	A numerical ID that the router assigns to a service group. The router contains a list of predefined services and custom services that can be viewed on the Firewall Rules screens (select **Network Security > Firewall**). When you add a custom service group, the service group is assigned the next ID following that of the most recently added service in the list.
Name	Name of the service group for identification and management purposes.
List of Services	Shows the services that are grouped, separated by commas (,).

3. Click the **Add** button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add Service Group
● IPv4 ○ IPv6
Services Configuration
Help
Name:
Available Services
AIM
BGP
BOOTP_CLIENT
BOOTP_SERVER
CU-SEEME:UDP
CU-SEEME:TCP
>>
<<
List of Selected Services
Apply
Reset

The following table lists the settings that are needed to add a new custom service group.

Table 36. The settings to add a custom service group

Setting	Description
Name	Name of the service group for identification and management purposes.
Available Services	This list includes all the available default services and custom services. This list does not show already grouped services, which display in the List of Selected Services list. Select the services that you want to group in a custom service group. To select multiple contiguous services, drag the pointer from the first item you want to select through the last item. To select noncontiguous services, hold the Ctrl key on the keyboard and click the services that you want to select.

Table 36. The settings to add a custom service group (continued)

Setting	Description
>>	Click this button to move the selected services from the Available Services list to the List of Selected Services list.
<<	To remove services from a custom group, click this button to move the services from the List of Selected Services list to the Available Services list.
List of Selected Services	This list includes all the services to be included in a new service group. To remove services from this group, select services as you do in the Available Services list. At least one service must be included in this list to add a new service group.

Click the **Apply** button.

Your changes are saved.

➤ To edit a custom service group:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Service Groups**.

   The Service Groups screen displays.

3. In the Custom Services Group table to the right of the service that you want to edit, click the **Edit** table button.
4. Modify the settings that you wish to change.

   See *Table 36* on page 185.

5. Click the **Apply** button.

   Your changes are saved.

➤ To delete a custom service group:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Service Groups**.

The Service Groups screen displays.

3. In the Custom Services Group 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 groups.
4. To delete the selected profile or profiles, click the **Delete** table button.

The information is deleted.

Configure IP Groups

A firewall is a security mechanism that selectively blocks or allows certain types of traffic in accordance with rules specified by network administrators.

The Firewall Rules screen allows selection of IP groups (LAN/WAN) while creating firewall rules. This screen allows the creation of custom IP groups against which firewall rules can be defined. Once defined, the new custom IP group appears in the **LAN Users** list and **WAN Users** list of the Firewall Rules screen based on the type of custom IP group.

➢ **To add a custom IP group:**

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

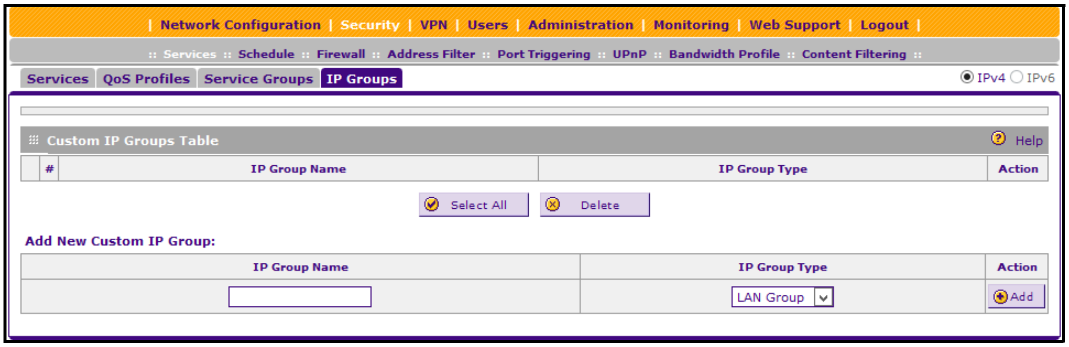
b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > IP Groups**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Services
QoS Profiles
Service Groups
IP Groups
● IPv4 ○ IPv6
Help
Select All
Delete
Add

Custom IP Groups Table

#	IP Group Name	IP Group Type	Action

Add New Custom IP Group:

IP Group Name	IP Group Type	Action
	LAN Group	Add

The following table lists all the custom IP groups and their settings.

Table 37. Custom IP group settings

Setting	Description
#	A numerical ID assigned to a custom IP group (by the router). The router contains a list of predefined IP groups which can be viewed from the Firewall Rules screen, which you access from the Security menu. Custom IP groups will be assigned an ID starting from 1, which is independent of default IP groups.
IP Group Name	Name of the custom IP group for identification and management purposes.
IP Group Type	Shows the type of custom IP group either as a LAN group or as a WAN group. You must specify the group type as either a source user or destination user when creating firewall rules.

Click the **Add** button.

Your changes are saved.

➢ To edit a custom IP group:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > IP Groups**.

   The IP Groups screen displays.

3. In the Custom IP Groups table to the right of the service that you want to edit, click the **Edit** table button.
4. Modify the settings that you wish to change.

   See *Table 37* on page 188.
5. Click the **Apply** button.

   Your changes are saved.

➢ **To delete a custom IP group:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Security > IP Groups**.

   The IP Groups screen displays.
3. In the Custom IP Groups table, select the check box to the left of each custom IP group that you want to delete or click the **Select All** table button to select all groups.
4. To delete the selected profile or profiles, click the **Delete** table button.

   The information is deleted.

Configure Content Filtering

To restrict access to certain sites on the Internet by internal LAN users, you can use the content filtering and web component blocking features of the VPN firewall. By default, these features are disabled; all requested traffic from any website is allowed. If you enable one or more of these features and users try to access a blocked site, they see a “Blocked by NETGEAR” message.

Note: Content filtering is supported for IPv4 users and groups only. Filtering is limited to HTTP traffic. HTTPS traffic cannot be filtered.

Several types of blocking are available:

- **Web component blocking**. 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. You can block the following web component types:
    - **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.

      Many websites require that cookies be accepted for the site to be accessed correctly. Blocking cookies might interfere with useful functions provided by these websites.
- **Keyword blocking (domain name blocking)**. You can specify up to 32 words to block. If any of these words appear in the website name (URL) or in a newsgroup name, the website or newsgroup is blocked by the VPN firewall.

  You can apply the keywords to one or more LAN groups. Requests from the computers in the groups are blocked where keyword blocking is enabled. Blocking does not occur for the computers in the groups where keyword blocking is 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.

  Here are some 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. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

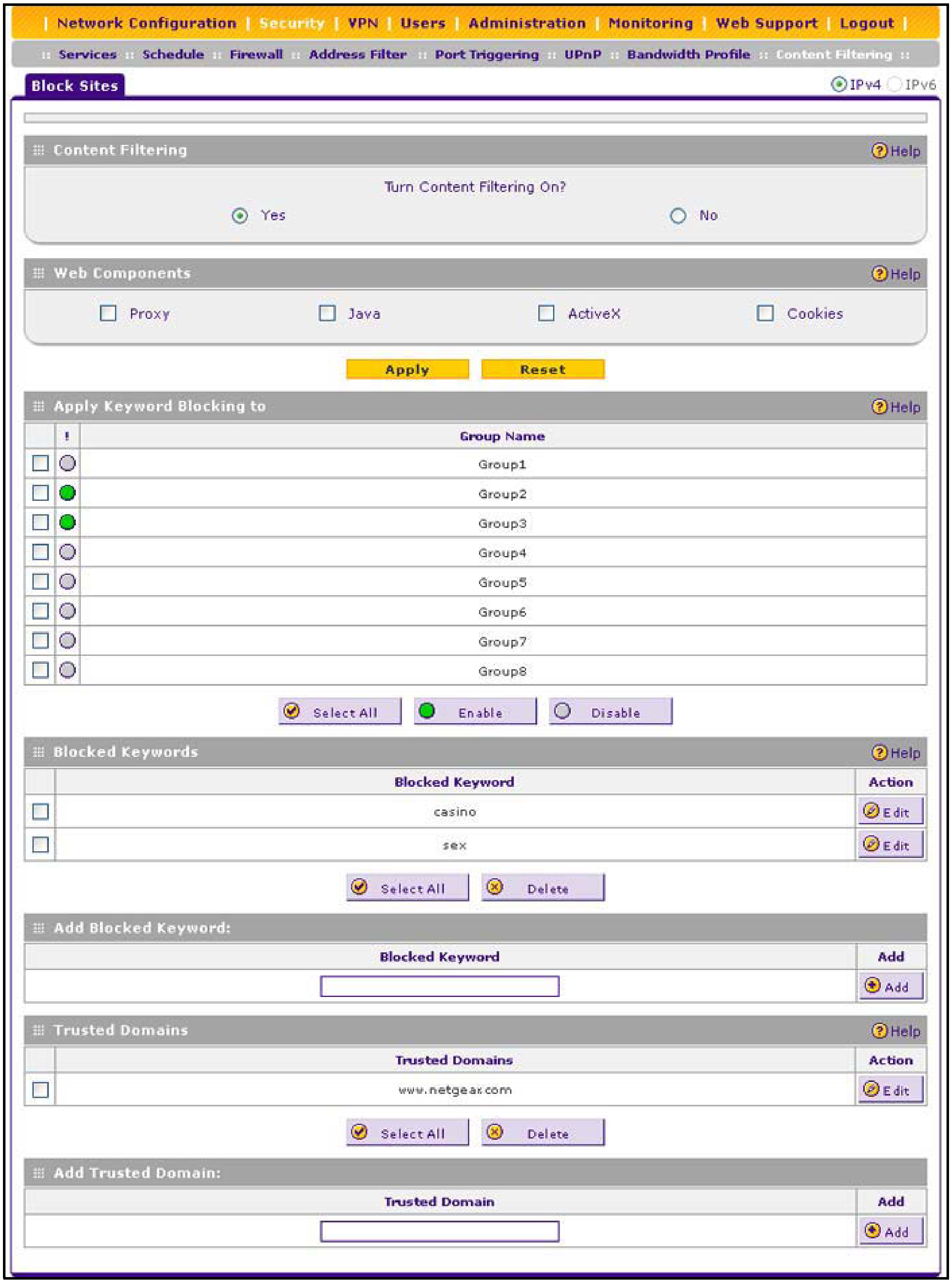
b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Content Filtering**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Block Sites
◉ IPv4 ○ IPv6
Help
Apply
Reset
Select All
Enable
Disable
Delete
Edit
Add

Content Filtering

Turn Content Filtering On?

◉ Yes ○ No

Web Components

□ Proxy □ Java □ ActiveX □ Cookies

Apply Keyword Blocking to

	!	Group Name
□	○	Group1
□	●	Group2
□	●	Group3
□	○	Group4
□	○	Group5
□	○	Group6
□	○	Group7
□	○	Group8

Blocked Keywords

	Blocked Keyword	Action
□	casino	Edit
□	sex	Edit

Add Blocked Keyword:

Blocked Keyword	Add
	Add

Trusted Domains

	Trusted Domains	Action
□	www.netgear.com	Edit

Add Trusted Domain:

Trusted Domain	Add
	Add

3. In the Content Filtering section, select the **Yes** radio button.

4. In the Web Components section, 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.

For more information, see *Configure Content Filtering* on page 189.

5. Click the **Apply** button.

   Your changes are saved.

➢ To apply keyword blocking to LAN groups:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Security > Content Filtering**.

   The Block Sites screen displays.
3. In the Apply Keyword Blocking to section, 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.
4. To activate keyword blocking for these groups, click the **Enable** button.

   To deactivate keyword blocking for the selected groups, click the **Disable** button.

   If you changed the LAN group names on the Edit Group Names screen, the new names are displayed on the Block Sites screen. For more information, see *Change Group Names in the Network Database* on page 77.
5. Click the **Apply** button.

   Your changes are saved.

➢ To build your list of blocked keywords or blocked domain names:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Content Filtering**.

   The Block Sites screen displays.

3. In the Add Blocked Keyword section, in the **Blocked Keyword** field, enter a keyword or domain name.
4. After each entry, click the **Add** table button.

   The keyword or domain name is added to the Blocked Keywords table.

5. To edit an entry, in the Action column to the right of the entry, click the **Edit** table button.

   For more information, see *Configure Content Filtering* on page 189.

6. Click the **Apply** button.

   Your changes are saved.

➤ **To build your list of trusted domains:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Content Filtering**.

   The Block Sites screen displays.

3. In the Add Trusted Domain section, in the **Trusted Domains** field, enter a domain name.
4. After each entry, click the **Add** table button.

   The domain name is added to the Trusted Domains table.

5. To edit an entry, in the Action column to the right of the entry, click the **Edit** table button.

   For more information, see *Configure Content Filtering* on page 189.

6. Click the **Apply** button.

   Your changes are saved.

Set a Schedule to Block or Allow Specific Traffic

Schedules define the time frames under which firewall rules can be applied. You can define three schedules, Schedule 1, Schedule 2, and Schedule 3, and you can select any one of these when defining firewall rules.

➢ **To set a schedule:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

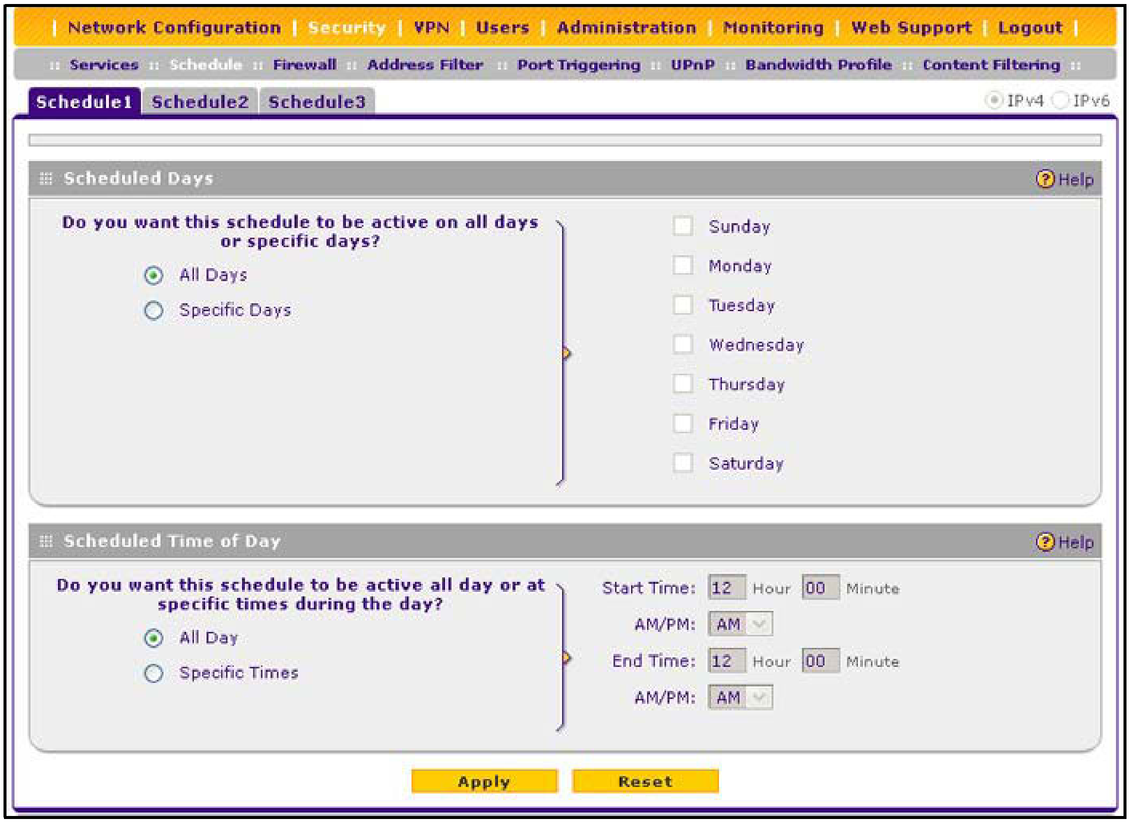
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Services > Schedule 1**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Schedule1
Schedule2
Schedule3
● IPv4 ○ IPv6
Help
Help
Apply
Reset

Scheduled Days

Do you want this schedule to be active on all days or specific days?

● All Days

○ Specific Days

□ Sunday

□ Monday

□ Tuesday

□ Wednesday

□ Thursday

□ Friday

□ Saturday

Scheduled Time of Day

Do you want this schedule to be active all day or at specific times during the day?

● All Day

○ Specific Times

Start Time: 12 Hour 00 Minute

AM/PM: AM

End Time: 12 Hour 00 Minute

AM/PM: AM

3. In the Scheduled Days section, select one of the following radio buttons:
   - **All Days**. The schedule is in effect all days of the week.
   - **Specific Days**. The schedule is 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.
4. In the Scheduled Time of Day section, select one of the following radio buttons:
   - **All Day**. The schedule is in effect all hours of the selected day or days.
   - **Specific Times**. The schedule is 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.
5. Click the **Apply** button.

   Your changes are saved to Schedule 1.
6. Repeat these steps to set to a schedule for Schedule 2 and Schedule 3.

Enable Source MAC Filtering

You can 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.

For additional ways of restricting outbound traffic, see *Outbound Rules* on page 128.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

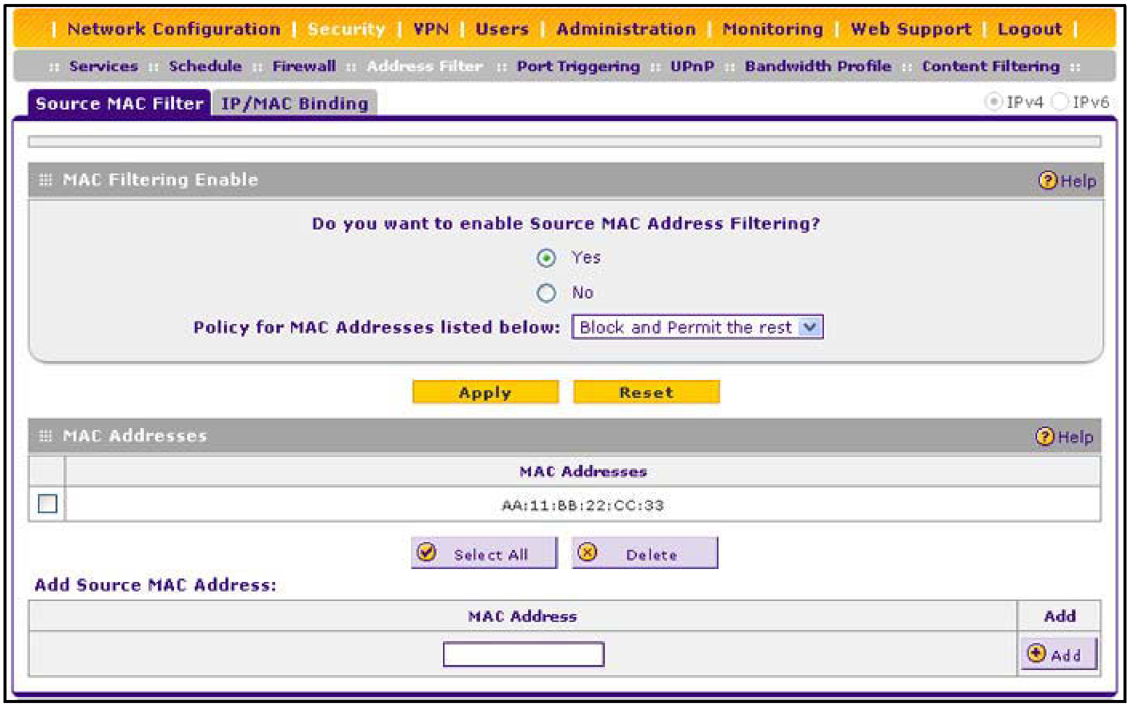
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Source MAC Filter | IP/MAC Binding
IPv4 IPv6
Help
Apply
Reset
Help
Select All
Delete
Add

MAC Filtering Enable

Do you want to enable Source MAC Address Filtering?

● Yes

○ No

Policy for MAC Addresses listed below: Block and Permit the rest

MAC Addresses

	MAC Addresses
□	AA:11:BB:22:CC:33

Add Source MAC Address:

MAC Address	Add
	Add

3. In the MAC Filtering Enable section, select the **Yes** radio button.

4. In the same section, from the **Policy for MAC Addresses listed below** 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.

5. Click the **Apply** button.

   Your changes are saved.

6. Build your list of source MAC addresses to be permitted or blocked by entering the first MAC address in the **MAC Address** field.

   A MAC address must be entered in the format xx:xx:xx:xx:xx:xx, in which x is a numeric (0 to 9) or a letter between a and f or A and F (inclusive), for example: aa:11:bb:22:cc:33.

⚠ WARNING:

If you select Permit and Block the rest from the 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.

7. Click the **Add** table button.

   The MAC address is added to the MAC Addresses table.

8. To add more MAC addresses to the MAC Addresses table, repeat the previous two steps.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter**.

   The Source MAC Filter screen displays.

3. 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.

4. Click the **Delete** table button.

   The information is deleted.

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 must be enabled on the VPN firewall. If the VPN firewall detects packets with an IP address that matches the IP address in the IP/MAC Bindings table but does not match the related MAC address in the IP/MAC Bindings table (or the other way around), the packets are dropped. If you enabled the logging option for the IP/MAC binding feature, these packets are logged before they are dropped. The VPN firewall displays the total number of dropped packets that violate either the IP-to-MAC binding or the MAC-to-IP binding.

You can bind IP addresses to MAC addresses for DHCP assignment on the LAN Groups screen. For more information, see *Manage the Network Database* on page 73.

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)

Three scenarios are possible in relation to the addresses in the IP/MAC Bindings table:

- Host 1 did not change its IP and MAC addresses. The IP and MAC addresses of a packet coming from Host 1 match those in the IP/MAC Bindings table.
- Host 2 changed its MAC address to 00:01:02:03:04:09. The IP address of the packet matches the IP address in the IP/MAC Bindings table but its MAC address does not match the MAC address in the IP/MAC Bindings table.
- Host 3 changed its IP address to 192.168.10.15. The MAC address of the packet matches the MAC address in the IP/MAC Bindings table but its IP address does not match the IP address in the IP/MAC Bindings table.

In this example, the VPN firewall blocks the traffic coming from Host 2 and Host 3 but allows the traffic coming from Host 1 to any external network. The total count of dropped packets is displayed.

IPv4/MAC Bindings

➤ **To set up a binding between a MAC address and an IPv4 address:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

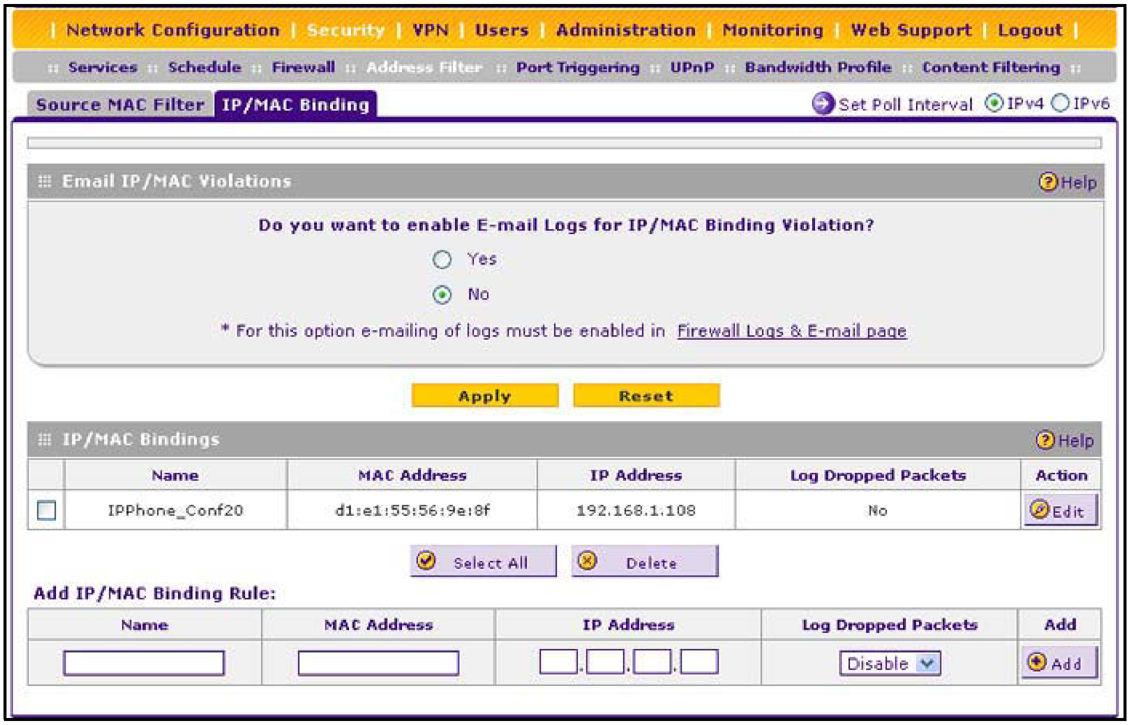
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter > IP/MAC Binding**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Source MAC Filter
IP/MAC Binding
Set Poll Interval
● IPv4 ○ IPv6
Help
Apply
Reset
Help
Select All
Delete
Edit
Add

Email IP/MAC Violations

Do you want to enable E-mail Logs for IP/MAC Binding Violation?

○ Yes

● No

* For this option e-mailing of logs must be enabled in Firewall Logs & E-mail page

IP/MAC Bindings

	Name	MAC Address	IP Address	Log Dropped Packets	Action
□	IPPhone_Conf20	d1:e1:55:56:9e:8f	192.168.1.108	No	Edit

Add IP/MAC Binding Rule:

Name	MAC Address	IP Address	Log Dropped Packets	Add
		. . .	Disable	Add

3. In the Email IP/MAC Violations section, specify if you want to enable email logs for IP/MAC binding violations.

You must 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 353).
- **No**. IP/MAC binding violations are not emailed.

4. Click the **Apply** button.

Your changes are saved.

5. In the IP/MAC Bindings sections of the screen, enter the settings as described in the following table:

Table 38. 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.

Table 38. IP/MAC Binding screen settings for IPv4 (continued)

Setting	Description
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 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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays.
3. In the IP/MAC Bindings table to the right of the IP/MAC binding that you want to edit, click the **Edit** table button.

   The Edit IP/MAC Binding screen displays.
4. Modify the settings that you wish to change.

   See *Table 38* on page 200. You can change the MAC address, IPv4 address, and logging status.
5. Click the **Apply** button.

   Your changes are saved.

➢ To remove one or more IP/MAC bindings from the table:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter > IP/MAC Binding**.

The IP/MAC Binding screen displays.

3. 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.

4. Click the **Delete** table button.

The information is deleted.

➤ **To change the IPv4 MAC polling interval from its default setting of 10 seconds:**

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

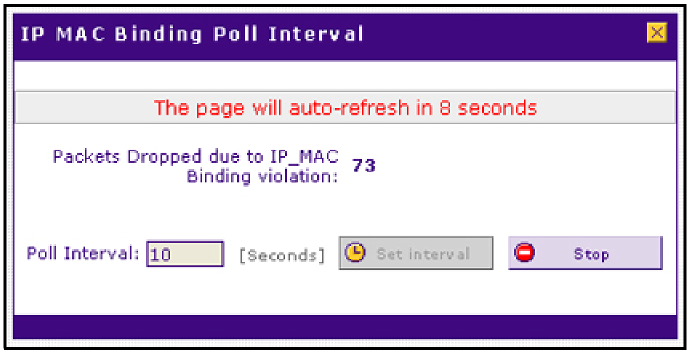
c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter > IP/MAC Binding**.

The IP/MAC Binding screen displays.

3. On the IP/MAC Bindings screen for IPv4, to the right of the IP/MAC Binding tab, click the **Set Poll Interval** option arrow.



IP MAC Binding Poll Interval

The page will auto-refresh in 8 seconds

Packets Dropped due to IP_MAC Binding violation: 73

Poll Interval: 10 [Seconds]

4. Click the **Stop** button.

Wait until the **Poll Interval** field becomes available.

5. Enter new poll interval in seconds.
6. Click the **Set Interval** button.

   Wait for the confirmation that the operation succeeded before you close the window.

IPv6/MAC Bindings

➢ **To set up a binding between a MAC address and an IPv6 address:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

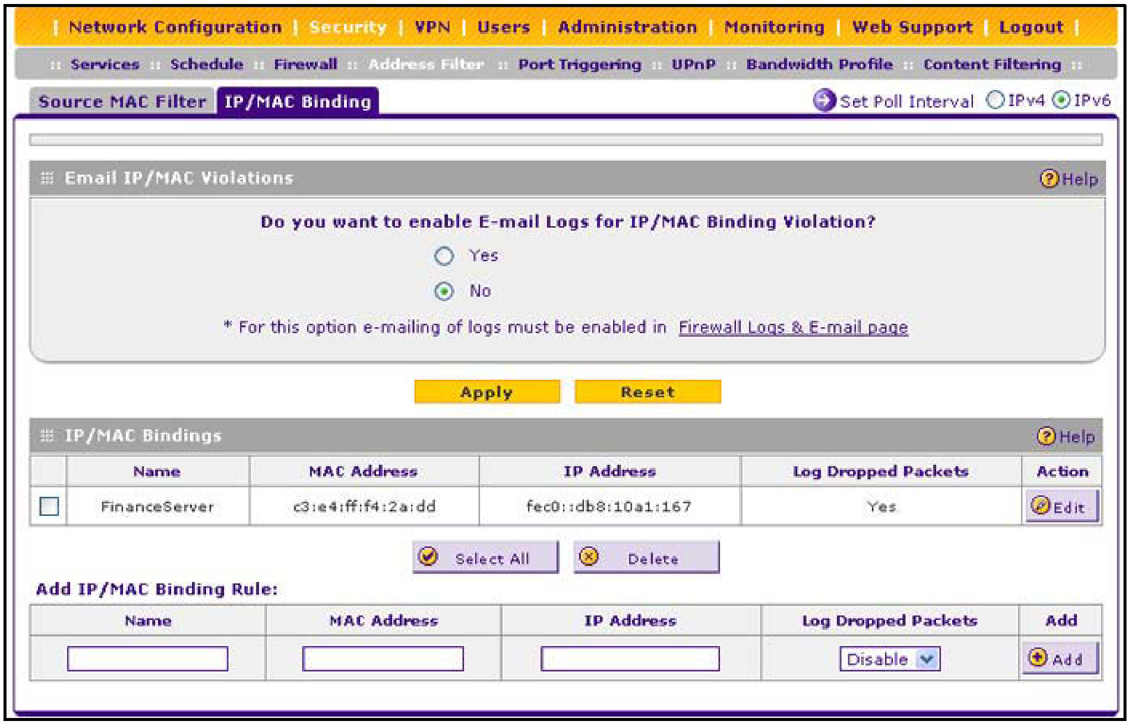
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays.

3. Select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Source MAC Filter
IP/MAC Binding
Set Poll Interval
○ IPv4 ● IPv6
Email IP/MAC Violations
Help
Apply
Reset
IP/MAC Bindings
Help
Select All
Delete

Do you want to enable E-mail Logs for IP/MAC Binding Violation?

○ Yes

● No

* For this option e-mailing of logs must be enabled in Firewall Logs & E-mail page

	Name	MAC Address	IP Address	Log Dropped Packets	Action
□	FinanceServer	c3:e4:ff:f4:2a:dd	fec0::db8:10a1:167	Yes	Edit

Add IP/MAC Binding Rule:

Name	MAC Address	IP Address	Log Dropped Packets	Add
			Disable	Add

4. In the Email IP/MAC Violations section, specify if you want to enable email logs for IP/MAC binding violations.

   You must 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.

     For more information, see *Configure Logging, Alerts, and Event Notifications* on page 353.

   - **No**. IP/MAC binding violations are not emailed.

5. Click the **Apply** button.

   Your changes are saved.

6. In the IP/MAC Bindings sections, enter the settings as described in the following table:

Table 39. 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 list. The default setting is Disable.

7. 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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays.

3. In the IP/MAC Bindings table to the right of the IP/MAC binding that you want to edit, click the **Edit** table button.

   The Edit IP/MAC Binding screen displays.

4. Modify the settings that you wish to change.

   See *Table 39* on page 204. You can change the MAC address, IPv6 address, and logging status.

5. Click the **Apply** button.

   Your changes are saved.

➢ **To remove one or more IP/MAC bindings from the table:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays.

3. 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.
4. Click the **Delete** table button.

   The information is deleted.

➢ **To change the IPv6 MAC polling interval from its default setting of 10 seconds:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

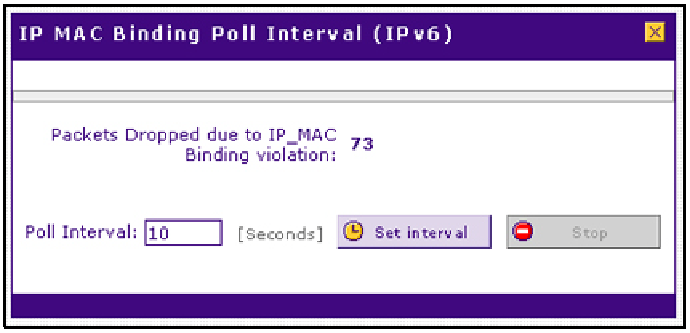
   c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays.

3. On the IP/MAC Bindings screen for IPv6, to the right of the IP/MAC Binding tab, click the **Set Poll Interval** option arrow.



IP MAC Binding Poll Interval (IPv6)

Packets Dropped due to IP_MAC Binding violation: 73

Poll Interval: 10 [Seconds]

4. Click the **Stop** button.

   Wait until the **Poll Interval** field becomes available.

5. Enter new poll interval in seconds.
6. Click the **Set Interval** button.

   Wait for the confirmation that the operation succeeded before you close the window.

Configure Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port triggering feature requires that you know the port numbers used by the application.

Note: Port triggering is supported for IPv4 devices only.

Once configured, port triggering operates as follows:

1. A computer makes an outgoing connection using a port number that is defined in the Port Triggering Rules table.
2. The VPN firewall records this connection, opens the additional incoming port or ports that are associated with the rule in the port triggering table and associates them with the computer.
3. The remote system receives the computer’s request and responds using the incoming port or ports that are associated with the rule in the port triggering table on the VPN firewall.
4. The VPN firewall matches the response to the previous request and forwards the response to the computer.

Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a request from the LAN network. As such, it would be handled in accordance with the inbound port forwarding rules and most likely would be blocked.

Note these restrictions on port triggering:

- Only one computer can use a port triggering application at any time.
- After a computer finishes using a port triggering application, a short time-out period passes before the application can be used by another computer. This time-out period is required so the VPN firewall can determine that the application terminates.

Note: For additional ways of allowing inbound traffic, see *Inbound Rules* on page 130.

➢ **To add a port triggering rule:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

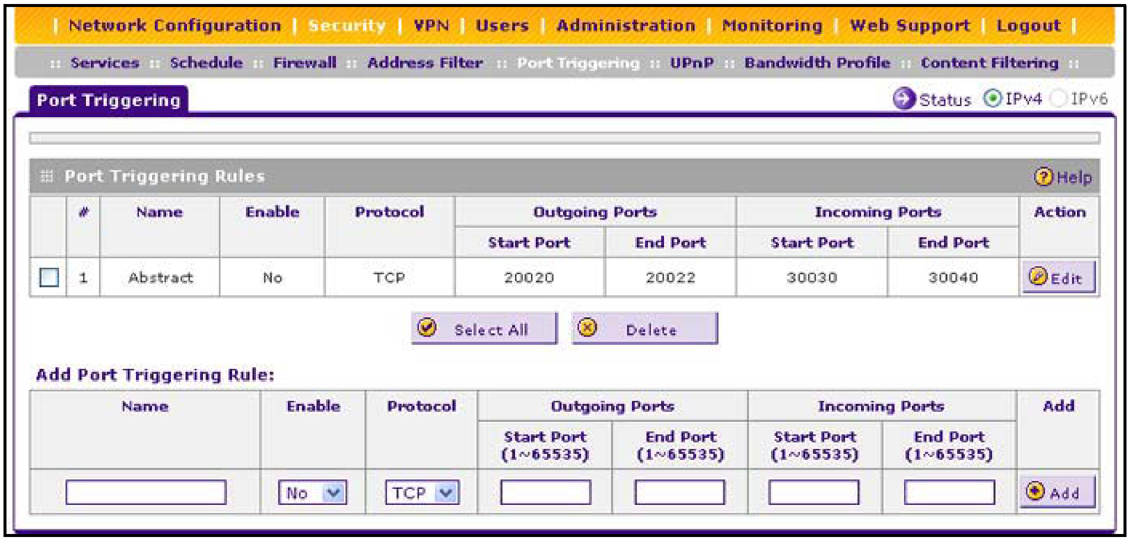
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Port Triggering**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Port Triggering
Status ● IPv4 ○ IPv6
Help
Select All
Delete
Edit
Add

Port Triggering Rules

	#	Name	Enable	Protocol	Outgoing Ports		Incoming Ports		Action
					Start Port	End Port	Start Port	End Port	
☐	1	Abstract	No	TCP	20020	20022	30030	30040	Edit

Add Port Triggering Rule:

Name	Enable	Protocol	Outgoing Ports		Incoming Ports		Add
			Start Port (1~65535)	End Port (1~65535)	Start Port (1~65535)	End Port (1~65535)	
	No	TCP					Add

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

Table 40. Port Triggering screen settings

Setting	Description	
Name	A descriptive name of the rule for identification and management purposes.	
Enable	From the list, select **Yes** to enable the rule. (You can define a rule but not enable it.) The default setting is No.	
Protocol	From the 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.

4. 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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Port Triggering**.

   The Port Triggering screen displays.

3. In the Port Triggering Rules table to the right of the port triggering rule that you want to edit, click the **Edit** table button.

   The Edit Port Triggering Rule screen displays.

4. Modify the settings that you wish to change.

   See *Table 40* on page 208.

5. Click the **Apply** button.

   Your changes are saved.

➢ To remove one or more port triggering rules from the table:

1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Security > Port Triggering**.

   The Port Triggering screen displays.
3. 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.
4. Click the **Delete** table button.

   The information is deleted.

➢ To display the status of the port triggering rules:

1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

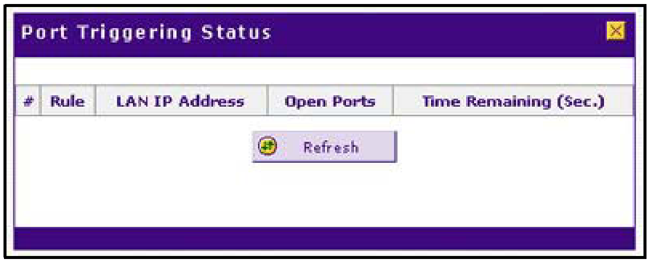
     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Security > Port Triggering**.

   The Port Triggering screen displays.

3. In the upper right of the Port Triggering screen, click the **Status** option arrow.



Port Triggering Status

#	Rule	LAN IP Address	Open Ports	Time Remaining (Sec.)

Configure Universal Plug and Play

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

➤ **To configure UPnP:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

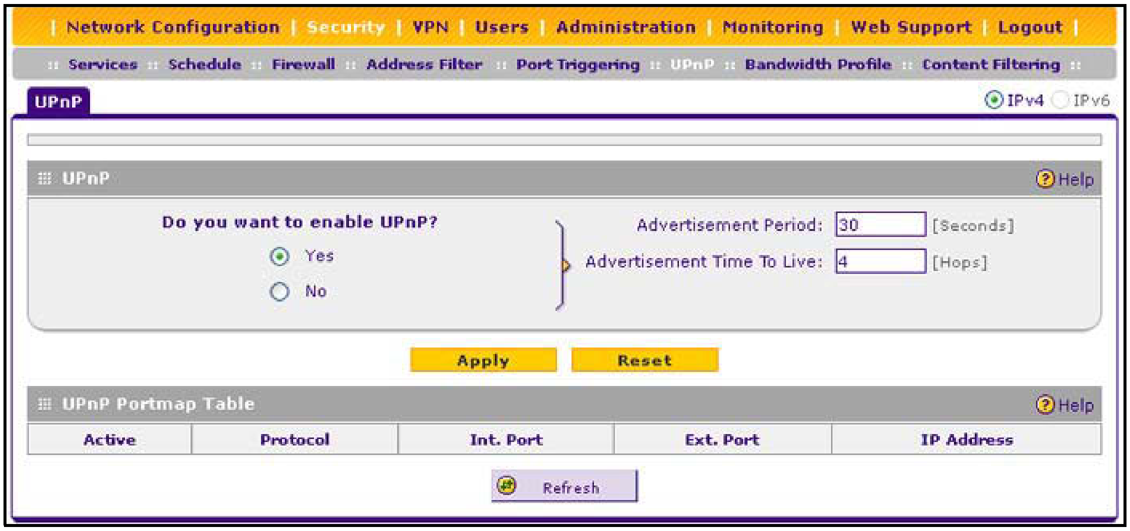
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > UPnP**.



| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
UPnP
● IPv4 ○ IPv6
UPnP
Help

Do you want to enable UPnP?

● Yes

○ No

Advertisement Period: 30 [Seconds]

Advertisement Time To Live: 4 [Hops]

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

The UPnP Portmap Table in the lower part of the screen shows the IP addresses and other settings of UPnP devices that accessed the VPN firewall and that were automatically detected by the VPN firewall:

- **Active**. A Yes or No indicates if the UPnP device port that established a connection is active or inactive.
- **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.

3. To enable the UPnP feature, select the **Yes** radio button.

   The feature is disabled by default. To disable the feature, select the **No** radio button.

4. Complete the following fields:
   - **Advertisement Period**. Enter the period in seconds that specifies how often the VPN firewall broadcasts 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 4 hops.

5. Click the **Apply** button.

   Your changes are saved.

To refresh the contents of the UPnP Portmap Table, click the **Refresh** button.

Virtual Private Networking Using IPSec and L2TP Connections

5

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

- *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*
- *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.

Note: Although the VPN firewall supports IPv6, the NETGEAR ProSafe VPN Client supports IPv4 only; a future release of the VPN client might support IPv6.

Configuring a VPN tunnel connection requires that you specify all settings on both sides of the VPN tunnel to match or mirror each other precisely, which can be a daunting task. The VPN Wizard efficiently guides you through the setup procedure with a series of questions that determine the IPSec keys and VPN policies it sets up. The VPN Wizard also configures the settings for the network connection: security association (SA), traffic selectors, authentication algorithm, and encryption. The settings that the VPN Wizard uses are based on the recommendations of the VPN Consortium (VPNC), an organization that promotes multivendor VPN interoperability.

The following sections provide wizard and NETGEAR ProSafe VPN Client software configuration procedures:

- *Create an IPv4 Gateway-to-Gateway VPN Tunnel with the Wizard*
- *Create an IPv6 Gateway-to-Gateway VPN Tunnel with the Wizard*
- *Create an IPv4 Client-to-Gateway VPN Tunnel with the Wizard*

Create an IPv4 Gateway-to-Gateway VPN Tunnel with the Wizard

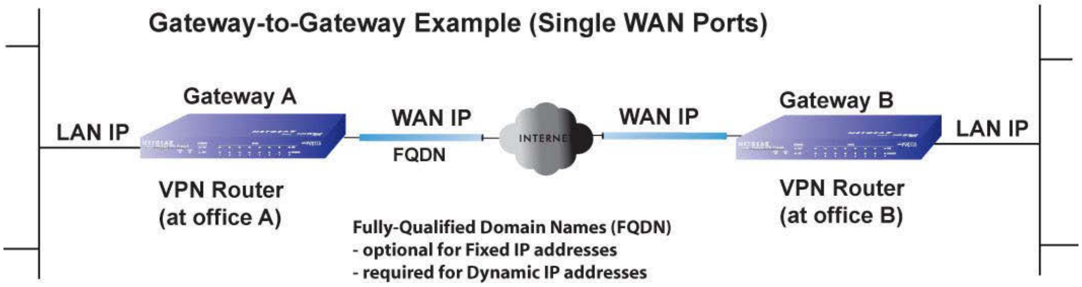

Gateway-to-Gateway Example (Single WAN Ports)
Gateway A
LAN IP
WAN IP
FQDN
INTERNET
WAN IP
Gateway B
LAN IP
VPN Router
(at office A)
VPN Router
(at office B)
Fully-Qualified Domain Names (FQDN)
- optional for Fixed IP addresses
- required for Dynamic IP addresses

Figure 16. Example of VPN tunnel

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 277.

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.

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 the option to configure the update interval is available, set the interval to an appropriately short time.

➤ **To set up an IPv4 gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

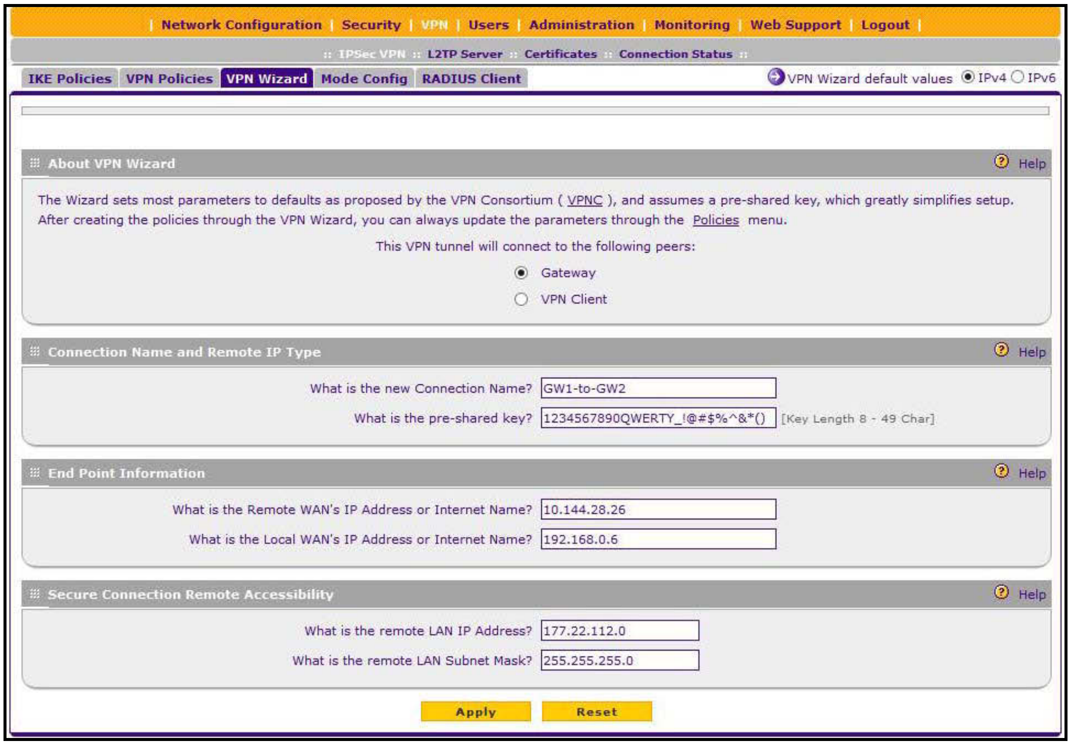
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Wizard**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
VPN Wizard default values ● IPv4 ○ IPv6
About VPN Wizard
Help
Connection Name and Remote IP Type
Help
End Point Information
Help
Secure Connection Remote Accessibility
Help
Apply
Reset

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers:

● Gateway

○ VPN Client

What is the new Connection Name? GW1-to-GW2

What is the pre-shared key? 1234567890QWERTY_!@#$%^&*() [Key Length 8 - 49 Char]

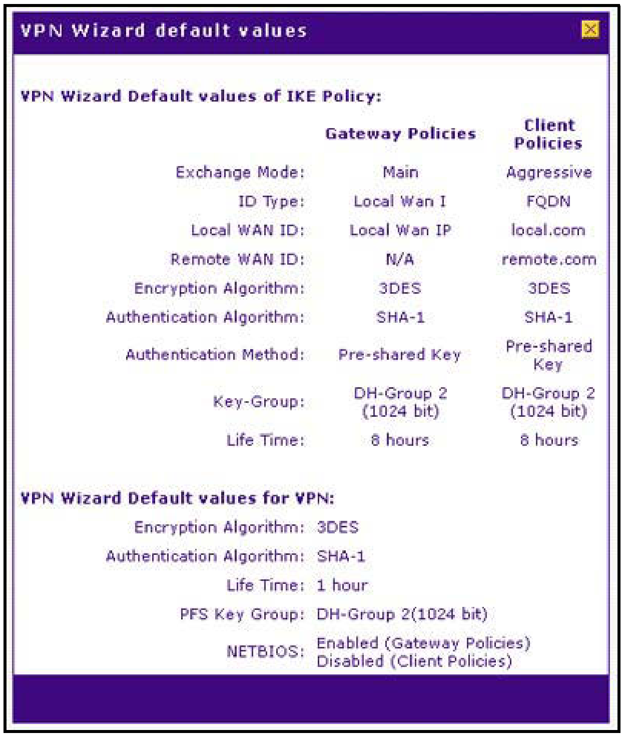
What is the Remote WAN's IP Address or Internet Name? 10.144.28.26

What is the Local WAN's IP Address or Internet Name? 192.168.0.6

What is the remote LAN IP Address? 177.22.112.0

What is the remote LAN Subnet Mask? 255.255.255.0

3. To view the wizard default settings, in the upper right of the screen, click the **VPN Wizard default values** option arrow.



VPN Wizard default values

VPN Wizard Default values of IKE Policy:

	Gateway Policies	Client Policies
Exchange Mode:	Main	Aggressive
ID Type:	Local Wan I	FQDN
Local WAN ID:	Local Wan IP	local.com
Remote WAN ID:	N/A	remote.com
Encryption Algorithm:	3DES	3DES
Authentication Algorithm:	SHA-1	SHA-1
Authentication Method:	Pre-shared Key	Pre-shared Key
Key-Group:	DH-Group 2 (1024 bit)	DH-Group 2 (1024 bit)
Life Time:	8 hours	8 hours

VPN Wizard Default values for VPN:

Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Life Time:	1 hour
PFS Key Group:	DH-Group 2(1024 bit)
NETBIOS:	Enabled (Gateway Policies) Disabled (Client Policies)

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

Table 41. 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.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key must be entered both here and on the remote VPN gateway. This key must be a minimum of 8 characters and must 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, the IPv4 address of the VPN firewall’s active WAN interface is automatically entered.

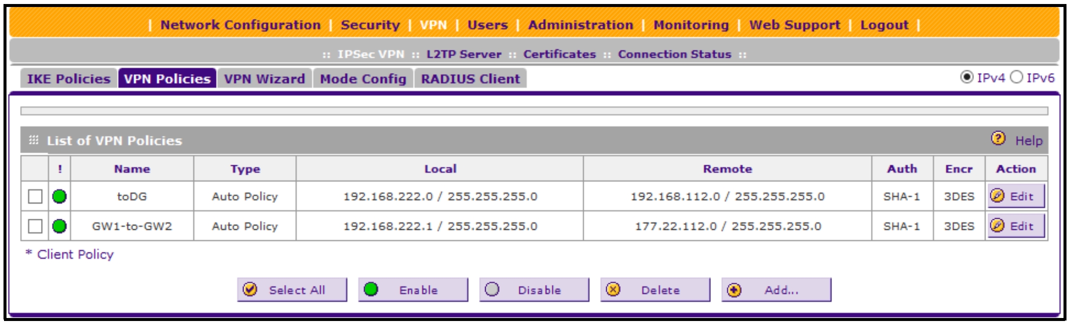
Table 41. IPSec VPN Wizard settings for an IPv4 gateway-to-gateway tunnel (continued)

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 must 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 must be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

5. Click the **Apply** button.

   Your changes are saved.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
List of VPN Policies
Help

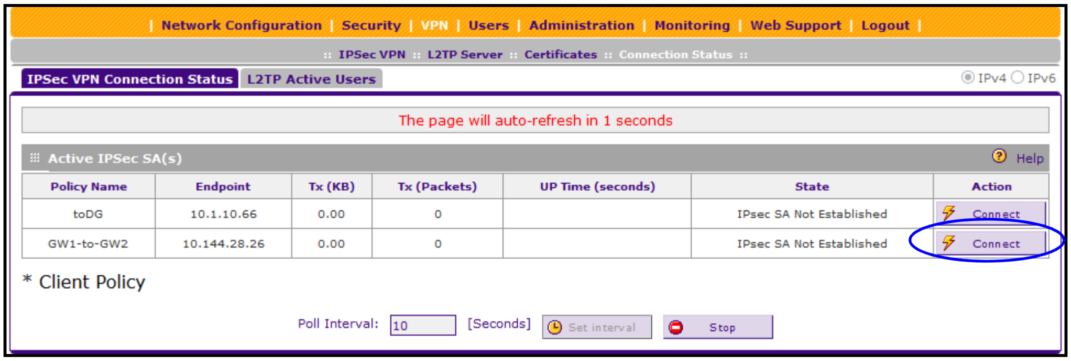
	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	toDG	Auto Policy	192.168.222.0 / 255.255.255.0	192.168.112.0 / 255.255.255.0	SHA-1	3DES	Edit
□	●	GW1-to-GW2	Auto Policy	192.168.222.1 / 255.255.255.0	177.22.112.0 / 255.255.255.0	SHA-1	3DES	Edit

* Client Policy

Select All
Enable
Disable
Delete
Add...

6. Configure a VPN policy on the remote gateway that allows connection to the VPN firewall.
7. Activate the IPSec VPN connection:

   a. Select **VPN > Connection Status**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
L2TP Active Users
● IPv4 ○ IPv6

The page will auto-refresh in 1 seconds

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	UP Time (seconds)	State	Action
toDG	10.1.10.66	0.00	0		IPsec SA Not Established	Connect
GW1-to-GW2	10.144.28.26	0.00	0		IPsec SA Not Established	Connect

* Client Policy

Poll Interval: 10 [Seconds]

   b. Locate the policy in the table, and click the **Connect** table button.

   The IPSec VPN connection becomes active.

Create an IPv6 Gateway-to-Gateway VPN Tunnel with the Wizard

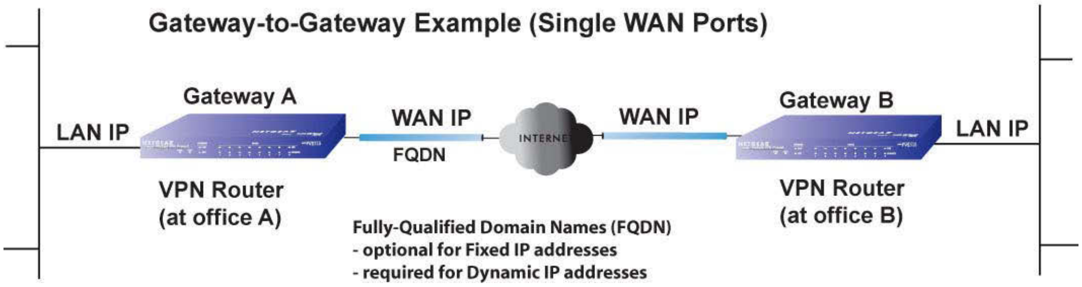

Gateway-to-Gateway Example (Single WAN Ports)
Gateway A
LAN IP
WAN IP
FQDN
INTERNET
WAN IP
Gateway B
LAN IP
VPN Router
(at office A)
VPN Router
(at office B)
Fully-Qualified Domain Names (FQDN)
- optional for Fixed IP addresses
- required for Dynamic IP addresses

Figure 17. Example of VPN tunnel

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 277.

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.

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 the option to configure the update interval is available, set the interval to an appropriately short time.

➤ **To set up an IPv6 gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

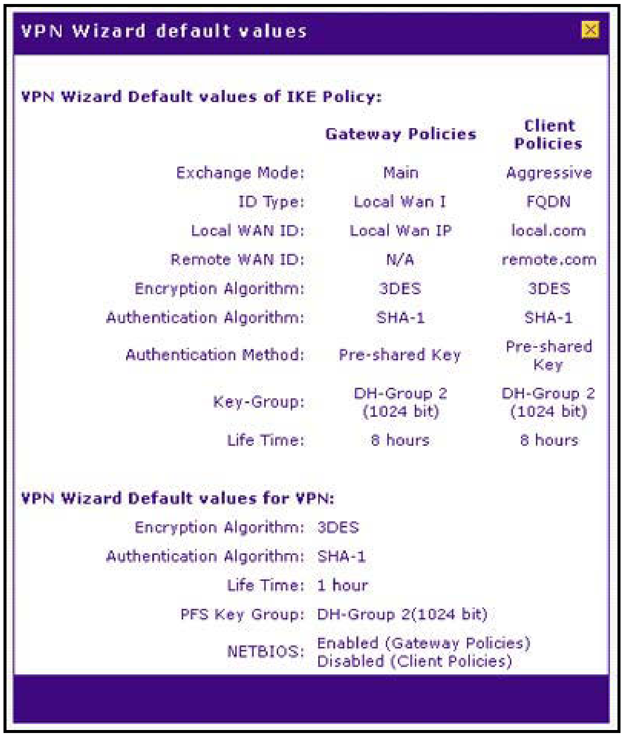
      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays.

3. In the upper right of the screen, select the **IPv6** radio button.

4. To view the wizard default settings, in the upper right of the screen, click the **VPN Wizard default values** option arrow.



VPN Wizard default values

VPN Wizard Default values of IKE Policy:

	Gateway Policies	Client Policies
Exchange Mode:	Main	Aggressive
ID Type:	Local Wan I	FQDN
Local WAN ID:	Local Wan IP	local.com
Remote WAN ID:	N/A	remote.com
Encryption Algorithm:	3DES	3DES
Authentication Algorithm:	SHA-1	SHA-1
Authentication Method:	Pre-shared Key	Pre-shared Key
Key-Group:	DH-Group 2 (1024 bit)	DH-Group 2 (1024 bit)
Life Time:	8 hours	8 hours

VPN Wizard Default values for VPN:

Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Life Time:	1 hour
PFS Key Group:	DH-Group 2(1024 bit)
NETBIOS:	Enabled (Gateway Policies) Disabled (Client Policies)

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

Table 42. 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.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key must be entered both here and on the remote VPN gateway. This key must be a minimum of 8 characters and must 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, the IPv6 address of the VPN firewall’s active WAN interface is automatically entered.

Table 42. 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 must 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 must be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

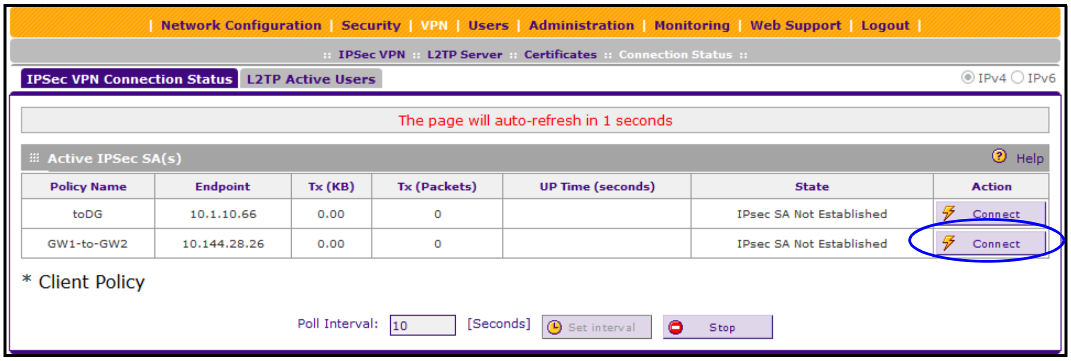
6. Click the **Apply** button.

   Your changes are saved.

7. Configure a VPN policy on the remote gateway that allows connection to the VPN firewall.

8. Activate the IPSec VPN connection:

   a. Select **VPN > Connection Status**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
L2TP Active Users
● IPv4 ○ IPv6
Active IPSec SA(s)
Help
Set interval
Stop

The page will auto-refresh in 1 seconds

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	UP Time (seconds)	State	Action
toDG	10.1.10.66	0.00	0		IPsec SA Not Established	Connect
GW1-to-GW2	10.144.28.26	0.00	0		IPsec SA Not Established	Connect

* Client Policy

Poll Interval: 10 [Seconds]

   b. Locate the policy in the table, and click the **Connect** table button.

   The IPSec VPN connection becomes active.

Create an IPv4 Client-to-Gateway VPN Tunnel with the Wizard

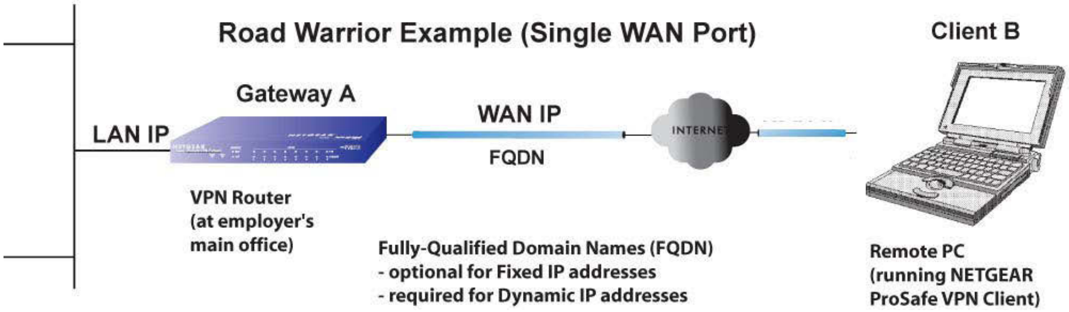

Road Warrior Example (Single WAN Port)
Client B
Gateway A
LAN IP
WAN IP
FQDN
INTERNET
VPN Router
(at employer's
main office)
Fully-Qualified Domain Names (FQDN)
- optional for Fixed IP addresses
- required for Dynamic IP addresses
Remote PC
(running NETGEAR
ProSafe VPN Client)

Figure 18. Example of VPN tunnel

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*
- *Use the NETGEAR VPN Client Wizard to Create a Secure Connection*
- *Manually Create a Secure Connection Using the NETGEAR VPN Client*

Use the VPN Wizard to Configure the Gateway for a Client Tunnel

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 the option to configure the update interval is available, set the interval to an appropriately short time.

➤ **To set up a client-to-gateway VPN tunnel using the VPN Wizard:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

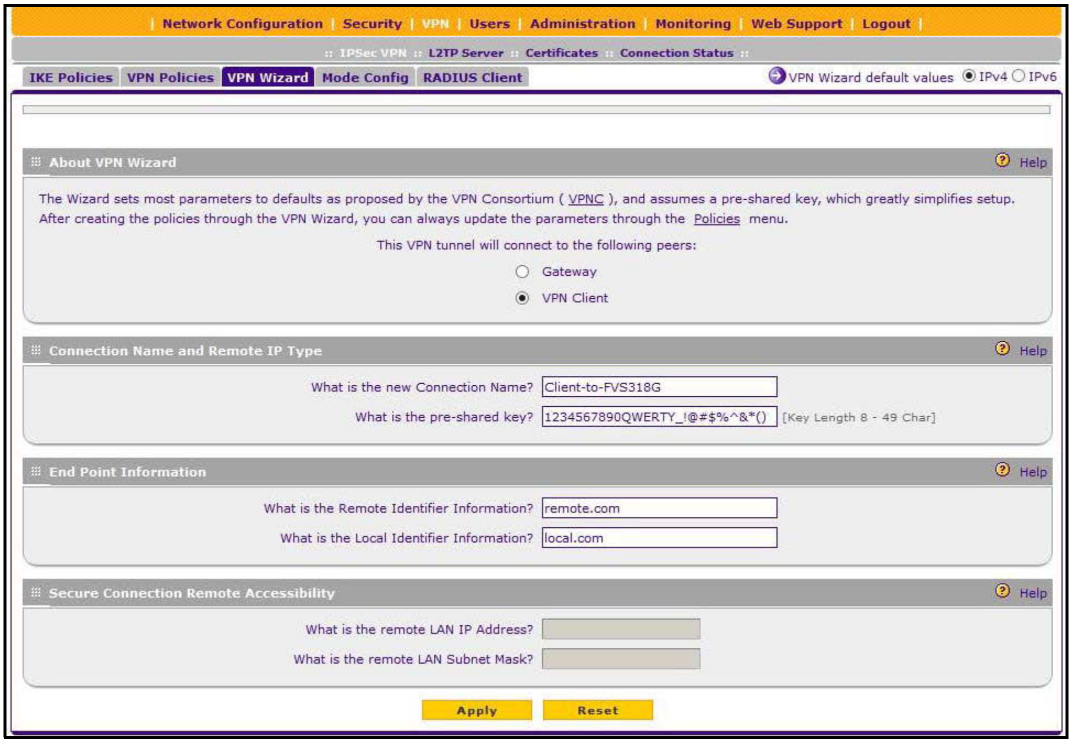
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Wizard**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
VPN Wizard default values
Help
Apply
Reset

● IPv4 ○ IPv6

About VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers:

○ Gateway
● VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? Client-to-FVS318G
What is the pre-shared key? 1234567890QWERTY_!@#$%^&*() [Key Length 8 - 49 Char]

End Point Information

What is the Remote Identifier Information? remote.com
What is the Local Identifier Information? local.com

Secure Connection Remote Accessibility

What is the remote LAN IP Address?
What is the remote LAN Subnet Mask?

3. To display the wizard default settings, in the upper right of the screen, click the **VPN Wizard default values** option arrow.

   A pop-up screen displays, showing the wizard default values. After you complete the wizard, you can modify these settings for the tunnel policy that you set up.

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

Table 43. 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.
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 must be entered both here and on the remote VPN gateway, or the remote VPN client. This key must be a minimum of 8 characters and cannot exceed 49 characters.

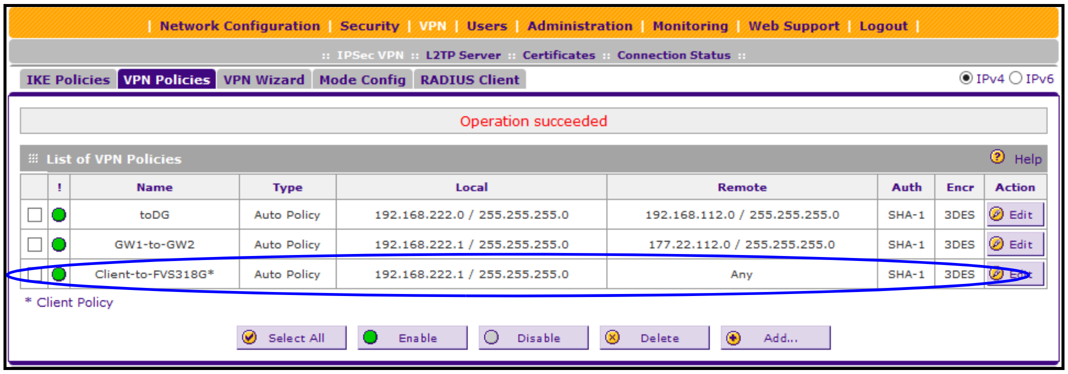
Table 43. IPSec VPN Wizard settings for a client-to-gateway tunnel (continued)

Setting	Description
End Point Information[a]	
What is the Remote Identifier Information?	When you select the **Client** radio button in the About VPN Wizard section, the default remote FQDN (remote.com) is automatically entered. Use the default remote FQDN, or enter another FQDN. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter **client.com** as the local ID on the VPN client.
What is the Local Identifier Information?	When you select the **Client** radio button in the About VPN Wizard section, the default local FQDN (local.com) is automatically entered. Use the default local FQDN, or enter another FQDN. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter **router.com** as the remote ID on the VPN client.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	These fields are masked out for VPN client connections.
What is the remote LAN Subnet Mask?	

a. Both local and remote endpoints must be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

5. Click the **Apply** button.

   Your changes are saved.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
Help
Select All
Enable
Disable
Delete
Add...

Operation succeeded

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	toDG	Auto Policy	192.168.222.0 / 255.255.255.0	192.168.112.0 / 255.255.255.0	SHA-1	3DES	Edit
□	●	GW1-to-GW2	Auto Policy	192.168.222.1 / 255.255.255.0	177.22.112.0 / 255.255.255.0	SHA-1	3DES	Edit
□	●	Client-to-FVS318G*	Auto Policy	192.168.222.1 / 255.255.255.0	Any	SHA-1	3DES	Edit

* Client Policy

6. (Optional) Collect the information that you must configure the VPN client.

You can print the following table to keep track of this information.

Table 44. 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

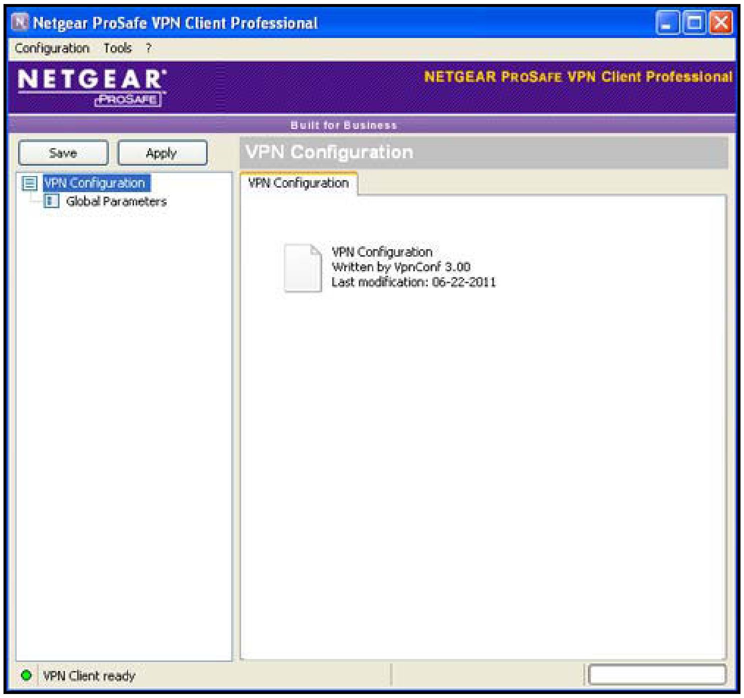
You can set up the VPN client in two different ways:

- **Configuration Wizard**. The Configuration Wizard configures the default settings and provides basic interoperability so that the VPN client can easily communicate with the VPN firewall (or third-party VPN devices). The Configuration Wizard does not let you enter the local and remote IDs, so you must manually enter this information. Of the two methods, the Configuration Wizard is the easier and preferred method. For more information, see *Use the NETGEAR VPN Client Wizard to Create a Secure Connection* on page 223.
- **Manual Method**. Instead of using the wizard on the VPN client, you can manually configure the VPN client. For more information, see *Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 228.

Note: Perform these tasks from a computer on which the NETGEAR ProSafe VPN Client is installed. The VPN client supports IPv4 only; a future release of the VPN client might support IPv6.

➤ **To use the Configuration Wizard to set up a VPN connection between the VPN client and the VPN firewall:**

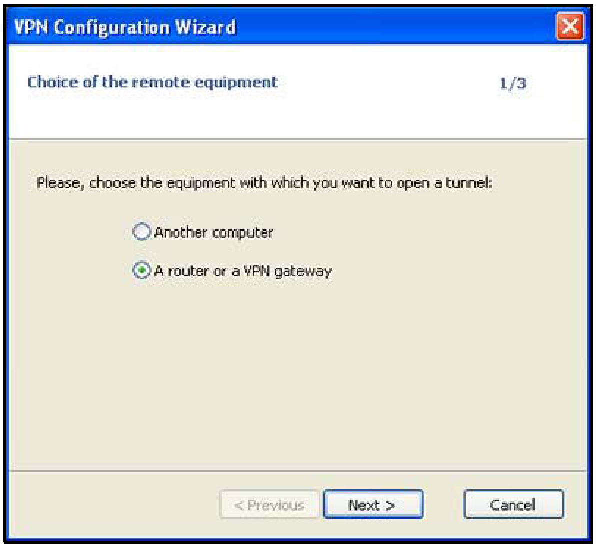
1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**.



VPN Configuration
Written by VpnConf 3.00
Last modification: 06-22-2011

VPN Client ready

2. From the main menu on the Configuration Panel screen, select **Configuration > Wizard**.



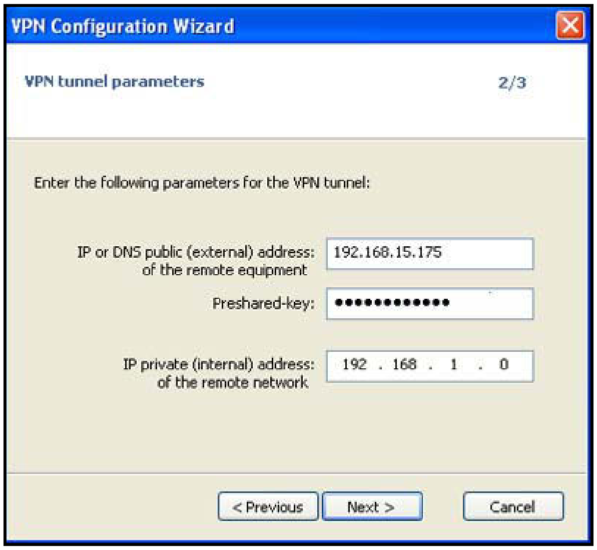
Choice of the remote equipment 1/3

Please, choose the equipment with which you want to open a tunnel:

○ Another computer

● A router or a VPN gateway

3. Select the **A router or a VPN gateway** radio button, and click the **Next** button.


VPN Configuration Wizard

VPN tunnel parameters 2/3

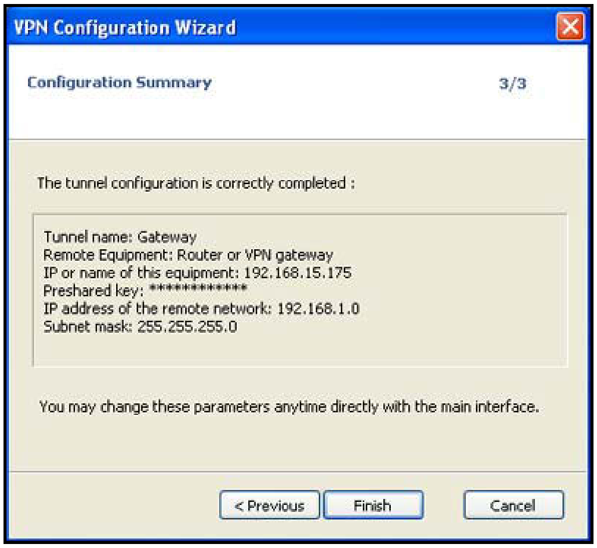
Enter the following parameters for the VPN tunnel:

IP or DNS public (external) address: of the remote equipment: 192.168.15.175

Preshared-key: ●●●●●●●●●●●●●

IP private (internal) address: of the remote network: 192 . 168 . 1 . 0

4. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. Enter the remote IP address or DNS name of the VPN firewall. For example, enter **192.168.15.175**.
   - **Preshared key**. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **I7!KL39dFG_8**.
   - **IP private (internal) address of the remote network**. Enter the remote private IP address of the VPN firewall. For example, enter **192.168.1.0**. This IP address enables communication with the entire 192.168.1.x subnet.
5. Click the **Next** button.


VPN Configuration Wizard

Configuration Summary 3/3

The tunnel configuration is correctly completed :

Tunnel name: Gateway
Remote Equipment: Router or VPN gateway
IP or name of this equipment: 192.168.15.175
Preshared key: *************
IP address of the remote network: 192.168.1.0
Subnet mask: 255.255.255.0

You may change these parameters anytime directly with the main interface.

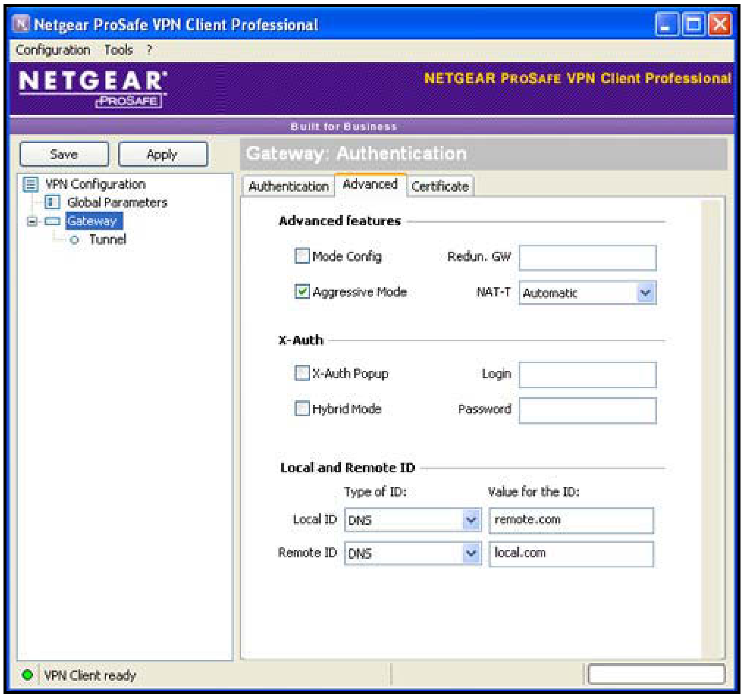
This screen is a summary screen of the new VPN configuration.

6. Click the **Finish** button.
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. In the Authentication pane, click the **Advanced** tab.



Advanced features

□ Mode Config Redun. GW

☑ Aggressive Mode NAT-T Automatic

X-Auth

□ X-Auth Popup Login

□ Hybrid Mode Password

Local and Remote ID

	Type of ID:	Value for the ID:
Local ID	DNS	remote.com
Remote ID	DNS	local.com

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

Table 45. VPN client advanced authentication settings

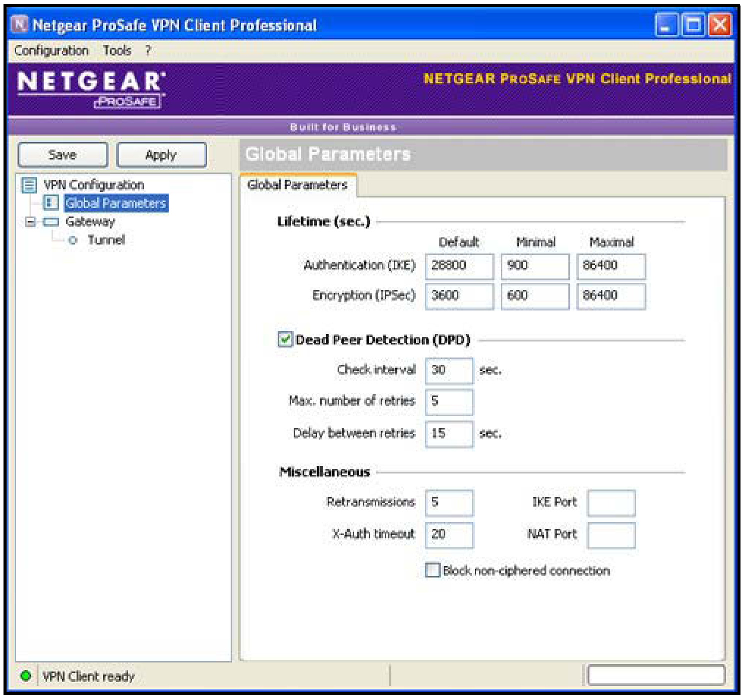
Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the VPN firewall.
NAT-T	Select **Automatic** from the list to enable the VPN client and VPN firewall to negotiate NAT-T.

Table 45. VPN client advanced authentication settings (continued)

Setting	Description
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **remote.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter **client.com** as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter **router.com** as the remote ID on the VPN client.

8. Configure the global parameters:

   a. In the left column of the Configuration Panel screen, click **Global Parameters**.



Lifetime (sec.)

	Default	Minimal	Maximal
Authentication (IKE)	28800	900	86400
Encryption (IPSec)	3600	600	86400

☑ Dead Peer Detection (DPD)

Check interval 30 sec.

Max. number of retries 5

Delay between retries 15 sec.

Miscellaneous

Retransmissions 5   IKE Port

X-Auth timeout 20   NAT Port

□ Block non-ciphered connection

   b. Specify the default lifetimes in seconds:

   - **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the VPN firewall.

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

9. To use the new settings immediately, click the **Apply** button.
10. To keep the settings for future use, click the **Save** button.

    The VPN client configuration is now complete.

Manually Create a Secure Connection Using the NETGEAR VPN Client

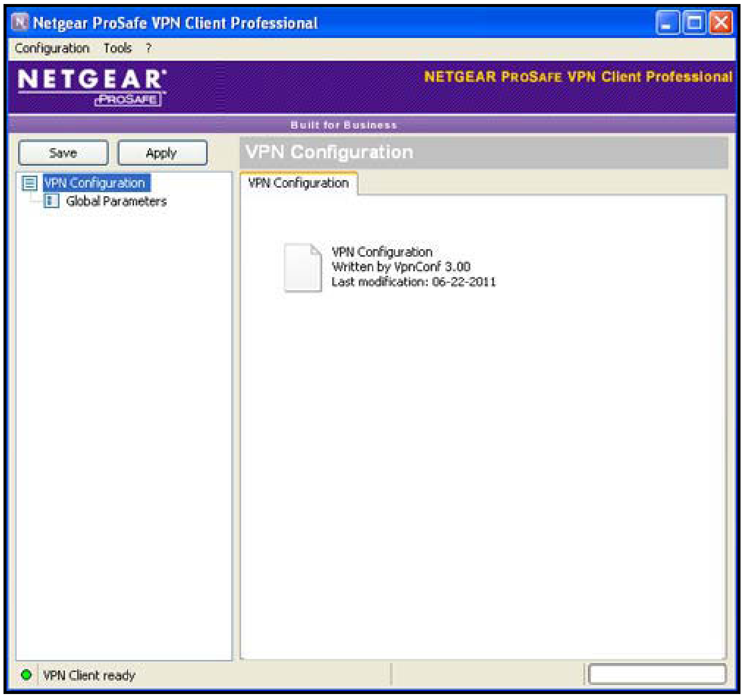
Perform these tasks from a computer on which the NETGEAR ProSafe VPN Client is installed.

To manually configure a VPN connection between the VPN client and the VPN firewall, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and specify the global parameters.

Configure the Authentication Settings (Phase 1 Settings)

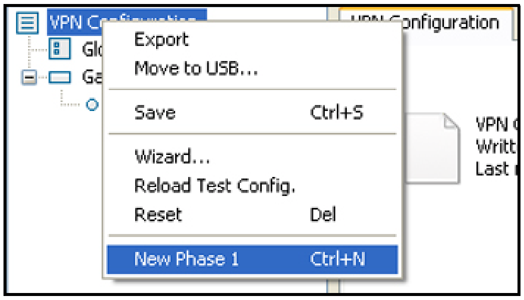
➢ **To create new authentication settings:**

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



VPN Configuration
Written by VpnConf 3.00
Last modification: 06-22-2011

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



3. Change the name of the authentication phase (the default is Gateway):

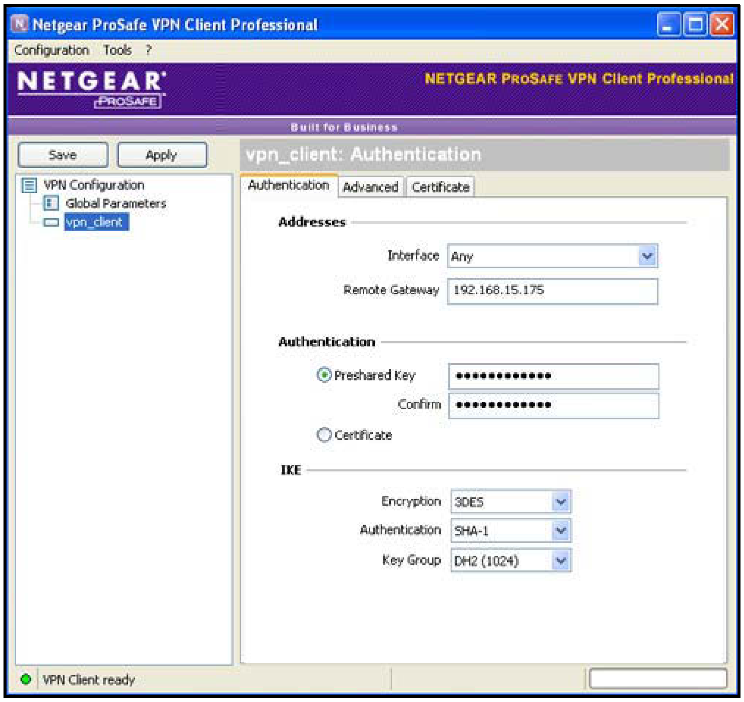
   a. Right-click the authentication phase name.

   b. Select **Rename**.

   c. Type **vpn_client**.

   d. Click anywhere in the tree list pane.

   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 must be a unique name.



Addresses

Interface: Any

Remote Gateway: 192.168.15.175

Authentication

● Preshared Key: ••••••••••••

Confirm: ••••••••••••

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA-1

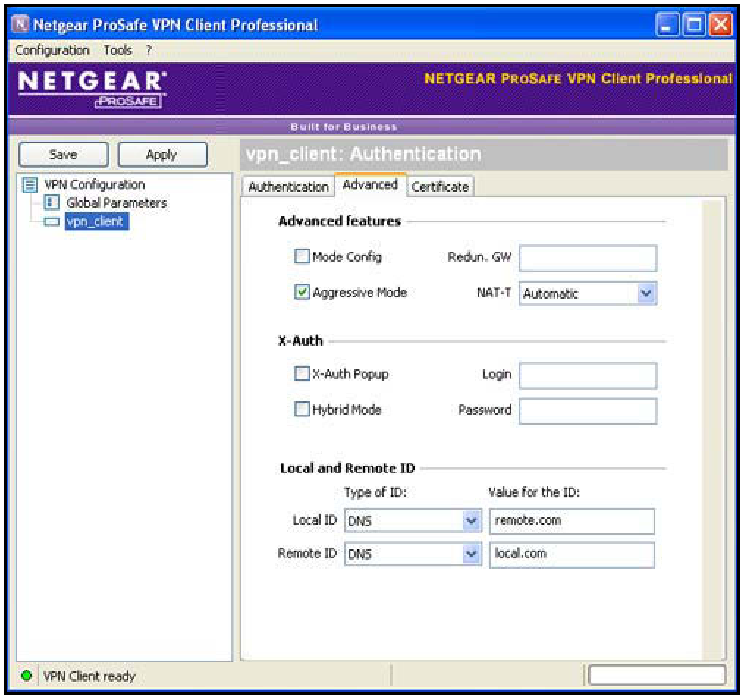
Key Group: DH2 (1024)

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

Table 46. VPN client authentication settings

Setting	Description	
Interface	Select **Any** from the list.	
Remote Gateway	Enter the remote IP address or DNS name of the VPN firewall. For example, enter **192.168.15.175**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **I7!KL39dFG_8**. Confirm the key in the **Confirm** field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the list.
	Authentication	Select the **SHA1** authentication algorithm from the list.
	Key Group	Select the **DH2 (1024)** key group from the list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. To use the new settings immediately, click the **Apply** button.
6. To keep the settings for future use, click the **Save** button.
7. Click the **Advanced** tab in the Authentication pane.



Advanced features

☐ Mode Config	Redun. GW

☑ Aggressive Mode	NAT-T Automatic

X-Auth

☐ X-Auth Popup	Login

☐ Hybrid Mode	Password

Local and Remote ID

	Type of ID:	Value for the ID:
Local ID	DNS	remote.com
Remote ID	DNS	local.com

VPN Client ready

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

Table 47. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the VPN firewall.
NAT-T	Select **Automatic** from the list to enable the VPN client and VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **remote.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter **client.com** as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter **router.com** as the remote ID on the VPN client.

9. To use the new settings immediately, click the **Apply** button.
10. To keep the settings for future use, click the **Save** button.

Create the IPSec Configuration (Phase 2 Settings)

On the VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

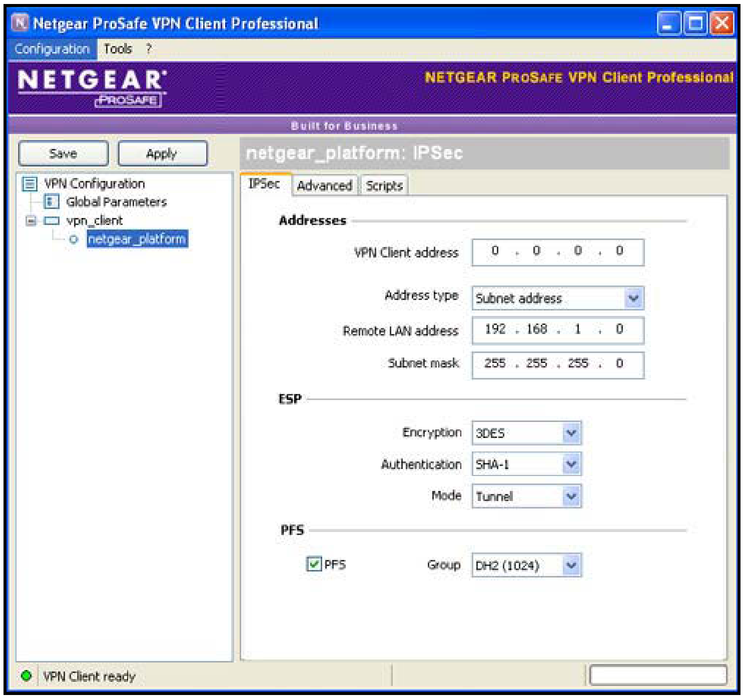
➤ **To create an IPSec configuration:**

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

   The Configuration Panel screen displays.

2. In the tree list pane of the Configuration Panel screen, right-click the **vpn_client** authentication phase name, and select **New Phase 2**.
3. 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.

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 must be a unique name.



netgear_platform: IPSec

Addresses

VPN Client address 0 . 0 . 0 . 0

Address type Subnet address

Remote LAN address 192 . 168 . 1 . 0

Subnet mask 255 . 255 . 255 . 0

ESP

Encryption 3DES

Authentication SHA-1

Mode Tunnel

PFS

☑ PFS Group DH2 (1024)

VPN Client ready

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

Table 48. VPN client IPSec configuration settings

Setting	Description	
VPN Client address	Either enter **0.0.0.0** as the IP address, or enter a virtual IP address that the VPN client uses in the VPN firewall’s LAN; the computer (for which the VPN client opened a tunnel) appears in the LAN with this IP address.	
Address Type	Select **Subnet address** from the 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 list.
	Authentication	Select **SHA-1** as the authentication algorithm. from the list
	Mode	Select **Tunnel** as the encapsulation mode from the list.
PFS and Group	Select the **PFS** check box, and select the **DH2 (1024)** key group. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

5. To use the new settings immediately, click the **Apply** button.
6. To keep the settings for future use, click the **Save** button.

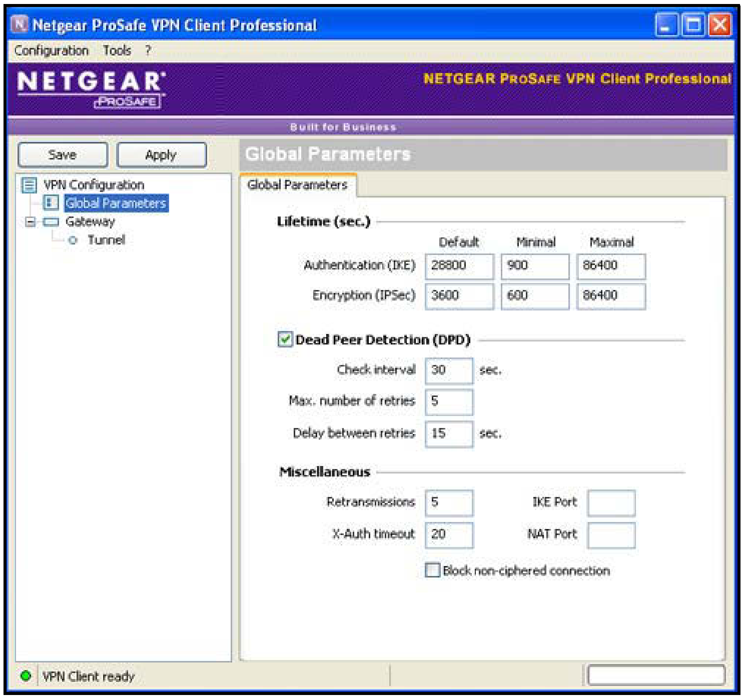
Configure the Global Parameters

➢ **To specify the global parameters:**

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

   The Configuration Panel screen displays.

2. Click **Global Parameters** in the left column of the Configuration Panel screen.



Lifetime (sec.)

	Default	Minimal	Maximal
Authentication (IKE)	28800	900	86400
Encryption (IPSec)	3600	600	86400

☑ Dead Peer Detection (DPD)

Check interval 30 sec.
Max. number of retries 5
Delay between retries 15 sec.

Miscellaneous

Retransmissions 5
IKE Port
X-Auth timeout 20
NAT Port
□ Block non-ciphered connection

VPN Client ready

3. Specify the default lifetimes in seconds:
   - **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the VPN firewall.
   - **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the VPN firewall.
4. To use the new settings immediately, click the **Apply** button.
5. To keep the settings for future use, click the **Save** button.

   The VPN firewall configuration is now complete.

Test the Connection and View Connection and Status Information

Both the NETGEAR ProSafe VPN Client and the VPN firewall provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a connection.

This section contains the following topics:

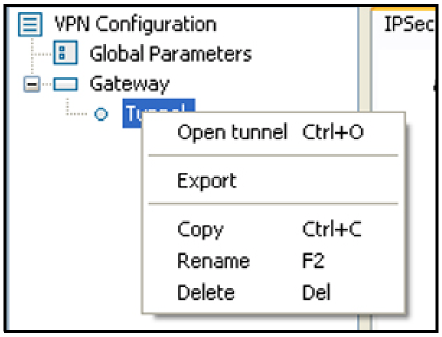
- *Test the NETGEAR VPN Client Connection*
- *NETGEAR VPN Client Status and Log Information*
- *View the VPN Firewall IPSec VPN Connection Status*
- *View the VPN Firewall IPSec VPN Log*

Test the NETGEAR VPN Client Connection

You can establish a connection in many ways. 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 configured) as the authentication phase name and *netgear_platform* (or any other name that you configured) as the IPSec configuration name.

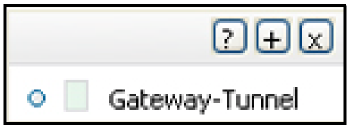
➤ **To establish a connection, use one of the following three methods:**

- **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**.

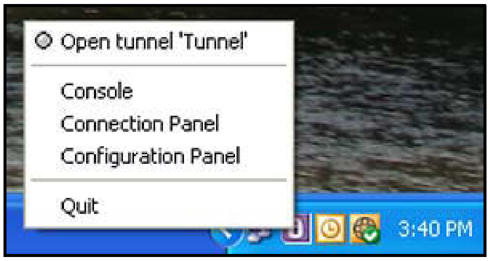


- **Use the Connection Panel screen**. On the main menu of the Configuration Panel screen, select **Tools > Connection Panel** to open the Connection Panel screen. Perform *one* of the following tasks:
  - Double-click **Gateway-Tunnel**.
  - Right-click **Gateway-Tunnel**, and select **Open tunnel**.

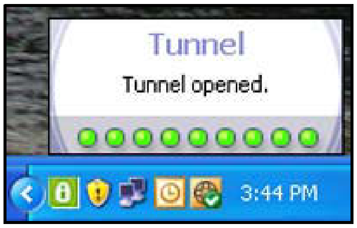
  - Click **Gateway-Tunnel**, and press Ctrl+O.



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



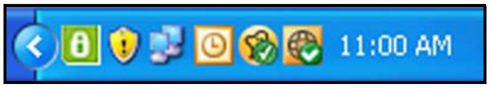
Whichever way you choose to open the tunnel, when the tunnel opens successfully, the *Tunnel opened* message displays above the system tray:


Tunnel

Tunnel opened.

Figure 19. Tunnel opened message

After the VPN client is launched, it displays an icon in the system tray that indicates whether a tunnel is opened, using a color code:



🟩 **Green icon:**
at least one VPN tunnel opened

🟪 **Purple icon:**
no VPN tunnel opened

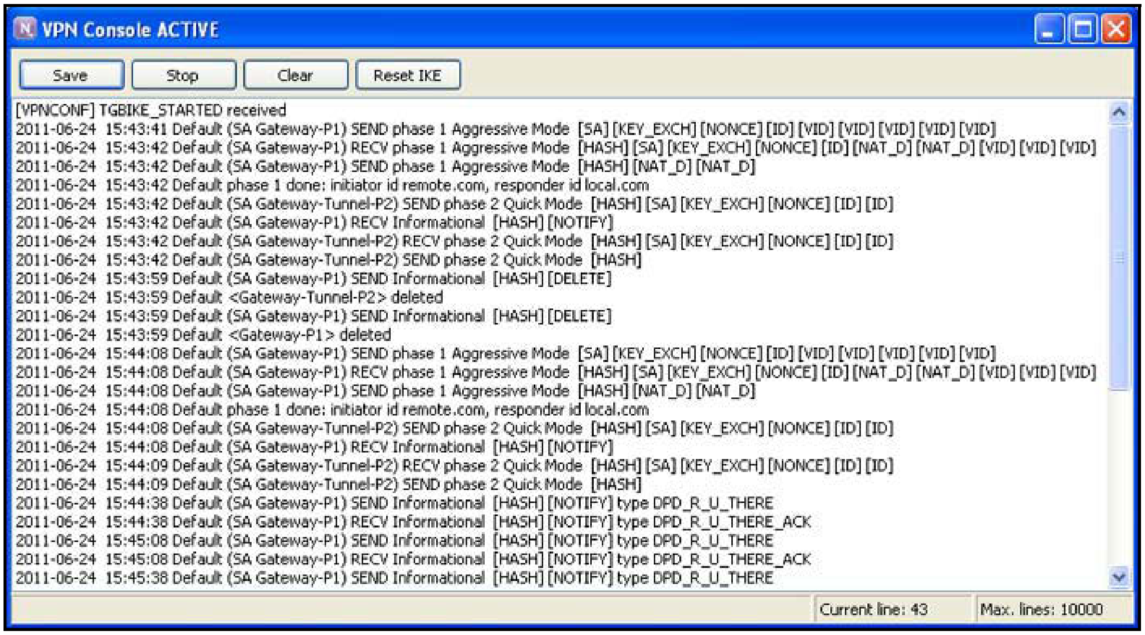
Figure 20. VPN client icon in system tray

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.



```
[VPNCONF] TGBIKE_STARTED received
2011-06-24  15:43:41 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode  [SA] [KEY_EXCH] [NONCE] [ID] [VID] [VID] [VID] [VID] [VID]
2011-06-24  15:43:42 Default (SA Gateway-P1) RECV phase 1 Aggressive Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [NAT_D] [NAT_D] [VID] [VID] [VID]
2011-06-24  15:43:42 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode  [HASH] [NAT_D] [NAT_D]
2011-06-24  15:43:42 Default phase 1 done: initiator id remote.com, responder id local.com
2011-06-24  15:43:42 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24  15:43:42 Default (SA Gateway-P1) RECV Informational  [HASH] [NOTIFY]
2011-06-24  15:43:42 Default (SA Gateway-Tunnel-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24  15:43:42 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode  [HASH]
2011-06-24  15:43:59 Default (SA Gateway-P1) SEND Informational  [HASH] [DELETE]
2011-06-24  15:43:59 Default <Gateway-Tunnel-P2> deleted
2011-06-24  15:43:59 Default (SA Gateway-P1) SEND Informational  [HASH] [DELETE]
2011-06-24  15:43:59 Default <Gateway-P1> deleted
2011-06-24  15:44:08 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode  [SA] [KEY_EXCH] [NONCE] [ID] [VID] [VID] [VID] [VID] [VID]
2011-06-24  15:44:08 Default (SA Gateway-P1) RECV phase 1 Aggressive Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [NAT_D] [NAT_D] [VID] [VID] [VID]
2011-06-24  15:44:08 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode  [HASH] [NAT_D] [NAT_D]
2011-06-24  15:44:08 Default phase 1 done: initiator id remote.com, responder id local.com
2011-06-24  15:44:08 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24  15:44:08 Default (SA Gateway-P1) RECV Informational  [HASH] [NOTIFY]
2011-06-24  15:44:09 Default (SA Gateway-Tunnel-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24  15:44:09 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode  [HASH]
2011-06-24  15:44:38 Default (SA Gateway-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_U_THERE
2011-06-24  15:44:38 Default (SA Gateway-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
2011-06-24  15:45:08 Default (SA Gateway-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_U_THERE
2011-06-24  15:45:08 Default (SA Gateway-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
2011-06-24  15:45:38 Default (SA Gateway-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_U_THERE
```

Current line: 43   Max. lines: 10000

View the VPN Firewall IPSec VPN Connection Status

➢ **To view the status of current IPSec VPN tunnels:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

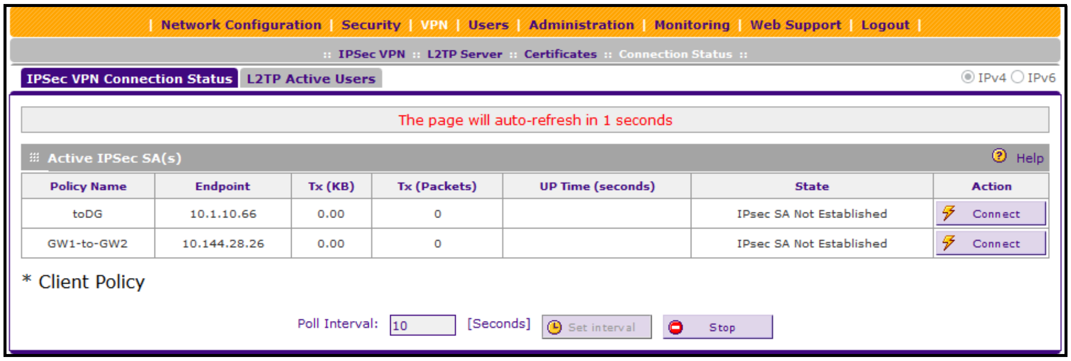
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Connection Status**.



| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
L2TP Active Users
● IPv4 ○ IPv6
Help

The page will auto-refresh in 1 seconds

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	UP Time (seconds)	State	Action
toDG	10.1.10.66	0.00	0		IPsec SA Not Established	Connect
GW1-to-GW2	10.144.28.26	0.00	0		IPsec SA Not Established	Connect

* Client Policy

Poll Interval: 10 [Seconds] Set interval Stop

The Active IPSec SA(s) table lists each active connection with the information that is described in the following table.

Table 49. 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 no connection exists, 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.

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

   The default poll interval is 10 seconds.

4. To stop polling, click the **Stop** button.

View the VPN Firewall IPSec VPN Log

➢ **To display the IPSec VPN log:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

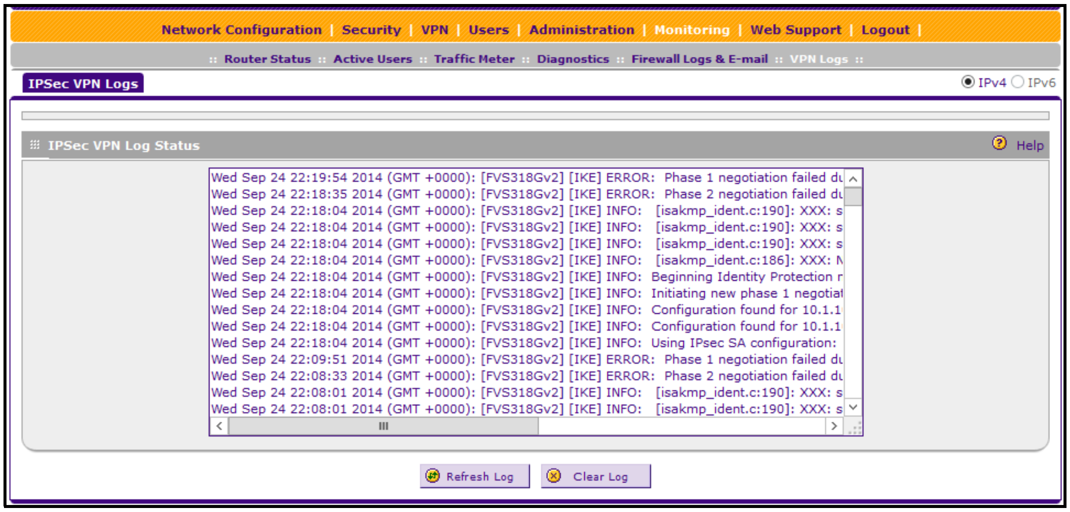
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > VPN Logs > IPSec VPN Logs**.


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
● IPv4 ○ IPv6
IPSec VPN Log Status
Help
Refresh Log
Clear Log

```
Wed Sep 24 22:19:54 2014 (GMT +0000): [FVS318Gv2] [IKE] ERROR:  Phase 1 negotiation failed du
Wed Sep 24 22:18:35 2014 (GMT +0000): [FVS318Gv2] [IKE] ERROR:  Phase 2 negotiation failed du
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:186]: XXX: N
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Beginning Identity Protection r
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Initiating new phase 1 negotiat
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Configuration found for 10.1.1
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Configuration found for 10.1.1
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Using IPsec SA configuration:
Wed Sep 24 22:09:51 2014 (GMT +0000): [FVS318Gv2] [IKE] ERROR:  Phase 1 negotiation failed du
Wed Sep 24 22:08:33 2014 (GMT +0000): [FVS318Gv2] [IKE] ERROR:  Phase 2 negotiation failed du
Wed Sep 24 22:08:01 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
Wed Sep 24 22:08:01 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
```

Manage IPSec VPN Policies

After you use 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.

This section contains the following topics:

- *Manage IKE Policies*
- *Manage VPN Policies*

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 the following:

- An automatically generated VPN policy (auto policy) must 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 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, and the following happens:
   - 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

➢ To access the IKE Policies list:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

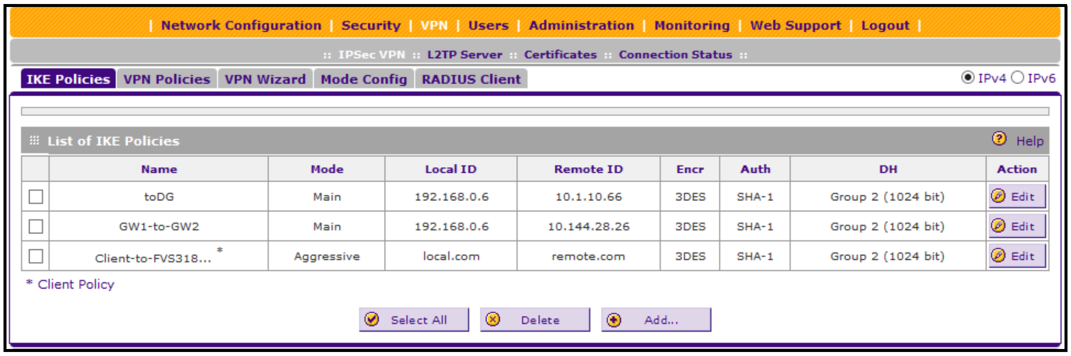
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
List of IKE Policies
Help

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	toDG	Main	192.168.0.6	10.1.10.66	3DES	SHA-1	Group 2 (1024 bit)	Edit
□	GW1-to-GW2	Main	192.168.0.6	10.144.28.26	3DES	SHA-1	Group 2 (1024 bit)	Edit
□	Client-to-FVS318... *	Aggressive	local.com	remote.com	3DES	SHA-1	Group 2 (1024 bit)	Edit

* Client Policy

Each policy contains the data that is described in the following table. These fields are described in more detail in *Table 51* on page 243.

Table 50. IKE Policies screen information for IPv4 and IPv6

Item	Description
Name	The name that identifies the IKE policy. When you use the VPN Wizard to set up a VPN policy, an accompanying IKE policy is automatically created with the same name that you select for the VPN policy. **Note:** The name is not supplied to the remote VPN endpoint.
Mode	The exchange mode: Main or Aggressive.
Local ID	The IKE/ISAKMP identifier of the VPN firewall. The remote endpoint must use this value as its remote ID.
Remote ID	The IKE/ISAKMP identifier of the remote endpoint, which must use the this value as its local ID.
Encr	The encryption algorithm that is used for the IKE security association (SA). This setting must match the setting on the remote endpoint.
Auth	The authentication algorithm that is used for the IKE SA. This setting must use match setting on the remote endpoint.
DH	The Diffie-Hellman (DH) group that is used when keys are exchanged. This setting must match the setting on the remote endpoint.

You cannot delete or edit an IKE policy for which the VPN policy is active without first disabling or deleting the VPN policy.

➢ To delete one or more IKE polices:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN**.

   The IKE Policies screen displays.

3. 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.

4. Click the **Delete** table button.

Manually Add or Edit an IKE Policy

➢ **To manually add an IKE policy for IPv4 or IPv6:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN**.

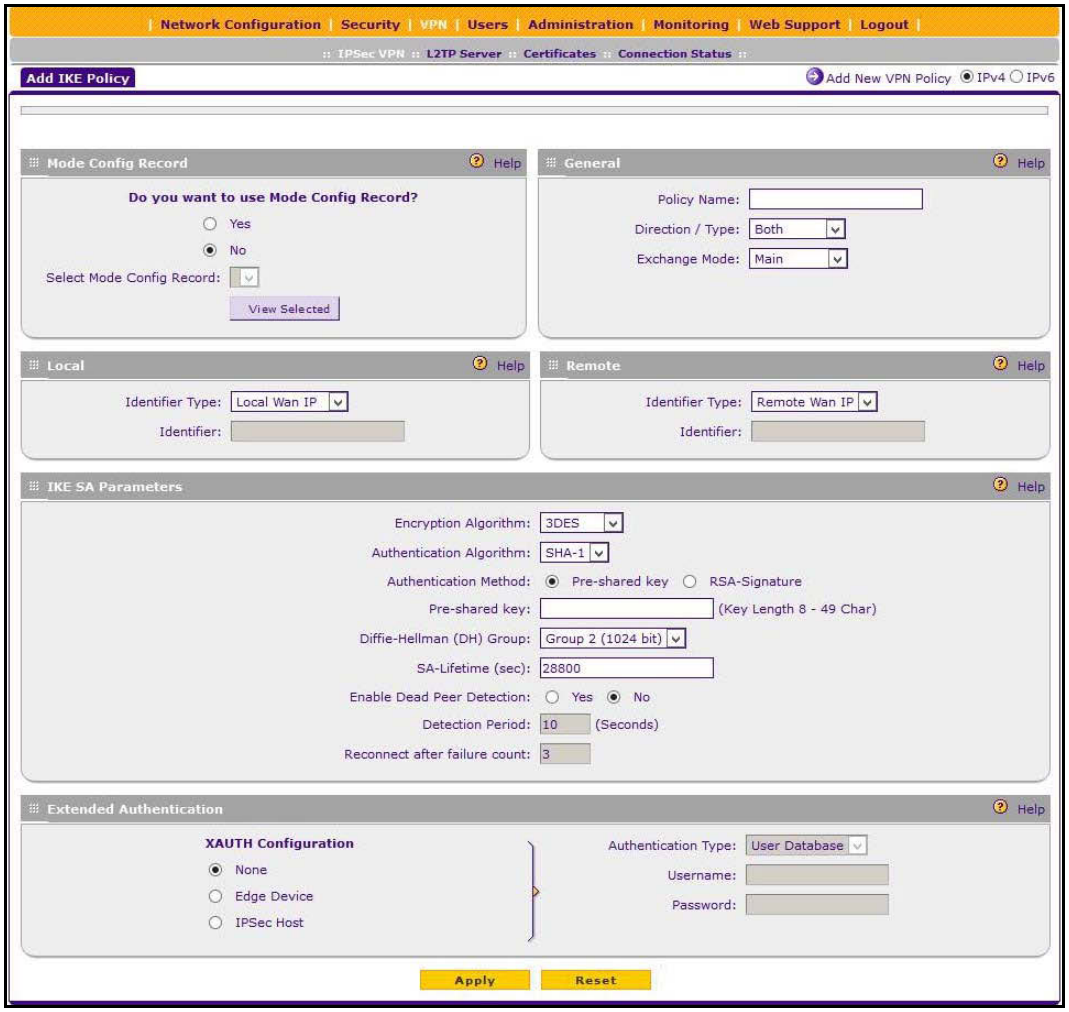
   The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.

3. Under the List of IKE Policies table, click the **Add** table button.

   The Add IKE Policy screen displays the IPv4 settings.

4. 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 5*.
- **IPv6**. Select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
Add IKE Policy
Add New VPN Policy
Help
View Selected
Apply
Reset

● IPv4 ○ IPv6

Mode Config Record

Do you want to use Mode Config Record?

○ Yes
● No

Select Mode Config Record:

General

Policy Name:
Direction / Type: Both
Exchange Mode: Main

Local

Identifier Type: Local Wan IP
Identifier:

Remote

Identifier Type: Remote Wan IP
Identifier:

IKE SA Parameters

Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: ● Pre-shared key ○ RSA-Signature
Pre-shared key: (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800
Enable Dead Peer Detection: ○ Yes ● No
Detection Period: 10 (Seconds)
Reconnect after failure count: 3

Extended Authentication

XAUTH Configuration

● None
○ Edge Device
○ IPSec Host

Authentication Type: User Database
Username:
Password:

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

Table 51. 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 261. Select one of the following radio buttons: • **Yes**. IP addresses are assigned to remote VPN clients. You must select a Mode Config record from the 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 list, select one of the Mode Config records that you defined on the Add Mode Config Record screen (see *Configure Mode Config Operation on the VPN Firewall* on page 262). **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 list, select the connection method for the VPN firewall: • **Initiator**. The VPN firewall initiates the connection to the remote endpoint. • **Responder**. The VPN firewall responds only to an IKE request from the remote endpoint. • **Both**. The VPN firewall can both initiate a connection to the remote endpoint and respond to an IKE request from the remote endpoint.	
Exchange Mode	From the list, select the mode of exchange between the VPN firewall and the remote VPN endpoint: • **Main**. This mode is slower than the Aggressive mode but more secure. • **Aggressive**. This mode is faster than the Main mode but less secure.	

Table 51. Add IKE Policy screen settings (continued)

Setting	Description	
Local		
Identifier Type	From the list, select one of the following ISAKMP identifiers to be used by the VPN firewall, and specify the identifier in the **Identifier** field: • **Local Wan IP**. The WAN IP address of the VPN firewall. When you select this option, the **Identifier** field automatically shows the IP address of the selected WAN interface. • **FQDN**. The Internet address for the VPN firewall. • **User FQDN**. The email address for a local VPN client or the VPN firewall. • **DER ASN1 DN**. A distinguished name (DN) that identifies the VPN firewall in the DER encoding and ASN.1 format.	
	Identifier	Depending on the selection of the **Identifier Type** list, enter the IP address, email address, FQDN, or distinguished name.
Remote		
Identifier Type	From the 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 Type** list, enter the IP address, email address, FQDN, or distinguished name.
IKE SA Parameters		
Encryption Algorithm	From the list, select an algorithm 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 list, select an algorithm 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 51. Add IKE Policy screen settings (continued)

Setting	Description	
Authentication Method	Select the authentication method: • **Pre-shared key**. A secret that is shared between the VPN firewall and the remote endpoint. • **RSA-Signature**. Uses the active self-signed certificate that you uploaded on the Certificates screen (see *Manage VPN Self-Signed Certificates* on page 311). The pre-shared key is masked out when you select the **RSA-Signature** button.	
	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 list, select the strength: • **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 276.	Select whether Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You must specify the detection period in the **Detection Period** field and the maximum number of times that the VPN firewall attempts to reconnect in the **Reconnect after failure count** field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default is 3 failures.

Table 51. Add IKE Policy screen settings (continued)

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td colspan="3"><b>Extended Authentication</b></td></tr>
<tr><td rowspan="4">XAUTH Configuration
<b>Note:</b> For more information about XAUTH and its authentication modes, see <i>Configure XAUTH for VPN Clients</i> on page 257.</td><td colspan="2">Select whether Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information:
• <b>None</b>. XAUTH is disabled. This the default setting.
• <b>Edge Device</b>. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, or RADIUS CHAP.
• <b>IPSec Host</b>. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination.</td></tr>
<tr><td>Authentication Type</td><td>For an Edge Device configuration, from the list, select the authentication type:
• <b>User Database</b>. XAUTH occurs through the VPN firewall’s user database. You can add users on the Add User screen (see <i>User Database Configuration</i> on page 259).
• <b>Radius PAP</b>. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the VPN firewall connects to a RADIUS server. For more information, see <i>RADIUS Client and Server Configuration</i> on page 259.
• <b>Radius CHAP</b>. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see <i>RADIUS Client and Server Configuration</i> on page 259.</td></tr>
<tr><td>Username</td><td>The user name for XAUTH.</td></tr>
<tr><td>Password</td><td>The password for XAUTH.</td></tr>
</table>

6. Click the **Apply** button.

   Your changes are saved.

➤ To edit an IKE policy:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN**.

   The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.

3. 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 4*.
   - **IPv6**. Select the **IPv6** radio button. The IKE Policies screen for IPv6 displays.

4. In the List of IKE Policies table, to the right of the IKE policy that you want to edit, click the **Edit** table button.

   The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen.

5. Modify the settings that you wish to change.

   See *Table 51* on page 243.

6. Click the **Apply** button.

   Your changes are saved.

Manage VPN Policies

You can create two types of VPN policies:

- **Manual**. You manually enter all settings (including the keys) for the VPN tunnel on the VPN firewall and on the remote VPN endpoint. No third-party server or organization is involved.
- **Auto**. Some settings for the VPN tunnel are generated automatically through the use of the IKE (Internet Key Exchange) Protocol to perform negotiations between the two VPN endpoints (the local ID endpoint and the remote ID endpoint). You still must manually enter all settings on the remote VPN endpoint (unless the remote VPN endpoint also includes a VPN Wizard).

When you use the VPN Wizard to create a VPN policy, only the Auto method is available.

In addition, a certification authority (CA) can also be used to perform authentication. For more information, see *Manage Digital Certificates for VPN Connections* on page 308.

For gateways to use a CA to perform authentication, you need a certificate from the CA for each VPN gateway. 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

You can add additional policies—either Auto or Manual—and manage the VPN policies that were 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 use 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 must use a matching SA; otherwise, it refuses the connection.

➢ To view the VPN policies:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

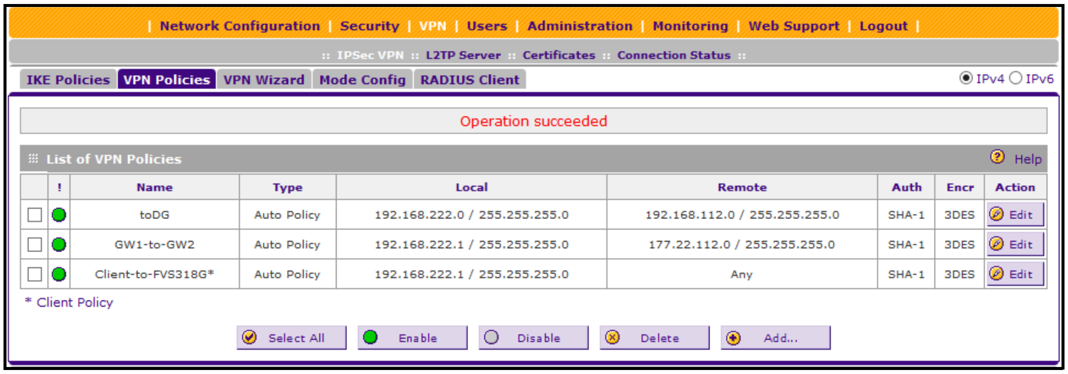
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Policies**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6

Operation succeeded

List of VPN Policies

? Help

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	toDG	Auto Policy	192.168.222.0 / 255.255.255.0	192.168.112.0 / 255.255.255.0	SHA-1	3DES	Edit
□	●	GW1-to-GW2	Auto Policy	192.168.222.1 / 255.255.255.0	177.22.112.0 / 255.255.255.0	SHA-1	3DES	Edit
□	●	Client-to-FVS318G*	Auto Policy	192.168.222.1 / 255.255.255.0	Any	SHA-1	3DES	Edit

* Client Policy

Select All
Enable
Disable
Delete
Add...

In the upper right of the screen, the **IPv4** radio button is selected by default. The VPN Policies screen displays the IPv4 settings.

3. To display the IPv6 settings on the IKE Policies screen, select the **IPv6** radio button.

Each policy contains the data that are described in the following table. These fields are described in more detail in *Table 53* on page 252.

Table 52. 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 must 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 must be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask.)
Auth	The authentication algorithm that is used for the VPN tunnel. This setting must match the setting on the remote endpoint.
Encr	The encryption algorithm that is used for the VPN tunnel. This setting must match the setting on the remote endpoint.

➢ To delete one or more VPN polices:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays.

3. 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.
4. Click the **Delete** table button.

- **To enable or disable one or more VPN policies:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays.
3. 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.
4. Click the **Enable** or **Disable** table button.

Manually Add or Edit a VPN Policy

- **To manually add a VPN policy:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

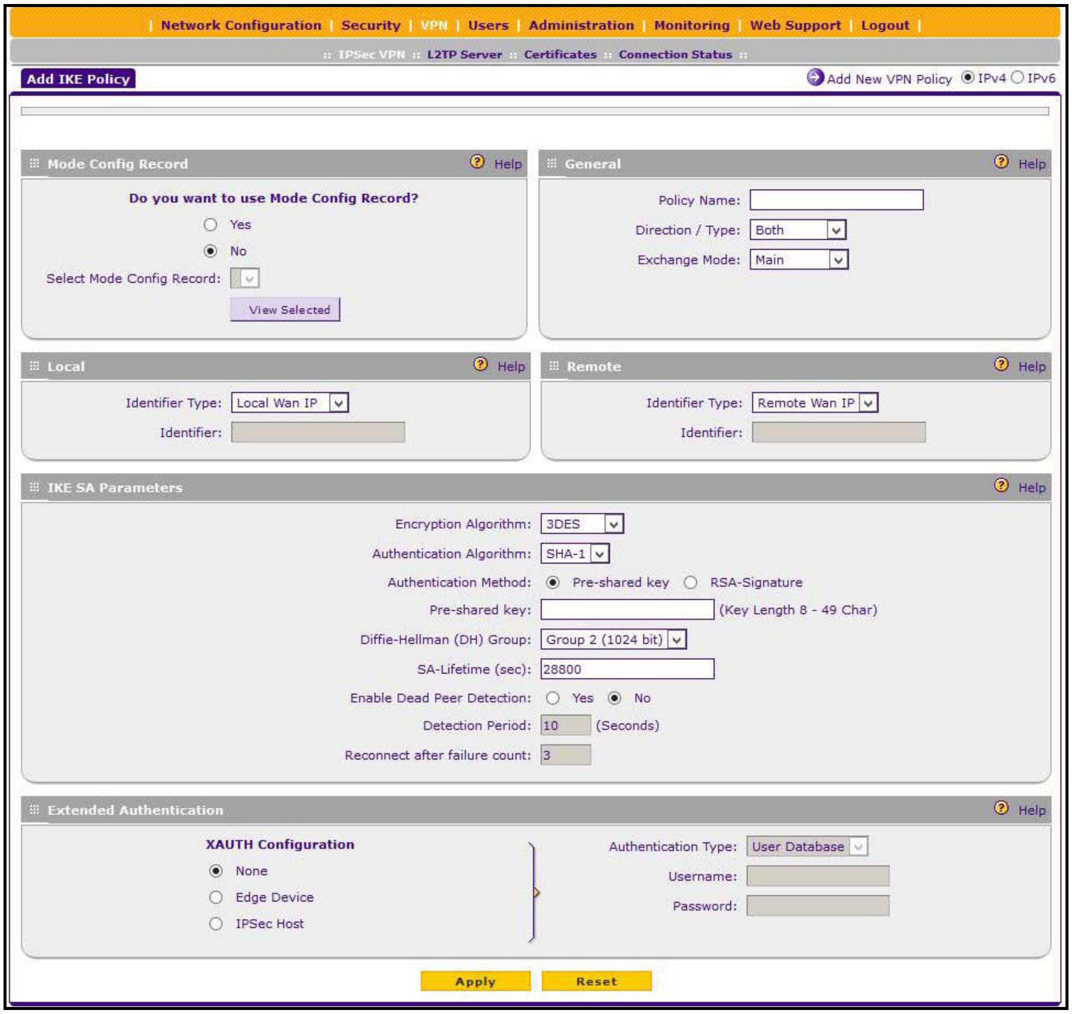
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays the IPV4 settings.
3. Under the List of VPN Policies table, click the **Add** table button.

   The Add New VPN Policy screen displays the IPv4 settings.
4. 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 5*.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
Add IKE Policy
Add New VPN Policy
Help
Apply
Reset
View Selected

● IPv4 ○ IPv6

Mode Config Record

Do you want to use Mode Config Record?

○ Yes

● No

Select Mode Config Record:

General

Policy Name:

Direction / Type: Both

Exchange Mode: Main

Local

Identifier Type: Local Wan IP

Identifier:

Remote

Identifier Type: Remote Wan IP

Identifier:

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group: Group 2 (1024 bit)

SA-Lifetime (sec): 28800

Enable Dead Peer Detection: ○ Yes ● No

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

Extended Authentication

XAUTH Configuration

● None

○ Edge Device

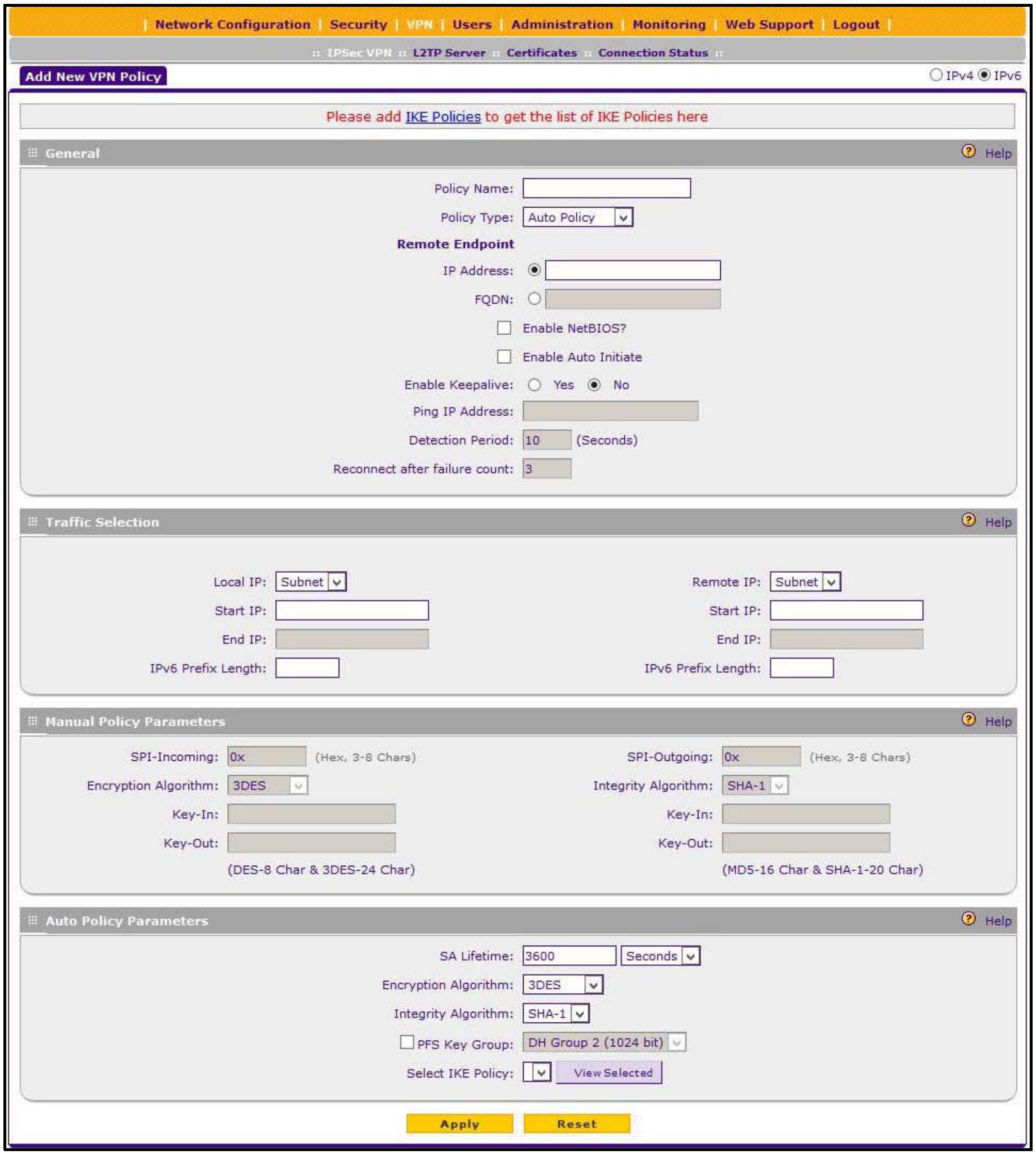
○ IPSec Host

Authentication Type: User Database

Username:

Password:

- **IPv6**. Select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
Add New VPN Policy
Help
Apply
Reset
View Selected

○ IPv4 ● IPv6

Please add IKE Policies to get the list of IKE Policies here

General

Policy Name:
Policy Type: Auto Policy
Remote Endpoint
IP Address: ●
FQDN: ○
□ Enable NetBIOS?
□ Enable Auto Initiate
Enable Keepalive: ○ Yes ● No
Ping IP Address:
Detection Period: 10 (Seconds)
Reconnect after failure count: 3

Traffic Selection

Local IP:	Subnet	Remote IP:	Subnet
Start IP:		Start IP:	
End IP:		End IP:	
IPv6 Prefix Length:		IPv6 Prefix Length:	

Manual Policy Parameters

SPI-Incoming:	0x (Hex, 3-8 Chars)	SPI-Outgoing:	0x (Hex, 3-8 Chars)
Encryption Algorithm:	3DES	Integrity Algorithm:	SHA-1
Key-In:		Key-In:	
Key-Out:		Key-Out:	
	(DES-8 Char & 3DES-24 Char)		(MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime: 3600 Seconds
Encryption Algorithm: 3DES
Integrity Algorithm: SHA-1
□ PFS Key Group: DH Group 2 (1024 bit)
Select IKE Policy:

5. 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 53. Add New VPN Policy screen settings for IPv4 and IPv6

Setting	Description
General	
Policy Name	A descriptive name of the VPN policy for identification and management purposes. **Note:** The name is not supplied to the remote VPN endpoint.

Table 53. Add New VPN Policy screen settings for IPv4 and IPv6 (continued)

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td>Policy Type</td><td colspan="2">From the list, select the policy type:
• <b>Auto Policy</b>. Some settings (the ones in the Manual Policy Parameters section) for the VPN tunnel are generated automatically.
• <b>Manual Policy</b>. All settings must be specified manually, including the ones in the Manual Policy Parameters section.</td></tr>
<tr><td>Remote Endpoint</td><td colspan="2">Select how the remote endpoint is defined:
• <b>IP Address</b>. Enter the IP address of the remote endpoint in the fields to the right of the radio button.
• <b>FQDN</b>. Enter the FQDN of the remote endpoint in the field to the right of the radio button.</td></tr>
<tr><td>Enable NetBIOS?</td><td colspan="2">Select this check box to enable NetBIOS broadcasts to travel over the VPN tunnel. For more information about NetBIOS, see <i>Configure NetBIOS Bridging with IPSec VPN</i> on page 280. This feature is disabled by default.</td></tr>
<tr><td>Enable Auto Initiate</td><td colspan="2">Select this check box to enable the VPN tunnel to autoestablish itself without the presence of any traffic.
<b>Note:</b> The direction and type of the IKE policy that is associated with this VPN policy must be either Initiator or Both but cannot be Responder. For more information, see <i>Manually Add or Edit an IKE Policy</i> on page 241.</td></tr>
<tr><td rowspan="4">Enable Keepalive
<b>Note:</b> See also <i>Configure Keep-Alives and Dead Peer Detection</i> on page 276.</td><td colspan="2">Select whether keep-alive is enabled:
• <b>Yes</b>. This feature is enabled: Periodically, the VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You must specify the ping IP address in the <b>Ping IP Address</b> field, the detection period in the <b>Detection Period</b> field, and the maximum number of keep-alive requests that the VPN firewall sends in the <b>Reconnect after failure count</b> field.
• <b>No</b>. This feature is disabled. This is the default setting.</td></tr>
<tr><td>Ping IP Address</td><td>The IP address that the VPN firewall pings. The address must be of a host that can respond to ICMP ping requests.</td></tr>
<tr><td>Detection Period</td><td>The period in seconds between the keep-alive requests. The default setting is 10 seconds.</td></tr>
<tr><td>Reconnect after failure count</td><td>The maximum number of keep-alive requests before the VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is 3 keep-alive requests.</td></tr>
</table>

Table 53. Add New VPN Policy screen settings for IPv4 and IPv6 (continued)

Setting	Description
Traffic Selection	
Local IP	From the list, select the address or addresses that are part of the VPN tunnel on the VPN firewall: • **Any**. All computers and devices on the network. You cannot select **Any** for both the VPN firewall and the remote endpoint. • **Single**. A single IP address on the network. Enter the IP address in the **Start IP Address** field. • **Range**. A range of IP addresses on the network. Enter the starting IP address in the **Start IP Address** field and the ending IP address in the **End IP Address** field. • **Subnet**. A subnet on the network. Enter the starting IP address in the **Start IP Address field**. In addition, enter the following: - **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 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** 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 parameter index (SPI) for the inbound policy. Enter a hexadecimal value between three and eight characters (for example, 0x1234).
Encryption Algorithm	From the list, select the algorithm 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 53. 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 parameter index (SPI) for the outbound policy. Enter a hexadecimal value between three and eight characters (for example, 0x1234).
Integrity Algorithm	From the list, select the algorithm 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 must be renegotiated. From the 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 list, select the algorithm 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 53. Add New VPN Policy screen settings for IPv4 and IPv6 (continued)

Setting	Description
Integrity Algorithm	From the list, select the algorithm 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 list. The DH group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the list, select the strength: • **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.

6. Click the **Apply** button.

   Your changes are saved.

➢ **To edit a VPN policy:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays the IPv4 settings.

3. 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 4*.
   - **IPv6**. Select the **IPv6** radio button. The VPN Policies screen for IPv6 displays.

4. In the List of VPN Policies table, to the right of the VPN policy that you want to edit, click the **Edit** table button.

The Edit VPN Policy screen displays. This screen shows the same fields as the Add New VPN Policy screen.

5. Modify the settings that you wish to change (see *Table 53* on page 252).
6. Click the **Apply** button.

   Your changes are saved.

Configure Extended Authentication (XAUTH)

When many VPN clients connect to a VPN firewall, you might want to use a unique user authentication method beyond relying on a single common pre-shared key for all clients. Although you could configure a unique VPN policy for each user, it is more efficient to authenticate users from a stored list of user accounts. XAUTH provides the mechanism for requesting individual authentication information from the user. A local user database or an external authentication server, such as a RADIUS server, provides a method for storing the authentication information centrally in the local network.

You can enable XAUTH when you manually add or edit an IKE policy. Two types of XAUTH are available:

- **Edge Device**. The VPN firewall is used as a VPN concentrator on which one or more gateway tunnels terminate. You must specify the authentication type to be used during verification of the credentials of the remote VPN gateways: the user database, RADIUS-PAP, or RADIUS-CHAP.
- **IPSec Host**. Authentication by the remote gateway through a user name and password that are associated with the IKE policy. The user name and password that are used to authenticate the VPN firewall must be specified on the remote gateway.

If a RADIUS-PAP server is enabled for authentication, XAUTH first checks the local user database for the user credentials. If the user account is not present, the VPN firewall then connects to a RADIUS server.

This section contains the following topics:

- *Configure XAUTH for VPN Clients*
- *User Database Configuration*
- *RADIUS Client and Server Configuration*

Configure XAUTH for VPN Clients

Once the XAUTH is enabled, you must establish user accounts in the user database to be authenticated against XAUTH, or you must enable a RADIUS-CHAP or RADIUS-PAP server.

You cannot modify an existing IKE policy to add XAUTH while the IKE policy is in use by a VPN policy. The VPN policy must be disabled before you can modify the IKE policy.

➤ **To enable and configure XAUTH:**

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN**.

   The IPSec VPN submenu tabs display with the IKE Policies for IPv4 screen in view.

3. Specify the IP version for which you want to edit an IKE policy:
   - **IPv4**. In the upper right, the **IPv4** radio button is already selected by default. Go to *Step 4*.
   - **IPv6**. Select the **IPv6** radio button. The IKE Policies screen for IPv6 displays.

4. In the List of IKE Policies table, to the right of the IKE policy for which you want to enable and configure XAUTH, click the **Edit** table button.

   The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen.

5. In the Extended Authentication section, complete the settings as described in the following table.

Table 54. Extended authentication settings for IPv4 and IPv6

Setting	Description
Select whether Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination.	
Authentication Type	For an Edge Device configuration, from the list, select the authentication type: • **User Database**. XAUTH occurs through the VPN firewall’s user database. You can add users on the Add User screen (see *User Database Configuration* on page 259). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client and Server Configuration* on page 259. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client and Server Configuration* on page 259.

Table 54. Extended authentication settings for IPv4 and IPv6 (continued)

Setting	Description
Username	The user name for XAUTH.
Password	The password for XAUTH.

6. Click the **Apply** button.

   Your changes are saved.

User Database Configuration

When XAUTH is enabled in an Edge Device configuration, users must be authenticated either by a local user database account or by an external RADIUS server. Whether or not you use a RADIUS server, you might want some users to be authenticated locally. These users must be added to the List of Users table on the Users screen, as described in *Configure User Accounts* on page 295.

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 must 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.

You can select the RADIUS authentication protocol (PAP or CHAP) on the Edit IKE Policy screen or Add IKE Policy screen. For more information, see *Configure XAUTH for VPN Clients* on page 257.

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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

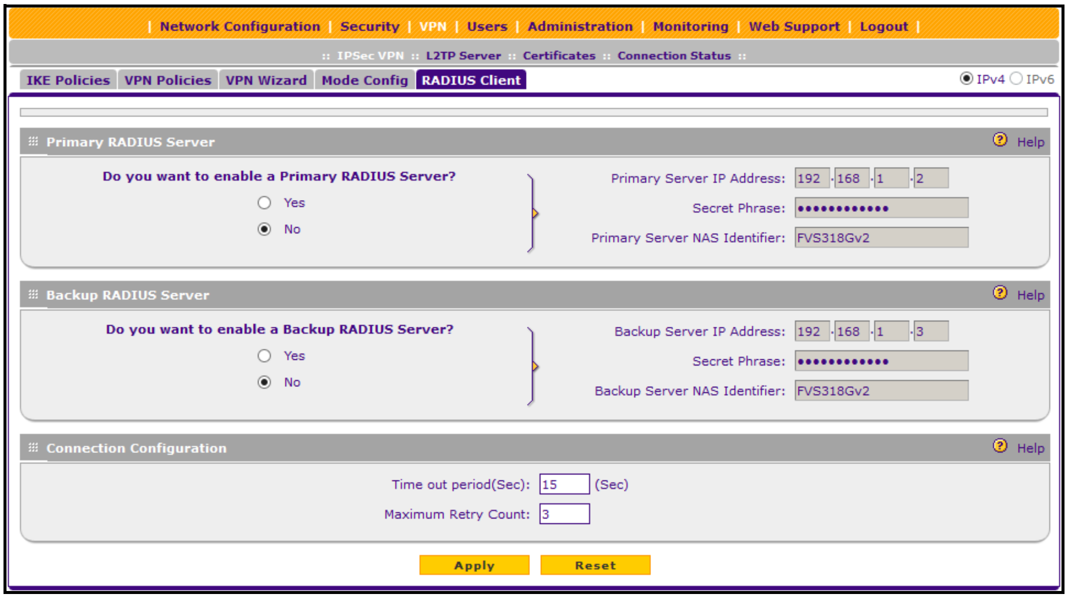
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > RADIUS Client**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
Help
Apply
Reset

● IPv4 ○ IPv6

Primary RADIUS Server

Do you want to enable a Primary RADIUS Server?

○ Yes

● No

Primary Server IP Address: 192 . 168 . 1 . 2

Secret Phrase: ●●●●●●●●●●●●

Primary Server NAS Identifier: FVS318Gv2

Backup RADIUS Server

Do you want to enable a Backup RADIUS Server?

○ Yes

● No

Backup Server IP Address: 192 . 168 . 1 . 3

Secret Phrase: ●●●●●●●●●●●●

Backup Server NAS Identifier: FVS318Gv2

Connection Configuration

Time out period(Sec): 15 (Sec)

Maximum Retry Count: 3

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

Table 55. RADIUS Client screen settings

Setting	Description
Primary RADIUS Server	
To enable and configure the primary RADIUS server, select the **Yes** radio button, and enter the settings for the three fields to the right. The default setting is that the **No** radio button is selected.	
Primary Server IP Address	The IPv4 address of the primary RADIUS server.
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the primary RADIUS server. The same secret phrase must be configured on both the client and the server.
Primary Server NAS Identifier	The primary Network Access Server (NAS) identifier that must be present in a RADIUS request. **Note:** The VPN firewall functions as an NAS, allowing network access to external users after verification of their authentication information. In a RADIUS transaction, the NAS must provide some NAS identifier information to the RADIUS server. Depending on the configuration of the RADIUS server, the VPN firewall's IP address might be sufficient as an identifier, or the server might require a name, which you must enter in this field.
Backup RADIUS Server	

Table 55. RADIUS Client screen settings (continued)

Setting	Description
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 must be configured on both the client and the server.
Backup Server NAS Identifier	The backup Network Access Server (NAS) identifier that must be present in a RADIUS request. **Note:** See the note earlier in this table for Primary Server NAS Identifier.
Connection Configuration	
Time out period	The period in seconds that the VPN firewall waits for a response from a RADIUS server. The default setting is 30 seconds.
Maximum Retry Counts	The maximum number of times that the VPN firewall attempts to connect to a RADIUS server. The default setting is 4 retry counts.

4. Click the **Apply** button.

   Your changes are saved.

Assign IPv4 Addresses to Remote Users

To simplify the process of connecting remote VPN clients to the VPN firewall, use the Mode Config feature to automatically assign IPv4 addresses to remote users, including a network access IP address, subnet mask, WINS server, and DNS address. Remote users are given IP addresses available in a secured network space so that remote users appear as seamless extensions of the network.

You can use the Mode Config feature in combination with an IPv6 IKE policy to assign IPv4 addresses to clients, but you cannot assign IPv6 addresses to clients.

This section contains the following topics:

- *Mode Config Operation*
- *Configure Mode Config Operation on the VPN Firewall*
- *Configure the ProSafe VPN Client for Mode Config Operation*
- *Test the Mode Config Connection*
- *Modify or Delete a Mode Config Record*

Mode Config Operation

After the IKE Phase 1 negotiation is complete, the VPN connection initiator (which is the remote user with a VPN client) requests the IP configuration settings such as the IP address, subnet mask, WINS server, and DNS address from the VPN firewall. The Mode Config feature allocates an IP address from the configured IP address pool and activates a temporary IPSec policy, using the information that is specified in the Traffic Tunnel Security Level section of the Mode Config record.

After configuring a Mode Config record, you must manually configure an IKE policy and select the newly created Mode Config record from the **Select Mode Config Record** list. For more information, see *Configure Mode Config Operation on the VPN Firewall* on page 262. You do not need to change any VPN policy.

An IP address that is allocated to a VPN client is released only after the VPN client gracefully disconnects or after the SA liftetime for the connection times out.

Configure Mode Config Operation on the VPN Firewall

To configure Mode Config on the VPN firewall, first create a Mode Config record, and then select the Mode Config record for an IKE policy.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

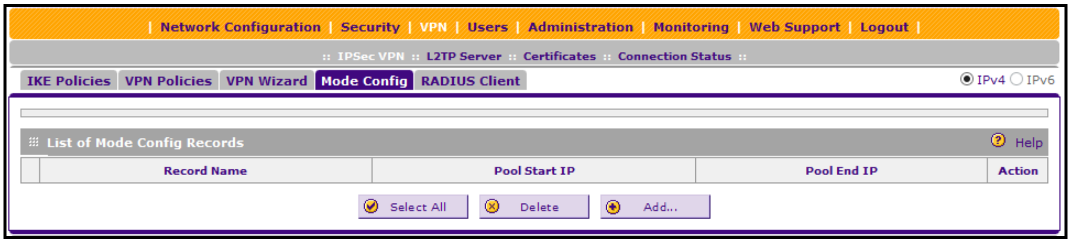
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

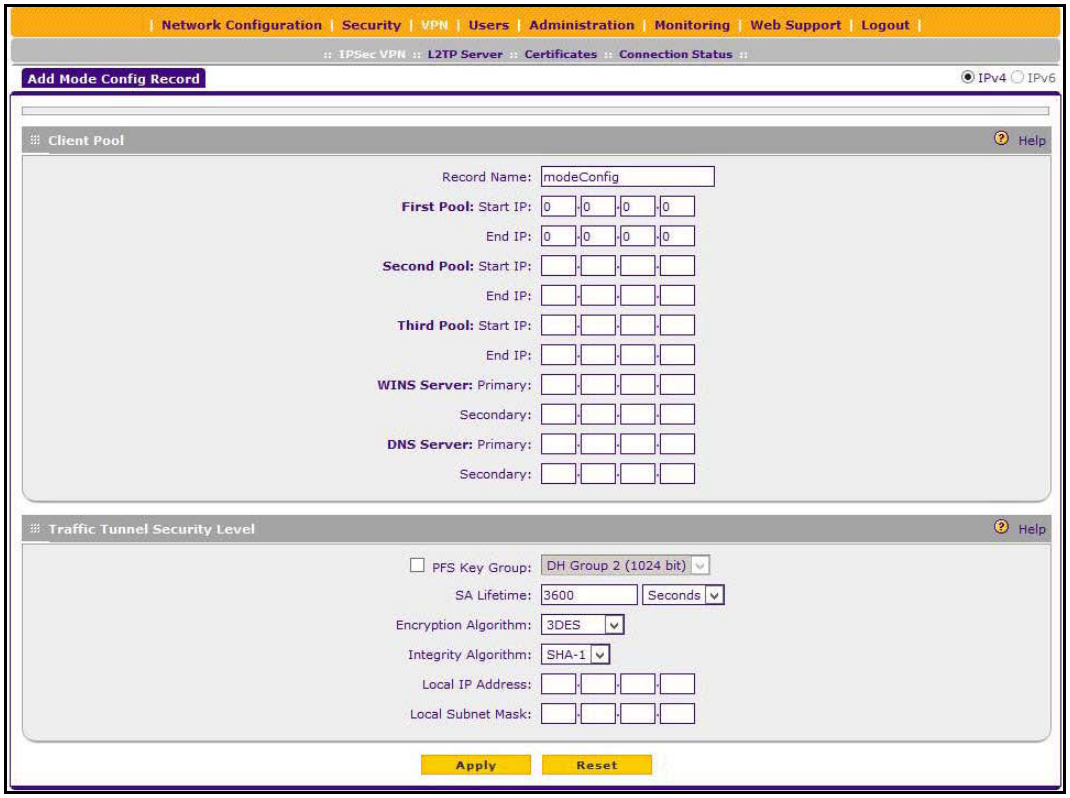
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > Mode Config**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
List of Mode Config Records
Help
Record Name
Pool Start IP
Pool End IP
Action
Select All
Delete
Add...

3. Under the List of Mode Config Records table, click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
Add Mode Config Record
● IPv4 ○ IPv6
Client Pool
Help
Traffic Tunnel Security Level
Help
Apply
Reset

Record Name: modeConfig

First Pool: Start IP: 0.0.0.0

End IP: 0.0.0.0

Second Pool: Start IP:

End IP:

Third Pool: Start IP:

End IP:

WINS Server: Primary:

Secondary:

DNS Server: Primary:

Secondary:

□ PFS Key Group: DH Group 2 (1024 bit)

SA Lifetime: 3600 Seconds

Encryption Algorithm: 3DES

Integrity Algorithm: SHA-1

Local IP Address:

Local Subnet Mask:

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

Table 56. Add Mode Config Record screen settings

Setting	Description
Client Pool	
Record Name	A descriptive name of the Mode Config record for identification and management purposes.
First Pool	Assign at least one range of IP pool addresses in the First Pool fields to enable the VPN firewall to allocate these to remote VPN clients. The **Second Pool** and **Third Pool** fields are optional. To specify any client pool, enter the **starting IP** address for the pool in the **Starting IP** field, and enter the ending IP address for the pool in the **Ending IP** field. **Note:** Make sure that no IP pool is within the range of the local network IP addresses. Use a different range of private IP addresses such as 172.16.xxx.xx.
Second Pool	
Third Pool	
WINS Server	If the local network includes a WINS serve, 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.

Table 56. Add Mode Config Record screen settings (continued)

Setting	Description
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 list. The DH group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the list, select the strength: • **Group 1 (768 bit)** • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and must be renegotiated. From the 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 list, select the algorithm 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 list, select the algorithm 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 that remote VPN clients can access. If you do not specify a local IP address, the VPN firewall's default LAN IP address is used (by default, 192.168.1.1).
Local Subnet Mask	The local subnet mask. Typically, this is 255.255.255.0. **Note:** If you do not specify a local IP address, you do not need to specify a subnet either.

5. Click the **Apply** button.

   Your changes are saved.

   Continue the Mode Config configuration procedure by configuring an IKE policy.

6. Select **VPN > IPSec VPN**.

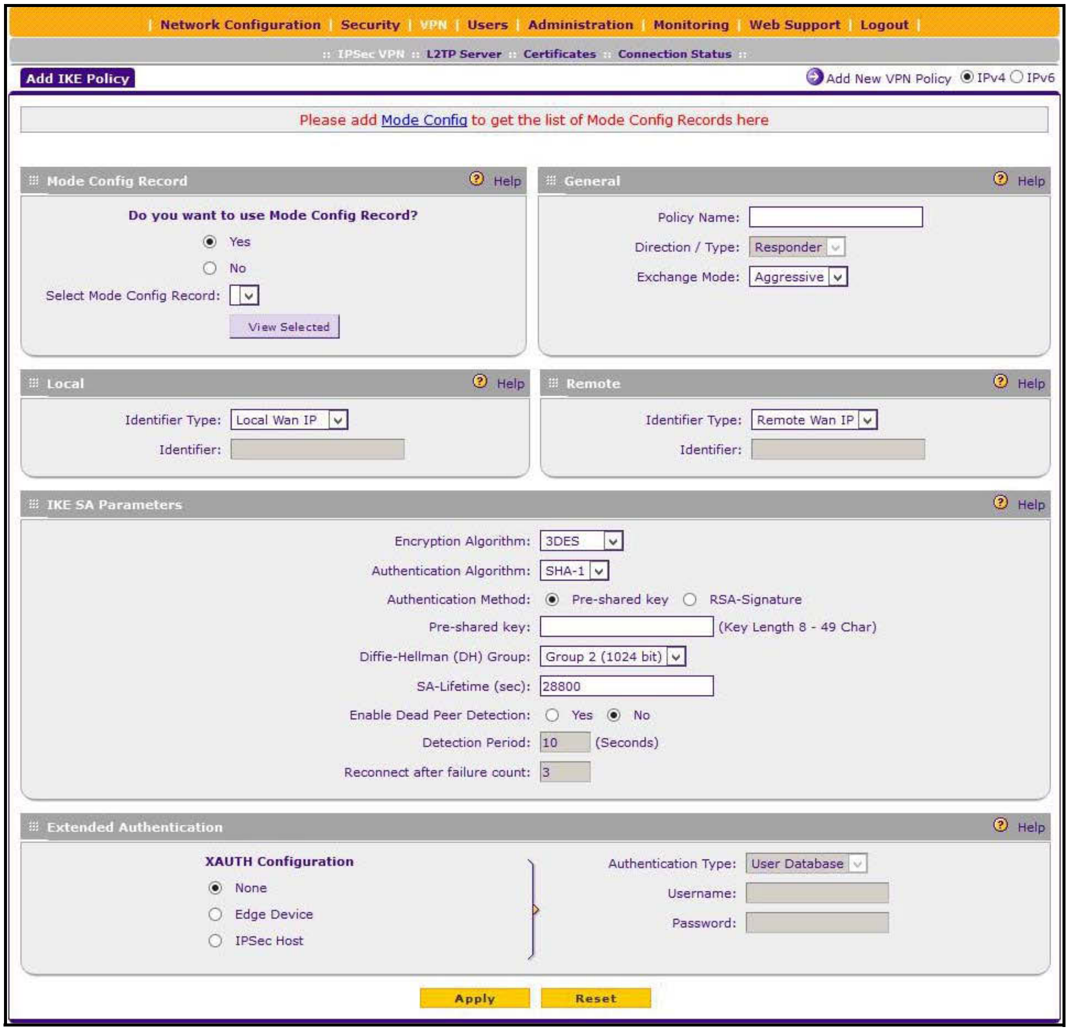
   The IPSec VPN submenu tabs display with the IKE Policies screen in view.

Under the List of IKE Policies table, click the **Add** table button.

7. The Add IKE Policy screen displays the IPv4 settings.
8. 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 9*.
   - **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).

     You can configure an IPv6 IKE policy to assign IPv4 addresses to clients, but you cannot assign IPv6 addresses to clients.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
Add IKE Policy
Add New VPN Policy
Help
View Selected
Apply
Reset

● IPv4 ○ IPv6

Please add Mode Config to get the list of Mode Config Records here

Mode Config Record

Do you want to use Mode Config Record?

● Yes

○ No

Select Mode Config Record:

General

Policy Name:

Direction / Type: Responder

Exchange Mode: Aggressive

Local

Identifier Type: Local Wan IP

Identifier:

Remote

Identifier Type: Remote Wan IP

Identifier:

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group: Group 2 (1024 bit)

SA-Lifetime (sec): 28800

Enable Dead Peer Detection: ○ Yes ● No

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

Extended Authentication

XAUTH Configuration

● None

○ Edge Device

○ IPSec Host

Authentication Type: User Database

Username:

Password:

9. On the Add IKE Policy screen, complete the settings as described in the following table.

The IKE policy settings that are described in the following table are specifically for a Mode Config configuration. *Table 51* on page 243 explains the general IKE policy settings.

Table 57. 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 list, select the Mode Config record that you created in *Step 5* on page *264*.
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. This ensures that the VPN firewall responds to an IKE request from the remote endpoint but does not initiate one.	
Exchange Mode	Aggressive mode is automatically selected when you select the Mode Config record in the Mode Config Record section.	
Local		
Identifier Type	From the list, select **FQDN**. **Note:** Mode Config requires that the VPN firewall (that is, the local endpoint) is defined by an FQDN.	
	Identifier	Enter an FQDN for the VPN firewall.
Remote		
Identifier Type	From the 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 must be an FQDN that is not used in any other IKE policy.
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 list, select the **3DES** algorithm.	
Authentication Algorithm	From the list, select the **SHA-1** algorithm to be used in the VPN header for the authentication process.	

Table 57. Add IKE Policy screen settings for a Mode Config configuration (continued)

Setting	Description	
Authentication Method	Select **Pre-shared key** as the authentication method, and enter a key in the **Pre-shared key** field.	
	Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote ("), single quote ('), or space in the key.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. From the 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 276.	Select whether Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You must specify the detection period in the **Detection Period** field and the maximum number of times that the VPN firewall attempts to reconnect in the **Reconnect after failure count** field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds. This example uses 30 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default setting is 3 failures.

Table 57. 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 257.	Select whether Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination.	
	Authentication Type	For an Edge Device configuration, from the list, select the authentication type: • **User Database**. XAUTH occurs through the VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 259). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client and Server Configuration* on page 259. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client and Server Configuration* on page 259.
	Username	The user name for XAUTH.
	Password	The password for XAUTH.

10. Click the **Apply** button.

    Your changes are saved.

Configure the ProSafe VPN Client for Mode Config Operation

When the Mode Config feature is enabled, the following information is negotiated between the VPN client and the VPN firewall during the authentication phase:

- Virtual IP address of the VPN client
- DNS server address (optional)
- WINS server address (optional)

The virtual IP address that is issued by the VPN firewall is displayed in the **VPN Client Address** field on the VPN client's IPSec pane.

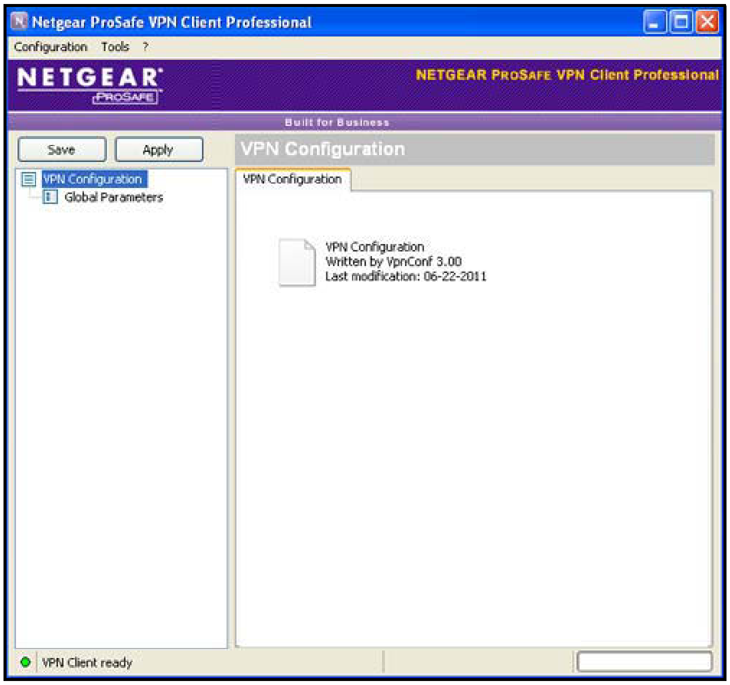
Perform these tasks from a computer on which the NETGEAR ProSafe VPN Client is installed.

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)

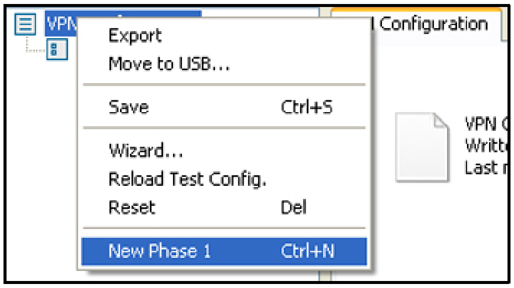
➤ **To create new authentication settings:**

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



VPN Configuration
Written by VpnConf 3.00
Last modification: 06-22-2011

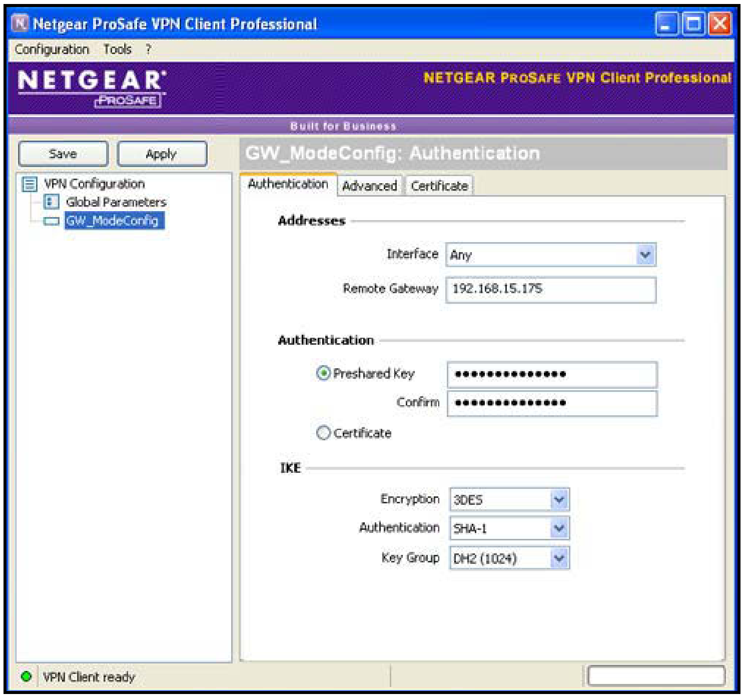
2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.



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.

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 must be a unique name.



GW_ModeConfig: Authentication

Addresses

Interface: Any

Remote Gateway: 192.168.15.175

Authentication

● Preshared Key: ••••••••••••••

Confirm: ••••••••••••••

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA-1

Key Group: DH2 (1024)

VPN Client ready

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

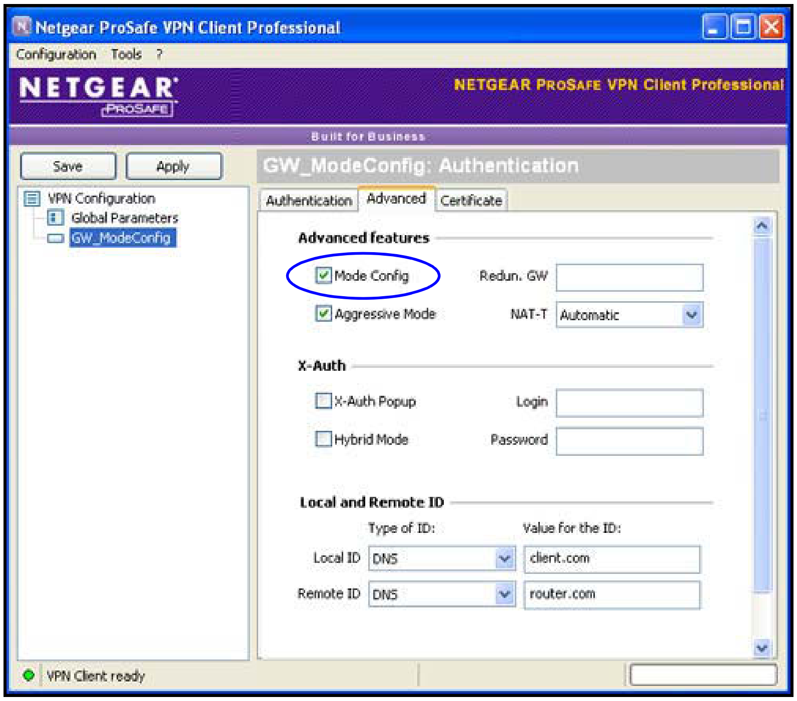
Table 58. VPN client authentication settings (Mode Config)

Setting	Description	
Interface	Select **Any** from the list.	
Remote Gateway	Enter the remote IP address or DNS name of the VPN firewall. For example, enter **192.168.15.175**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **H8!spsf3#JYK2!**. Confirm the key in the **Confirm** field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the list.
	Authentication	Select the **SHA1** authentication algorithm from the list.
	Key Group	Select the **DH2 (1024)** key group from the list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. To use the new settings immediately, click the **Apply** button.

6. To keep the settings for future use, click the **Save** button.

7. Click the **Advanced** tab in the Authentication pane.



GW_ModeConfig: Authentication

Advanced features

☑ Mode Config Redun. GW

☑ Aggressive Mode NAT-T Automatic

X-Auth

□ X-Auth Popup Login

□ Hybrid Mode Password

Local and Remote ID

	Type of ID:	Value for the ID:
Local ID	DNS	client.com
Remote ID	DNS	router.com

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

Table 59. VPN client advanced authentication settings (Mode Config)

Setting	Description
Advanced features	
Mode Config	Select this check box to enable Mode Config.
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the VPN firewall.
NAT-T	Select **Automatic** from the list to enable the VPN client and VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the **Local ID** list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **client.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the **Remote ID** list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **router.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client.

9. To use the new settings immediately, click the **Apply** button.

10. To keep the settings for future use, click the **Save** button.

Create the Mode Config IPSec Configuration (Phase 2 Settings)

On the VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➢ **To create an IPSec configuration:**

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

   The Configuration Panel screen displays.

2. In the tree list pane of the Configuration Panel screen, right-click the **GW_ModeConfig** authentication phase name, and select **New Phase 2**.

3. Change the name of the IPSec configuration (the default is Tunnel):

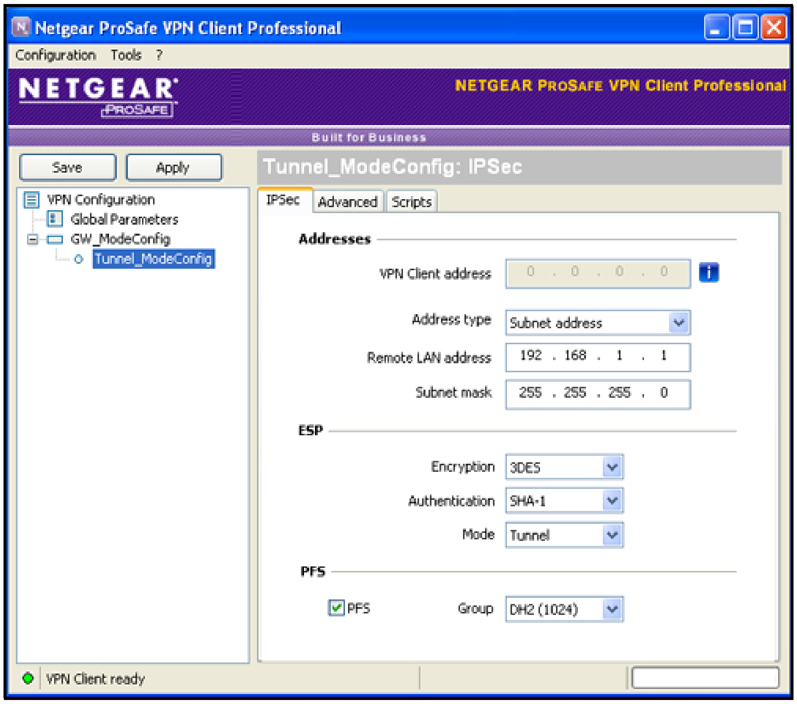
   a. Right-click the IPSec configuration name.

   b. Select **Rename**.

   c. Type **Tunnel_ModeConfig**.

   d. Click anywhere in the tree list pane.

   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 must be a unique name.



Tunnel_ModeConfig: IPSec

Addresses

VPN Client address 0 . 0 . 0 . 0

Address type Subnet address

Remote LAN address 192 . 168 . 1 . 1

Subnet mask 255 . 255 . 255 . 0

ESP

Encryption 3DES

Authentication SHA-1

Mode Tunnel

PFS

☑ PFS Group DH2 (1024)

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

Table 60. VPN client IPSec configuration settings (Mode Config)

Setting	Description	
VPN Client address	This field is masked out because Mode Config is selected. After an IPSec connection is established, the IP address that is issued by the VPN firewall displays in this field.	
Address Type	Select **Subnet address** from the list.	
Remote host address	The address that you must enter depends on whether you specified a LAN IP network address in the **Local IP Address** field on the Add Mode Config Record screen of the VPN firewall: • If you left the **Local IP Address** field blank, enter the VPN firewall's default LAN IP address as the remote host address that opens the VPN tunnel. For example, enter **192.168.1.1**. • If you specified a LAN IP network address in the **Local IP Address** field, enter the address that you specified as the remote host address that opens the VPN tunnel.	
Subnet mask	Enter **255.255.255.0** as the remote subnet mask of the VPN firewall that opens the VPN tunnel. This is the LAN IP subnet mask that you specified in the **Local Subnet Mask** field on the Add Mode Config Record screen of the VPN firewall. If you left the **Local Subnet Mask** field blank, enter the VPN firewall's default IP subnet mask.	
ESP	Encryption	From the list, select **3DES** as the encryption algorithm.
	Authentication	From the list, select **SHA-1** as the authentication algorithm.
	Mode	From the list, select **Tunnel** as the encapsulation mode.
PFS and Group	Select the **PFS** check box, and select the **DH2 (1024)** key group from the list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

5. To use the new settings immediately, click the **Apply** button.
6. To keep the settings for future use, click the **Save** button.

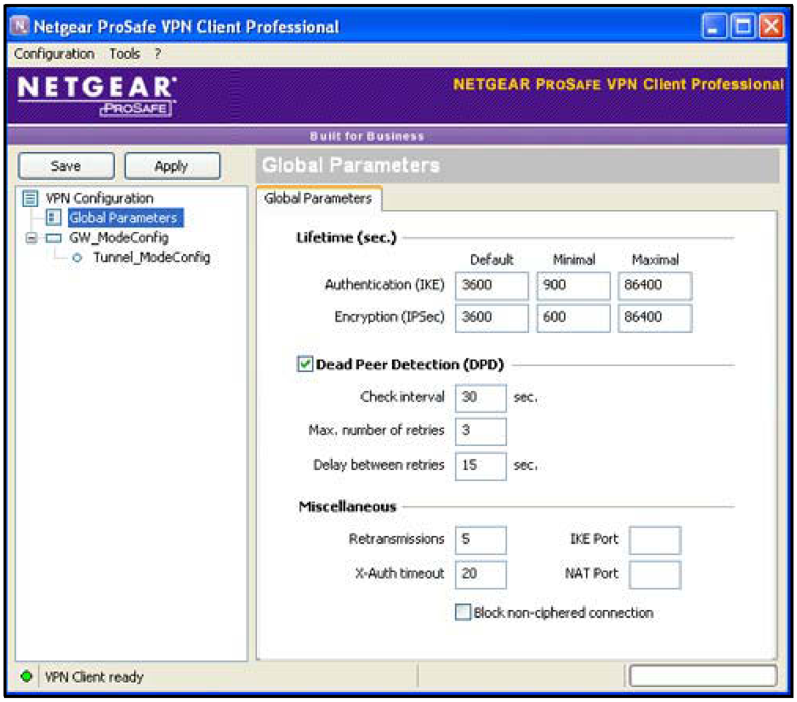
Configure the Mode Config Global Parameters

➤ **To specify the global parameters:**

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

   The Configuration Panel screen displays.

2. In the left column of the Configuration Panel screen, click **Global Parameters**.



Global Parameters

Lifetime (sec.)

	Default	Minimal	Maximal
Authentication (IKE)	3600	900	86400
Encryption (IPSec)	3600	600	86400

☑ Dead Peer Detection (DPD)

Check interval 30 sec.

Max. number of retries 3

Delay between retries 15 sec.

Miscellaneous

Retransmissions 5 IKE Port

X-Auth timeout 20 NAT Port

☐ Block non-ciphered connection

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

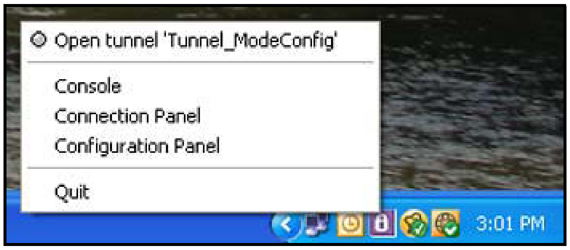
     The default setting is 28800 seconds (eight hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (one hour).
   - **Encryption (IPSec)**, **Default**. Enter **3600** seconds.
4. Select the **Dead Peer Detection (DPD)** check box, and configure the following DPD settings to match the configuration on the VPN firewall:
   - **Check Interval**. Enter **30** seconds.
   - **Max. number of entries**. Enter **3** retries.
   - **Delay between entries**. Leave the default delay setting of 15 seconds.
5. To use the new settings immediately, click the **Apply** button.
6. To keep the settings for future use, click the **Save** button.

The Mode Config configuration of the VPN client is now complete.

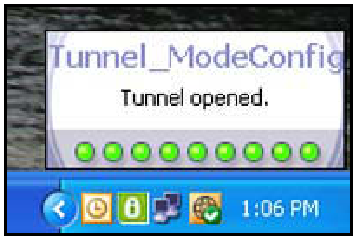
Test the Mode Config Connection

➢ **To test the Mode Config connection from the VPN client to the VPN firewall:**

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



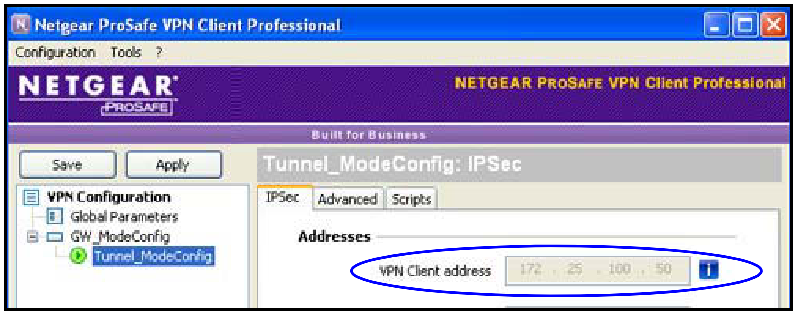
When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray, and the VPN client displays a green icon in the system tray.


Tunnel_ModeConfig

Tunnel opened.

2. Verify that the VPN firewall issued an IP address to the VPN client.

   This IP address displays in the **VPN Client address** field on the IPSec pane of the VPN client.



VPN Client address 172 . 25 . 100 . 50

3. From the client computer, ping a computer on the VPN firewall LAN.

Modify or Delete a Mode Config Record

Note: Before you modify or delete a Mode Config record, make sure that it is not used in an IKE policy.

➢ **To edit a Mode Config record:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > Mode Config**.

   The Mode Config screen displays.

3. In the Action column for the record that you want to modify, click the **Edit** button.

   The Edit Mode Config Record screen displays. This screen is identical to the Add Mode Config Record screen.

4. Modify the settings as described in *Table 56* on page 263.
5. Click the **Apply** button.

   Your changes are saved.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > Mode Config**.

   The Mode Config screen displays.

3. 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.
4. Click the **Delete** table button.

Configure Keep-Alives and Dead Peer Detection

In some cases, you might not want a VPN tunnel to be disconnected when traffic is idle, for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require a VPN tunnel to remain connected, you can use the keep-alive and Dead Peer Detection (DPD) features to prevent the tunnel from being disconnected and to force a reconnection if the tunnel disconnects for any reason.

For DPD to function, the peer VPN device on the other end of the tunnel must also support DPD. Keep-alive, though less reliable than DPD, does not require any support from the peer device.

This section contains the following topics:

- *Configure Keep-Alives*
- *Configure Dead Peer Detection*

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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

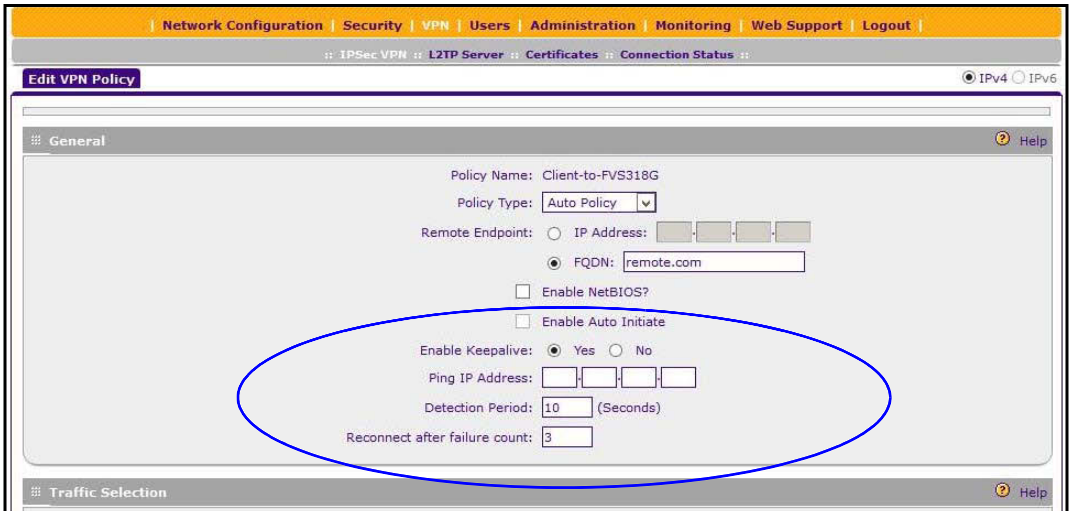
2. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays the IPv4 settings.

3. 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 4*.
   - **IPv6**. Select the **IPv6** radio button.

     The VPN Policies screen for IPv6 displays.

4. In the List of VPN Policies table, to the right of the VPN policy that you want to edit, click the **Edit** table button.



Policy Name: Client-to-FVS318G

Policy Type: Auto Policy

Remote Endpoint: ○ IP Address:

● FQDN: remote.com

□ Enable NetBIOS?

□ Enable Auto Initiate

Enable Keepalive: ● Yes ○ No

Ping IP Address:

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

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

Table 61. Keep-alive settings

Setting	Description	
General		
Enable Keepalive	Select the **Yes** radio button to enable the keep-alive feature. Periodically, the VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You must specify the ping IP address in the **Ping IP Address** field, the detection period in the **Detection Period** field, and the maximum number of keep-alive requests that the VPN firewall sends in the **Reconnect after failure count** field.	
	Ping IP Address	The IP address that the VPN firewall pings. The address must be of a host that can respond to ICMP ping requests.
	Detection Period	The period in seconds between the keep-alive requests. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of keep-alive requests before the VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is 3 keep-alive requests.

6. Click the **Apply** button.

   Your changes are saved.

Configure Dead Peer Detection

The Dead Peer Detection (DPD) feature lets the VPN firewall maintain the IKE SA by exchanging periodic messages with the remote VPN peer.

➤ **To configure DPD on a configured IKE policy:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN**.

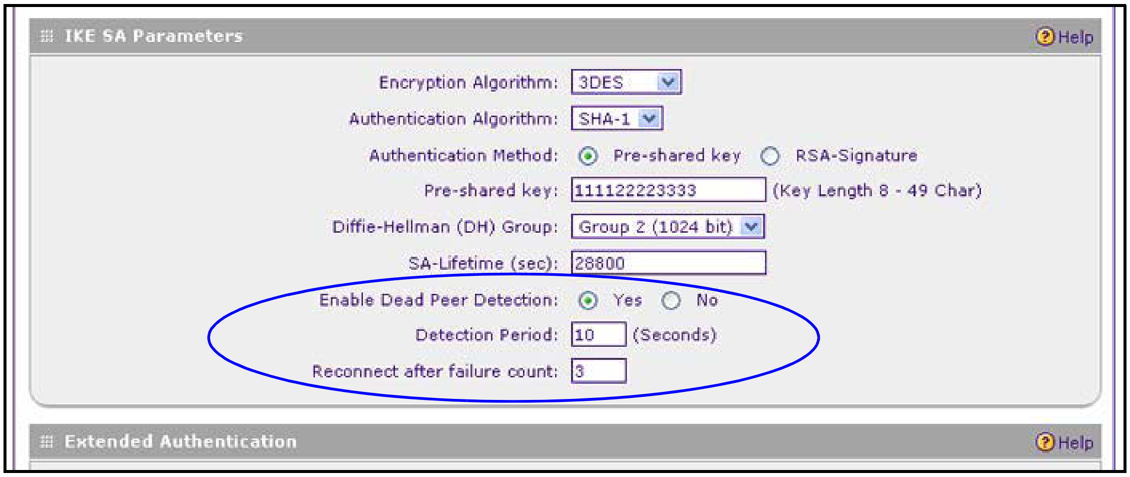
   The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.

3. 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 4*.
   - **IPv6**. Select the **IPv6** radio button.

     The IKE Policies screen for IPv6 displays.

4. In the List of IKE Policies table, to the right of the IKE policy that you want to edit, click the **Edit** table button.



Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: ● Pre-shared key ○ RSA-Signature
Pre-shared key: 111122223333 (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

5. In the IKE SA Parameters section, locate the DPD fields, and complete the settings as described the following table.

Table 62. Dead Peer Detection settings

Setting	Description	
IKE SA Parameters		
Enable Dead Peer Detection	Select the **Yes** radio button to enable DPD. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You must specify the detection period in the **Detection Period** field and the maximum number of times that the VPN firewall attempts to reconnect in the **Reconnect after failure count** field.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default setting is 3 failures.

6. Click the **Apply** button.

   Your changes are saved.

Configure NetBIOS Bridging with IPSec VPN

Windows networks use the Network Basic Input/Output System (NetBIOS) for several basic network services such as naming and neighborhood device discovery. Because VPN routers do not usually pass NetBIOS traffic, these network services do not function for hosts on opposite ends of a VPN connection. To solve this problem, you can configure the VPN firewall to bridge NetBIOS traffic over the VPN tunnel.

➤ **To enable NetBIOS bridging on a configured VPN tunnel:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

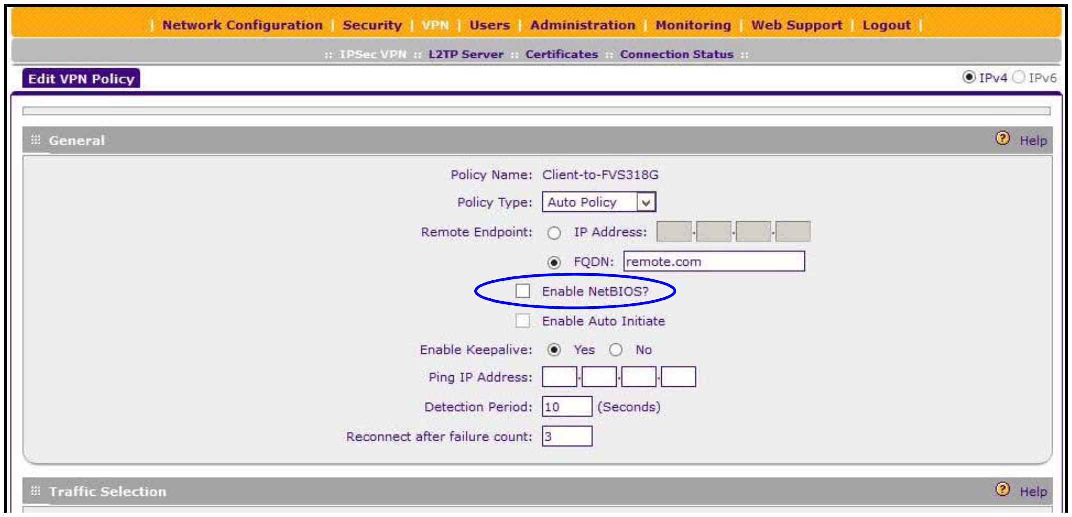
      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Policies**.

The VPN Policies screen displays.

3. 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 4*.
   - **IPv6**. Select the **IPv6** radio button.

     The VPN Policies screen for IPv6 displays.
4. In the List of VPN Policies table, to the right of the VPN policy that you want to edit, click the **Edit** table button.



Policy Name: Client-to-FVS318G

Policy Type: Auto Policy

Remote Endpoint: ○ IP Address: ● FQDN: remote.com

□ Enable NetBIOS?

□ Enable Auto Initiate

Enable Keepalive: ● Yes ○ No

Ping IP Address:

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

5. Select the **Enable NetBIOS?** check box.
6. Click the **Apply** button.

   Your changes are saved.

Configure the L2TP Server

As an alternate solution to IPSec VPN tunnels, you can configure a Layer 2 Tunneling Protocol (L2TP) server on the VPN firewall to allow users to access L2TP clients over L2TP tunnels. A maximum of 25 simultaneous L2TP user sessions are supported. (The very first IP address of the L2TP address pool is used for distribution to the VPN firewall.)

An L2TP Access Concentrator (LAC) typically initiates a tunnel to fulfill a connection request from an L2TP user; the L2TP server accommodates the tunnel request. After an L2TP tunnel is established, the L2TP user can connect to an L2TP client that is located behind the VPN firewall.

IPSec VPN provides stronger authentication and encryption than L2TP. (Packets that traverse the L2TP tunnel are not encapsulated by IPSec.)

You must enable the L2TP server on the VPN firewall, specify an L2TP server address pool, and create L2TP user accounts. (L2TP users are authenticated through local authentication with geardomain.) For information about how to create L2TP user accounts, see *Configure User Accounts* on page 295.

➢ To enable the L2TP server and configure the L2TP server pool:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

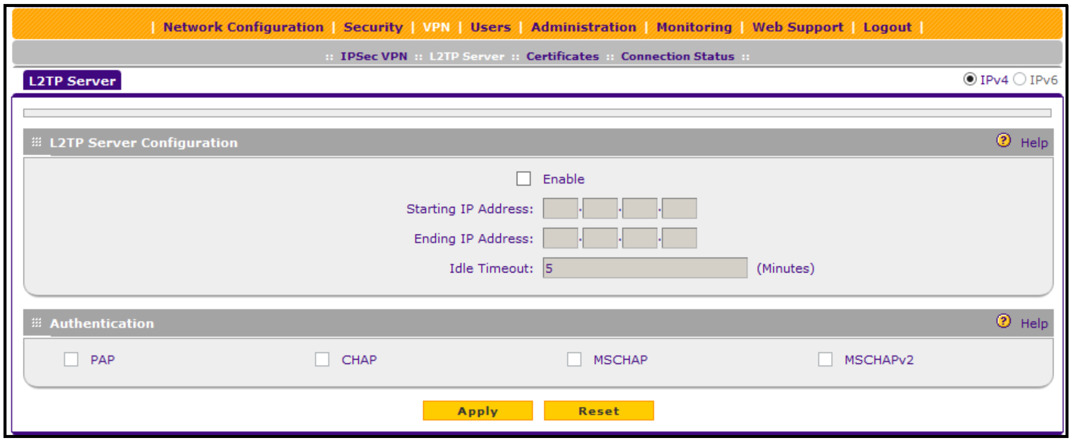
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > L2TP Server**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
L2TP Server
Help
Help
Apply
Reset

● IPv4 ○ IPv6

L2TP Server Configuration

□ Enable

Starting IP Address: ___.___.___.___

Ending IP Address: ___.___.___.___

Idle Timeout: 5 (Minutes)

Authentication

□ PAP □ CHAP □ MSCHAP □ MSCHAPv2

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

Table 63. 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 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 63. 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).	

5. Click the **Apply** button.

   Your changes are saved.

View the Active L2TP Users

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

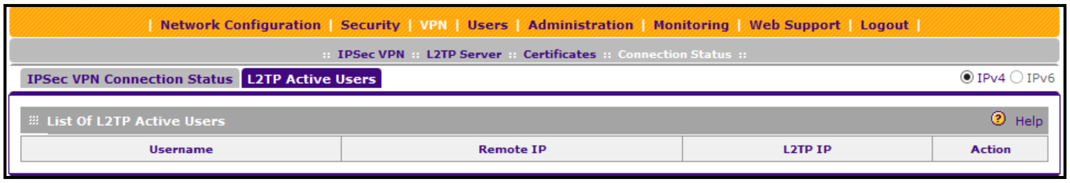
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Connection Status > L2TP Active Users**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
L2TP Active Users
● IPv4 ○ IPv6
Help

List Of L2TP Active Users

Username	Remote IP	L2TP IP	Action

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

Table 64. L2TP Active Users screen information

Item	Description
Username	The name of the L2TP user that you defined (see *Configure User Accounts* on page 295).
Remote IP	The client’s IP address on the remote LAC.

Table 64. L2TP Active Users screen information (continued)

Item	Description
L2TP IP	The IP address that is assigned by the L2TP server on the VPN firewall.
Action	Click the **Disconnect** table button to terminate the L2TP connection.

6 Manage Users, Authentication, and VPN Certificates

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

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

The VPN Firewall's Authentication Process and Options

Users are assigned to a group, and a group is assigned to a domain. Therefore, you must first create any domains, then groups, and then user accounts.

You must create name and password accounts for all users who must be able to connect to the VPN firewall. This includes administrators and guests. Accounts for IPSec VPN clients are required only if you enable extended authentication (XAUTH) in your IPSec VPN configuration.

Users connecting to the VPN firewall must be authenticated before being allowed to access the VPN firewall or the VPN-protected network. The login screen that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines the authentication method that is used.

Except in the case of IPSec VPN users, when you create a user account, you must specify a group. When you create a group, you must specify a domain.

IPSec VPN and L2TP users do not belong to a domain and are not assigned to a group.

Do not confuse the authentication groups with the LAN groups. For more information, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 71.

The following table summarizes the external authentication protocols and methods that the VPN firewall supports.

Table 65. 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).
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. For more about WiKID authentication, see *Appendix B, Two-Factor Authentication*.
NT Domain	A network-validated domain-based authentication method that functions with a Microsoft Windows NT Domain authentication server. This authentication method was superseded by Microsoft Active Directory authentication but is supported to authenticate legacy Windows clients.

Table 65. External authentication protocols and methods (continued)

Authentication Protocol or Method	Description
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

This section contains the following topics:

- *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. The default domain of the VPN firewall is named geardomain. You cannot delete the default domain.

Create Domains

➢ **To create a domain:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

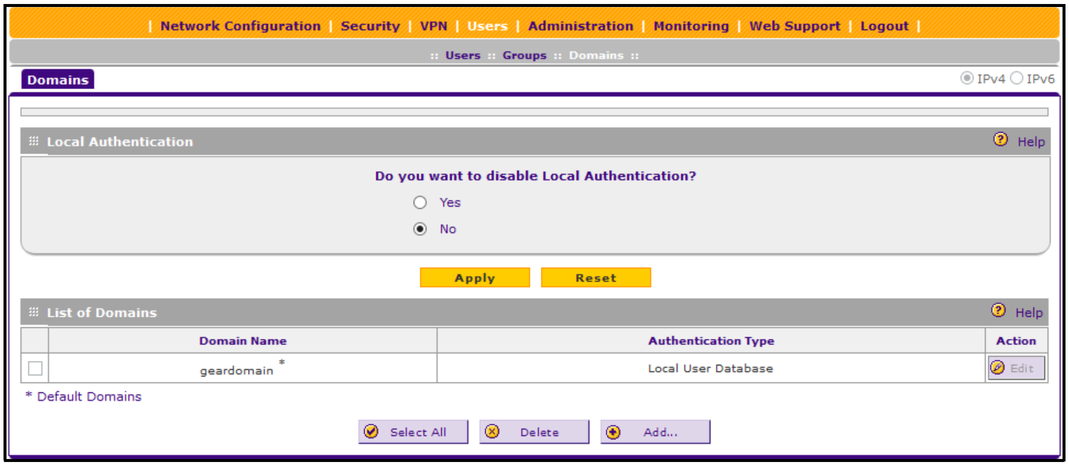
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Domains**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Domains
◉ IPv4 ○ IPv6
Help
Apply
Reset
Help
Select All
Delete
Add...

Local Authentication

Do you want to disable Local Authentication?

○ Yes

● No

List of Domains

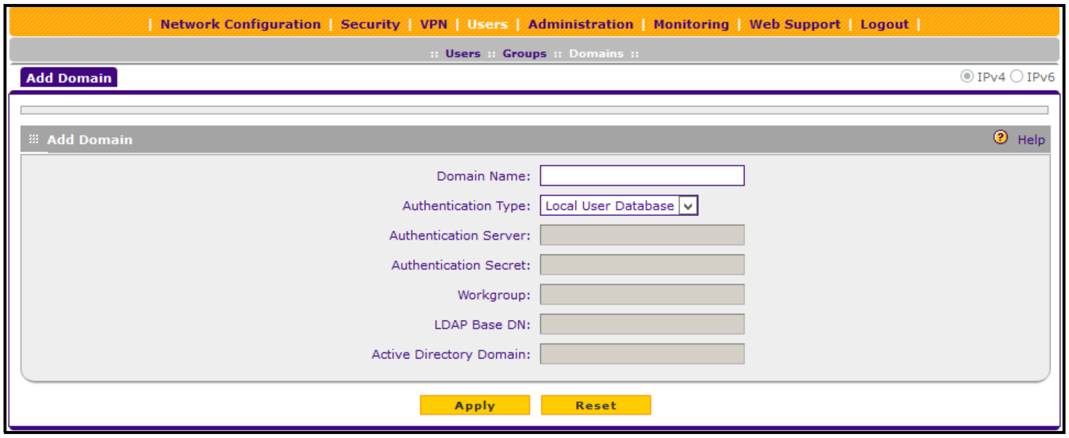
	Domain Name	Authentication Type	Action
□	geardomain *	Local User Database	Edit

* Default Domains

The List of Domains table displays the following fields:

- **Check box**. Allows you to select the domain in the table.
- **Domain Name**. The name of the domain.
- **Authentication Type**. The authentication method that is assigned to the domain.
- **Action**. The **Edit** table button, which provides access to the Edit Domain screen.

3. Under the List of Domains table, click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Add Domain
◉ IPv4 ○ IPv6
Help
Apply
Reset

Add Domain

Domain Name:	
Authentication Type:	Local User Database
Authentication Server:	
Authentication Secret:	
Workgroup:	
LDAP Base DN:	
Active Directory Domain:	

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

Table 66. Add Domain screen settings

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the list, select the authentication method that the VPN firewall applies: • **Local User Database (default)**. Users are authenticated locally on the VPN firewall. This is the default setting. You do not need to complete any other fields on this screen. • **Radius-PAP**. RADIUS Password Authentication Protocol (PAP). Complete the following fields: - **Authentication Server** - **Authentication Secret** • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the following fields: - **Authentication Server** - **Authentication Secret** • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the following fields: - **Authentication Server** - **Authentication Secret** • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the following fields: - **Authentication Server** - **Authentication Secret**

Table 66. 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 259).	• **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 L**DAP Encryption** list: - **Authentication Server** - **Active Directory Domain** • **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the following fields, and make a selection from the **LDAP Encryption** list: - **Authentication Server** - **LDAP Base DN**
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 is a user in the LDAP directory with read access to all the users that you would like to import into the VPN firewall. This 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.

5. Click the **Apply** button.

   Your changes are saved.

6. If you use local authentication, make sure that it is not disabled: in the Local Authentication section of the Domain screen, select the **No** radio button.

   A combination of local and external authentication is supported.

⚠ **WARNING:**

If you disable local authentication, make sure that at least one external administrative user is specified; otherwise, access to the VPN firewall is blocked.

7. Click the **Apply** button.

   Your changes are saved.

Delete Domains

You cannot delete the geardomain default domain.

➢ **To delete one or more domains:**

1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Users > Domains**.

   The Domains screen displays.
3. 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.
4. Click the **Delete** table button.

   The information is deleted.

Edit Domains

You cannot edit the geardomain default domain.

➢ **To edit a domain:**

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Domains**.

   The Domains screen displays.

3. In the Action column of the List of Domains table, for the domain that you want to edit, click the **Edit** table button.

   The Edit Domains screen displays. This screen is similar to the Add Domains screen.

4. Modify the settings as described in *Table 66* on page 289. You cannot modify the **Domain Name** and **Authentication Type** fields.

5. Click the **Apply** button.

   Your changes are saved.

Configure Groups

The use of groups simplifies the configuration of VPN policies when different restrictions and access controls apply to different sets of users. It also simplifies the configuration of web access exception rules. Like the default domain of the VPN firewall, the default group is also named geardomain. The default group geardomain is assigned to the default domain geardomain. You cannot delete the default domain geardomain, nor its associated default group geardomain.

IPSec VPN and L2TP users do not belong to a domain and are not assigned to a group.

For information about LAN groups, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 71.

IMPORTANT:

When you create a domain on the Domains screen (see *Create Domains* on page 287), 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.

Create Groups

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.

➢ To create a VPN group:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

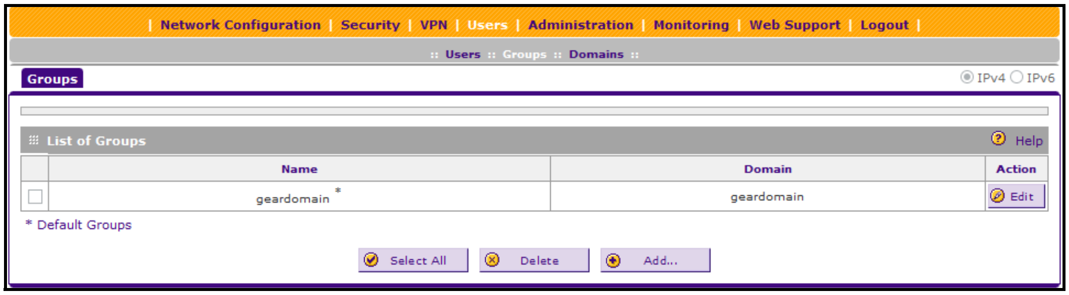
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Groups**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Groups
◉ IPv4 ○ IPv6
List of Groups
Help
Select All
Delete
Add...

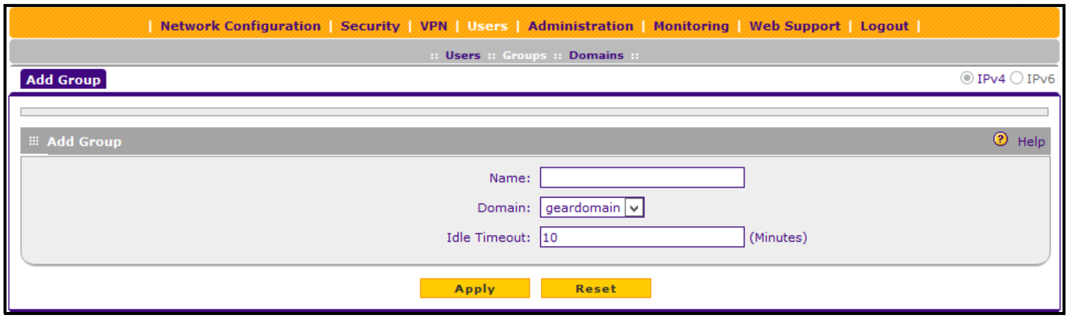
	Name	Domain	Action
□	geardomain *	geardomain	Edit

* Default Groups

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.
- **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.

3. Under the List of Groups table, click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Add Group
◉ IPv4 ○ IPv6
Add Group
Help
Apply
Reset

Name:
Domain: geardomain
Idle Timeout: 10 (Minutes)

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

Table 67. Add Group screen settings

Setting	Description
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.
Domain	The list shows the domains that are listed on the Domain screen. From the list, select the domain with which the group is associated. For information about how to configure domains, see *Configure Domains* on page 287.
Idle Timeout	The period after which an idle user is automatically logged out of the VPN firewall's web management interface. The default idle time-out period is 10 minutes.

5. Click the **Apply** button.

   Your changes are saved.

Delete Groups

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.

➢ To delete one or more groups:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Groups**.

The Groups screen displays.

3. 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.
4. Click the **Delete** table button.

   The information is deleted.

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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Groups**.

   The Groups screen displays.

3. In the Action column of the List of Groups table, for the group that you want to edit, click the **Edit** table button.

   The Edit Groups screen displays. This screen is identical to the Add Groups screen.

4. Modify the settings as described in *Table 67* on page 294.
5. Click the **Apply** button.

   Your changes are saved.

Configure User Accounts

When you create a user account, you must assign the user to a user group. When you create a group, you must assign the group to a domain that specifies the authentication method. Therefore, you should first create any domains, then groups, and then user accounts.

IPSec VPN and L2TP users do not belong to a domain and are not assigned to a group.

Two default user accounts are available:

- A user with the name **admin** and the password **password**. This is a user who is assigned 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 is assigned 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:

- **Administrator**. A user who is assigned full access and the capacity to change the VPN firewall configuration (that is, read-write access).
- **Guest user**. A user who can only view the VPN firewall configuration (that is, read-only access).
- **IPSec VPN user**. A user who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 257).
- **L2TP user**. A user who can connect over an L2TP connection to an L2TP client that is located behind the VPN firewall.

➢ To create a user account:

1. Log in to the unit:

    a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

    The NETGEAR Configuration Manager Login screen displays.

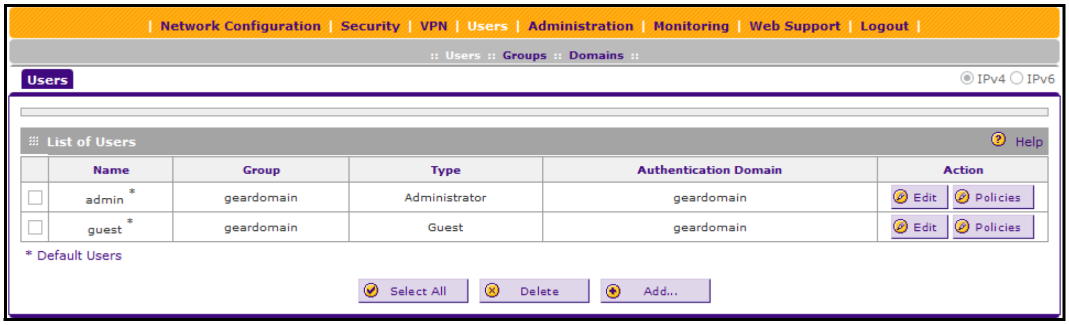
    b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

    Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

    c. Click the **Login** button.

    The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Users**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Users
● IPv4 ○ IPv6
Help
Select All
Delete
Add...

List of Users

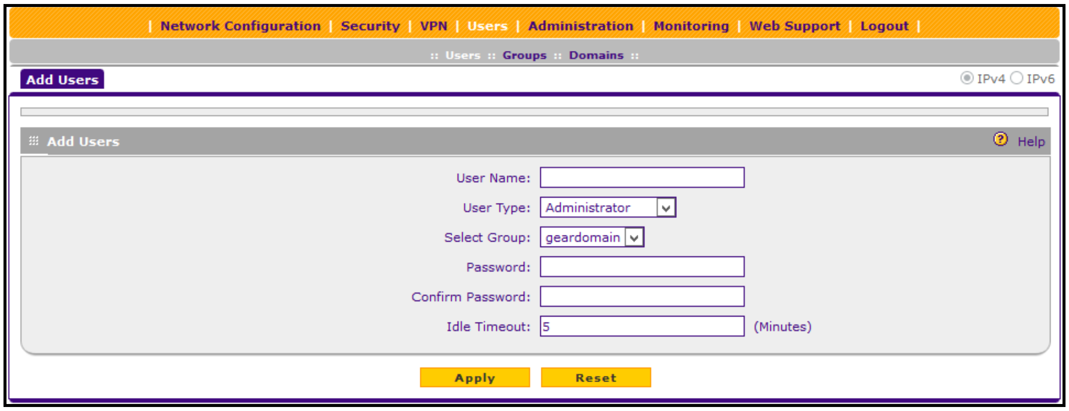
	Name	Group	Type	Authentication Domain	Action
□	admin *	geardomain	Administrator	geardomain	Edit Policies
□	guest *	geardomain	Guest	geardomain	Edit Policies

* Default Users

The List of Users table displays the users and displays the following fields:

- **Check box**. Allows you to select the user in the table.
- **Name**. The name of the user. If the user name is appended by an asterisk, the user is a default user that is preconfigured on the VPN firewall and cannot be deleted.
- **Group**. The group to which the user is assigned.
- **Type**. The type of access credentials that are assigned to the user.
- **Authentication Domain**. The authentication domain to which the user is assigned.
- **Action**. The **Edit** table button, which provides access to the Edit User screen, and the **Policies** table button, which provides access to the policy screens.

3. Under the List of Users table, click the **Add** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Add Users
● IPv4 ○ IPv6
Help
Apply
Reset

Add Users

User Name:	
User Type:	Administrator
Select Group:	geardomain
Password:	
Confirm Password:	
Idle Timeout:	5 (Minutes)

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

Table 68. Add Users screen settings

Setting	Description
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	From the list, select one of the predefined user types that determines the access credentials: • **Administrator**. A user with full access and the capacity to change the VPN firewall configuration (that is, read/write access). • **Guest User**. A user who can only view the VPN firewall configuration (that is, read-only access). • **IPSEC VPN User**. A user who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 257). • **L2TP User**. A user who can connect over an L2TP connection to an L2TP client that is located behind the VPN firewall.
Select Group	The list shows the groups that are listed on the Group screen. From the list, select the group to which the user is assigned. For information about how to configure groups, see *Configure Groups* on page 292. **Note:** The user is assigned to the domain that is associated with the selected group.
Password	The password that the user must enter to gain access to the VPN firewall.
Confirm Password	This field must be identical to the password that you entered in the **Password** field.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes.

5. Click the **Apply** button.

   Your changes are saved.

You cannot delete the default admin, user, or guest user.

➢ **To delete one or more user accounts:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Users**.

   The Users screen displays.

3. 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.
4. Click the **Delete** table button.

   The information is deleted.

Set User Login Policies

You can restrict the ability of defined users to log in to the VPN firewall’s web management interface. You can also require or prohibit logging in from certain IP addresses or from particular browsers.

This section contains the following topics:

- *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. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.

   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

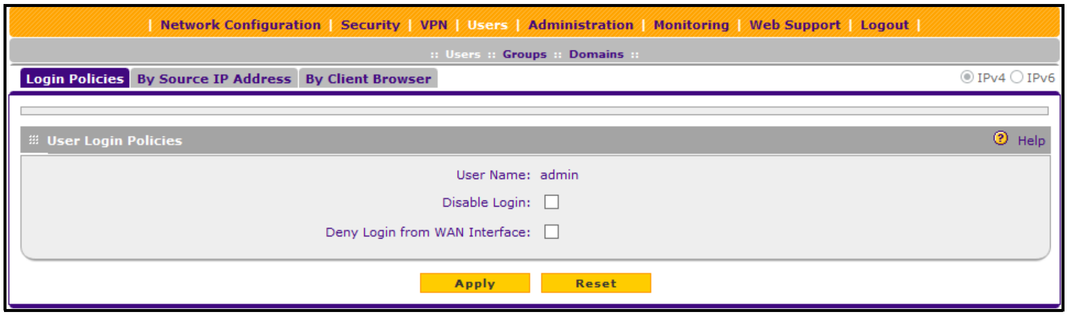
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Users**.

   The Users screen displays.

3. In the Action column of the List of Users table, for the user for which you want to set login policies, click the **Policies** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Login Policies
By Source IP Address
By Client Browser
● IPv4 ○ IPv6
User Login Policies
Help
Apply
Reset

User Name: admin

Disable Login: □

Deny Login from WAN Interface: □

4. Make the following optional selections:
   - To prohibit the user from logging in to the VPN firewall, select the **Disable Login** check box.
   - To prohibit the user from logging in from the WAN interface, select the **Deny Login from WAN Interface** check box.

     In this case, the user can log in only from the LAN interface.

   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.

5. Click the **Apply** button.

   Your changes are saved.

Configure Login Restrictions Based on IPv4 Addresses

➤ **To restrict logging in based on IPv4 addresses:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

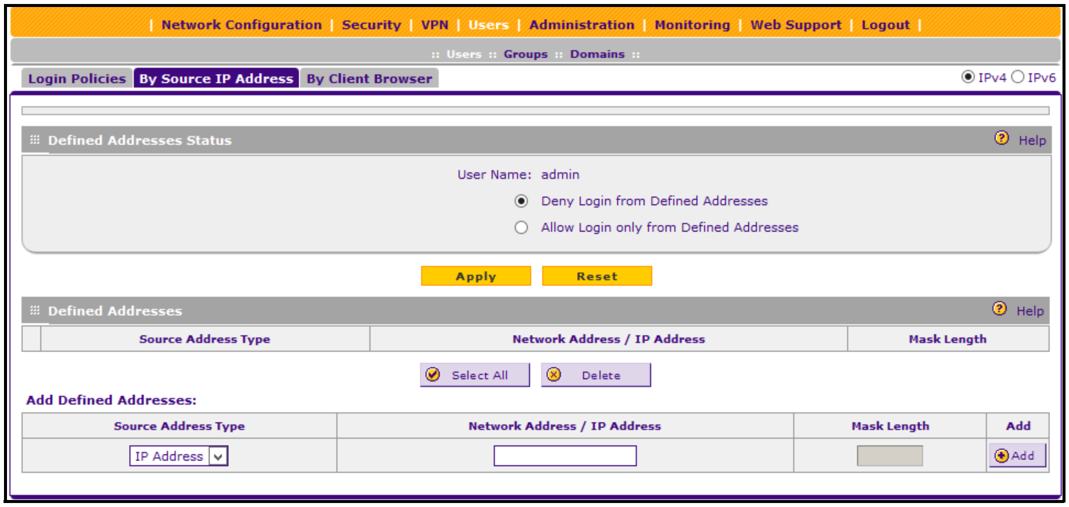
2. Select **Users > Users**.

   The Users screen displays.

3. In the Action column of the List of Users table, for the user for which you want to set login policies, click the **Policies** table button.

The policies submenu tabs display, with the Login Policies screen in view.

4. Click the **By Source IP Address** submenu tab.



User Name: admin

● Deny Login from Defined Addresses

○ Allow Login only from Defined Addresses

	Source Address Type	Network Address / IP Address	Mask Length

Add Defined Addresses:

Source Address Type	Network Address / IP Address	Mask Length	Add
IP Address			Add

5. In the Defined Addresses Status section, 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 the **Apply** button.

   Your changes are saved.

7. In the Add Defined Addresses section, add an address to the Defined Addresses table by entering the settings as described in the following table:

Table 69. Defined addresses settings for IPv4

Setting	Description
Source Address Type	Select the type of address from the list: • **IP Address**. A single IPv4 address. • **IP Network**. A subnet of IPv4 addresses. You must enter a netmask length in the **Mask Length** field.
Network Address / IP Address	Depending on your selection from the **Source Address Type** 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.

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 IPv4 addresses:**

1. Log in to the unit:
    a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

       The NETGEAR Configuration Manager Login screen displays.

    b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

       Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

    c. Click the **Login** button.

       The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Users**.

   The Users screen displays.

3. Click the **By Source IP Address** submenu tab.
4. 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.
5. Click the **Delete** table button.

   The information is deleted.

Configure Login Restrictions Based on IPv6 Addresses

- **To restrict logging in based on IPv6 addresses:**

1. Log in to the unit:
    a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

       The NETGEAR Configuration Manager Login screen displays.

    b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

       Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

    c. Click the **Login** button.

       The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

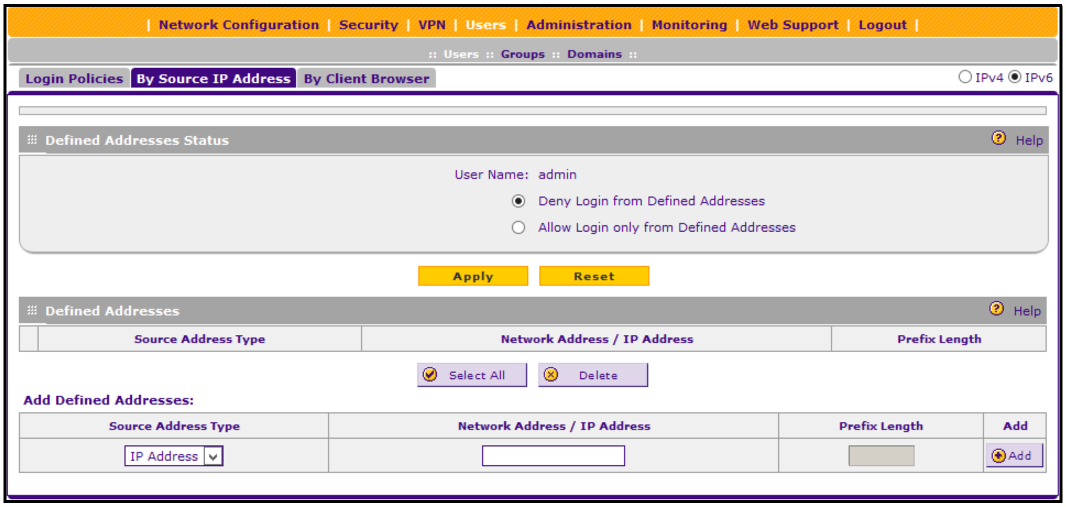
2. Select **Users > Users**.

   The Users screen displays.

3. In the Action column of the List of Users table, for the user for which you want to set login policies, click the **Policies** table button.

   The policies submenu tabs display, with the Login Policies screen in view.

4. Click the **By Source IP Address** submenu tab.
5. In the upper right of the screen, select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Login Policies
By Source IP Address
By Client Browser
○ IPv4 ● IPv6
Help
Apply
Reset
Select All
Delete
Add

Defined Addresses Status

User Name: admin

● Deny Login from Defined Addresses

○ Allow Login only from Defined Addresses

Defined Addresses

	Source Address Type	Network Address / IP Address	Prefix Length

Add Defined Addresses:

Source Address Type	Network Address / IP Address	Prefix Length	Add
IP Address			Add

6. In the Defined Addresses Status section, 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.
7. Click the **Apply** button.

   Your changes are saved.
8. In the Add Defined Addresses section, add an address to the Defined Addresses table by entering the settings as described in the following table:

Table 70. Defined addresses settings for IPv6

Setting	Description
Source Address Type	Select the type of address from the list: • **IP Address**. A single IPv6 address. • **IP Network**. A subnet of IPv6 addresses. You must enter a prefix length in the **Prefix Length** field.
Network Address / IP Address	Depending on your selection from the **Source Address Type** 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.

9. Click the **Add** table button.

   The address is added to the Defined Addresses table.
10. Repeat *Step 8* and *Step 9* for any other addresses that you want to add to the Defined Addresses table.

➤ **To delete one or more IPv6 addresses:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Users**.

   The Users screen displays.

3. Click the **By Source IP Address** submenu tab.
4. 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.
5. Click the **Delete** table button.

   The information is deleted.

Configure Login Restrictions Based on Web Browser

➤ **To restrict logging in based on the user's browser:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

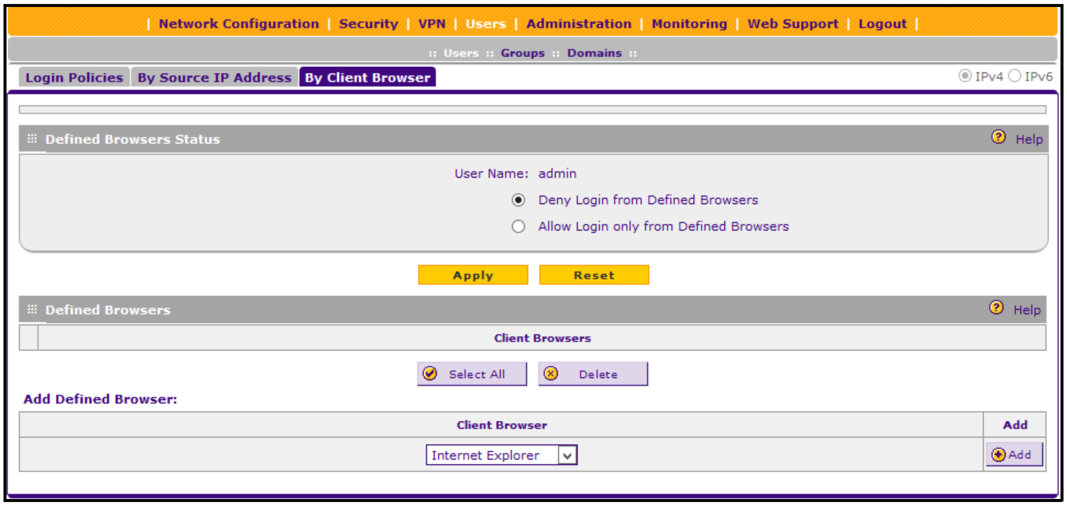
2. Select **Users > Users**.

   The Users screen displays.

3. In the Action column of the List of Users table, for the user for which you want to set login policies, click the **Policies** table button.

   The policies submenu tabs display, with the Login Policies screen in view.

4. Click the **By Client Browser** submenu tab.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Login Policies
By Source IP Address
By Client Browser
Help
Apply
Reset
Help
Select All
Delete
Add
Add

◉ IPv4 ○ IPv6

Defined Browsers Status

User Name: admin

● Deny Login from Defined Browsers

○ Allow Login only from Defined Browsers

Defined Browsers

	Client Browsers

Add Defined Browser:

Client Browser	Add
Internet Explorer	Add

5. 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.
6. Click the **Apply** button.

   Your changes are saved.
7. In the Add Defined Browser section, add a browser to the **Defined Browsers** table by selecting one of the following browsers from the list:
   - **Internet Explorer**.
   - **Opera**.
   - **Netscape Navigator**.
   - **Firefox**. Mozilla Firefox.
   - **Mozilla**. Other Mozilla browsers.
8. Click the **Add** table button.

   The browser is added to the **Defined Browsers** table.
9. Repeat *Step 7* and *Step 8* for any other browsers that you want to add to the Defined Browsers table.

➢ To delete one or more browsers:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Users**.

   The Users screen displays.

3. Click the **By Client Browser** submenu tab.
4. 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.
5. Click the **Delete** table button.

   The information is deleted.

Change Passwords and Other User Settings

For any user, you can change the password, user type, and idle time-out settings. Only administrators are assigned read/write access. All other users are assigned read-only access.

- 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.
- The most secure password contains no dictionary words from any language and is a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 32 characters.
- After a factory defaults reset, the password and time-out value are changed back to **password** and five minutes, respectively.

Once they are established, you cannot change the user name or the group. If you must change the user name or the group, delete the user account and recreate it with the correct name or group.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

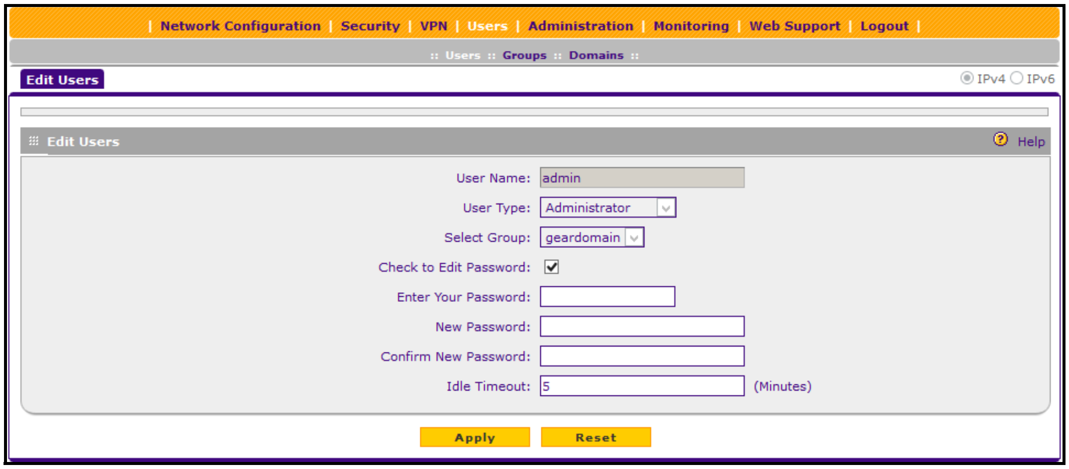
c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Users > Users**.

The Users screen displays.

3. In the Action column of the List of Users table, for the user for which you want to modify the settings, click the **Edit** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Edit Users
● IPv4 ○ IPv6
Edit Users
Help
Apply
Reset

User Name: admin

User Type: Administrator

Select Group: geardomain

Check to Edit Password: ☑

Enter Your Password:

New Password:

Confirm New Password:

Idle Timeout: 5 (Minutes)

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

Table 71. Edit User screen settings

Setting	Description	
Select User Type	From the list, select one of the predefined user types that determines the access credentials: • **Administrator**. User with full access and the capacity to change the VPN firewall configuration (that is, read/write access). • **Guest (readonly)**. User who can only view the VPN firewall configuration (that is, read-only access). • **IPSEC VPN User**. You cannot change an existing user from the IPSEC VPN User type to another type or from another type to the IPSEC VPN User type. • **L2TP User**. You cannot change an existing user from the L2TP User type to another type or from another type to the L2TP User type.	
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 logged in.
	New Password	Enter the new password.
	Confirm New Password	Reenter the new password for confirmation.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes.	

5. Click the **Apply** button.

Your changes are saved.

Manage Digital Certificates for VPN Connections

The VPN firewall uses digital certificates (also known as X509 certificates) during the Internet Key Exchange (IKE) authentication phase to authenticate connecting IPSec VPN gateways or clients, or to be authenticated by remote entities. You can do the following:

- On the VPN firewall, you can enter a digital certificate on the IKE Policies screen, on which the certificate is referred to as an RSA signature.
- On the VPN client, you can enter a digital certificate on the Authentication pane in the Configuration Panel screen.

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 must be used for one of the purposes defined by the extension. For example, if the digital certificate contains the extKeyUsage extension that is defined for SNMPv2, the same certificate cannot be used for secure web management. The extKeyUsage would govern the certificate acceptance criteria on the VPN firewall when the same digital certificate is being used for secure web management.

On the VPN firewall, the uploaded digital certificate is checked for validity and purpose. The digital certificate is accepted when it passes the validity test and the purpose matches its use. The check for the purpose must correspond to its use for IPSec VPN. If the defined purpose is for IPSec VPN, the digital certificate is uploaded to both the IPSec VPN certificate repository. However, if the defined purpose is for IPSec VPN only, the certificate is uploaded only to the IPSec VPN certificate repository.

The VPN firewall uses digital certificates to authenticate connecting VPN gateways or clients, and to be authenticated by remote entities. A digital certificate that authenticates a server, for example, is a file that contains the following elements:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

You can obtain a digital certificate from a well-known commercial certification authority (CA) such as Verisign or Thawte, or you can generate and sign your own digital certificate. Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server’s identity. A self-signed digital certificate triggers a warning from most browsers because it provides no protection against identity theft of the server.

The VPN firewall contains a self-signed digital certificate from NETGEAR. This certificate can be downloaded from the VPN firewall login screen for browser import. However, NETGEAR recommends that you replace this digital certificate with a digital certificate from a well-known commercial CA before you deploy the VPN firewall in your network.

This section contains the following topics:

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

VPN Certificates

You can view the loaded digital certificates, upload a new digital certificate, and generate a certificate signing request (CSR). The VPN firewall typically holds two types of digital certificates:

- **CA certificates**. Each CA issues its own digital certificate to validate communication with the CA and to verify the validity of digital certificates that are signed by the CA.
- **Self-signed certificates**. The digital certificates 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.

  For more information, see *Manage VPN CA Certificates* on page 309.

- **Active Self Certificates table**. Contains the self-signed certificates that were issued by CAs and that you uploaded.

  For more information, see *Manage VPN Self-Signed Certificates* on page 311.

- **Self Certificate Requests table**. Contains the self-signed certificate requests that you generated. These requests were either submitted to CAs or not, and CAs either issued digital certificates for these requests or did not. Only the self-signed certificates in the Active Self Certificates table are active on the VPN firewall.

  For more information, see *Manage VPN Self-Signed Certificates* on page 311.

- **Certificate Revocation Lists (CRL) table**. Contains the lists with digital certificates that were 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.

  For more information, see *Manage the VPN Certificate Revocation List* on page 316.

Manage VPN CA Certificates

➢ **To view and upload trusted certificates:**

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

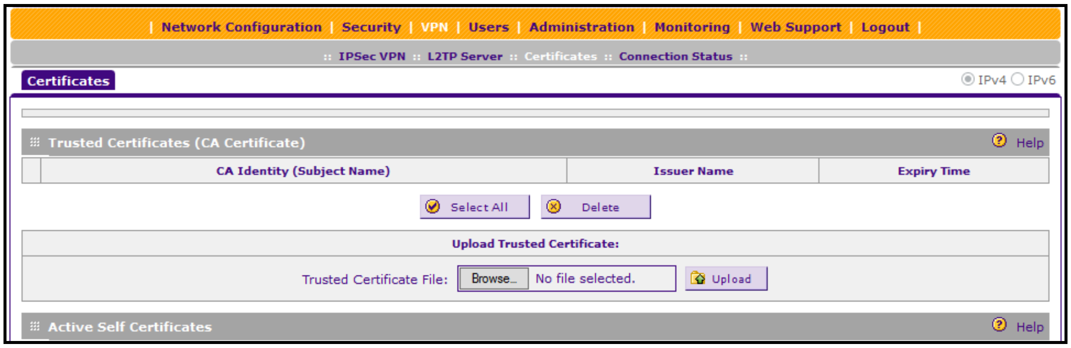
b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Certificates**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
Certificates
● IPv4 ○ IPv6
Trusted Certificates (CA Certificate)
Help
CA Identity (Subject Name)
Issuer Name
Expiry Time
Select All
Delete
Upload Trusted Certificate:
Trusted Certificate File:
Browse...
No file selected.
Upload
Active Self Certificates
Help

The Trusted Certificates (CA Certificate) table lists the digital certificates of CAs and contains the following fields:

- **CA Identity (Subject Name)**. The organization or person to whom the digital certificate is issued.
- **Issuer Name**. The name of the CA that issued the digital certificate.
- **Expiry Time**. The date after which the digital certificate becomes invalid.

➢ To upload a digital certificate of a trusted CA on the VPN firewall:

1. Download a digital certificate file from a trusted CA and store it on your computer.

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Certificates**.

   The Certificates screen displays.

3. In the Upload Trusted Certificates section of the screen, navigate to the trusted digital certificate file that you downloaded on your computer and click the **Browse** button.
4. Click the **Upload** table button.

   If the verification process on the VPN firewall approves the digital certificate for validity and purpose, the digital certificate is added to the Trusted Certificates (CA Certificates) table.

➢ **To delete one or more digital certificates:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Certificates**.

   The Certificates screen displays.

3. 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.
4. Click the **Delete** table button.

   The information is deleted.

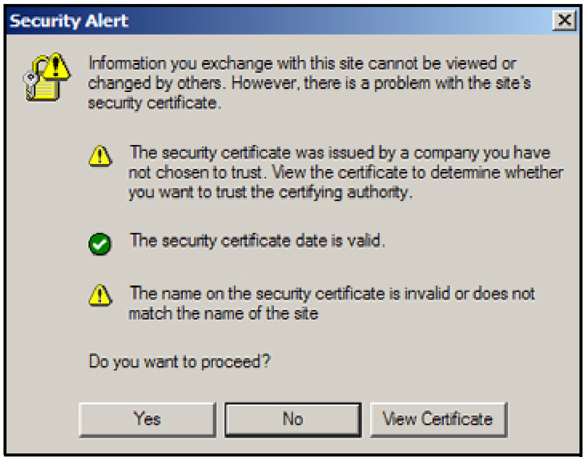
Manage VPN Self-Signed Certificates

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.)

A security alert can be generated for a security certificate for three reasons:

- The security certificate was issued by a company you did not choose 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.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Generate a CSR and Obtain a Self-Signed Certificate from a CA

To use a self-signed certificate, you first must request the digital certificate from a CA and download and activate the digital certificate on the VPN firewall. To request a self-signed certificate from a CA, you must generate a certificate signing request (CSR) for and on the VPN firewall. The CSR is a file that contains information about your company and about the device that holds the certificate. Refer to the CA for guidelines about the information that you must include in your CSR.

➤ **To generate a new CSR file, obtain a digital certificate from a CA, and upload it to the VPN firewall:**

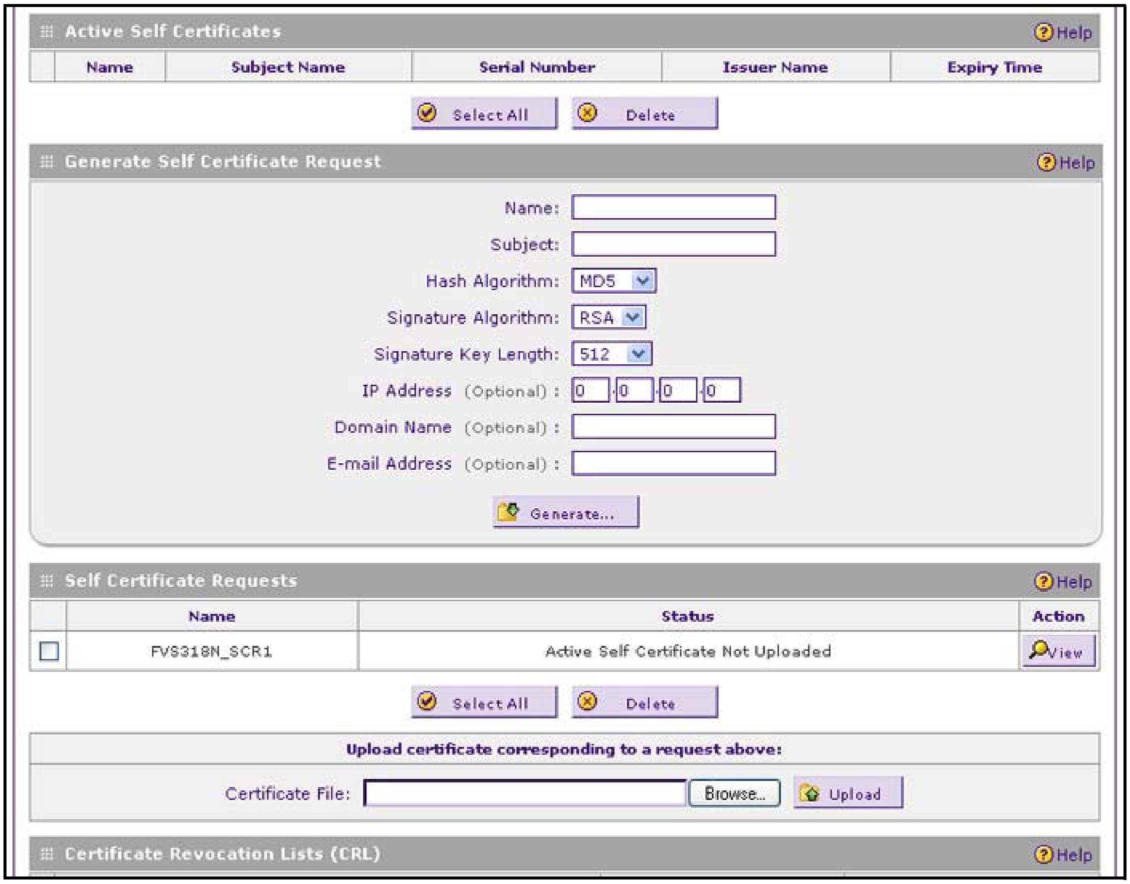
1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **VPN > Certificates**.

The Certificates screen displays. Scroll down.



Active Self Certificates ?Help

	Name	Subject Name	Serial Number	Issuer Name	Expiry Time

Generate Self Certificate Request ?Help

Name:	
Subject:	
Hash Algorithm:	MD5
Signature Algorithm:	RSA
Signature Key Length:	512
IP Address (Optional) :	0 . 0 . 0 . 0
Domain Name (Optional) :	
E-mail Address (Optional) :	

Self Certificate Requests ?Help

	Name	Status	Action
□	FVS318N_SCR1	Active Self Certificate Not Uploaded	View

Upload certificate corresponding to a request above:

Certificate File:

Certificate Revocation Lists (CRL) ?Help

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

Table 72. 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 use the same value in the **Subject** field.
Hash Algorithm	From the list, select the hash algorithm: • **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 list, the only possible selection is **RSA**. In other words, RSA is the default to generate a CSR.

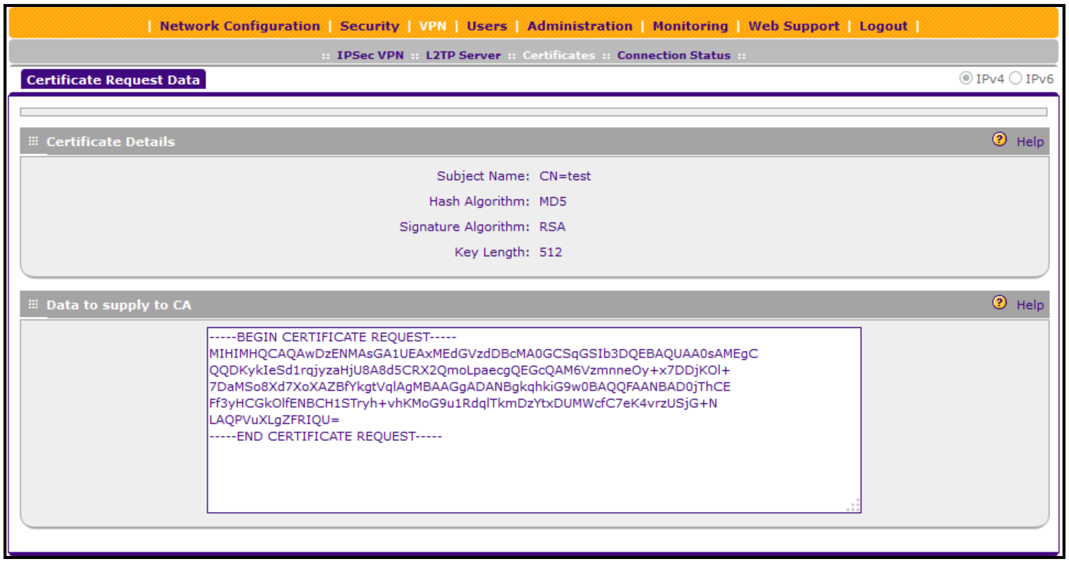
Table 72. Generate self-signed certificate request settings (continued)

Setting	Description	
Signature Key Length	From the list, select the signature key length 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.

4. Click the **Generate** table button.

   A new SCR is created and added to the Self Certificate Requests table.

5. To view the new SCR, in the Self Certificate Requests table, in the Action column, click the **View** table button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
Certificate Request Data
● IPv4 ○ IPv6
Certificate Details
Help
Data to supply to CA
Help

Subject Name: CN=test
Hash Algorithm: MD5
Signature Algorithm: RSA
Key Length: 512

```
-----BEGIN CERTIFICATE REQUEST-----
MIHIMHQCAQAwDzENMAsGA1UEAxMEdGVzdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgC
QQDKykIeSd1rqjyzaHjU8A8d5CRX2QmoLpaecgQEGcQAM6VzmnneOy+x7DDjKOl+
7DaMSo8Xd7XoXAZBfYkgtVqlAgMBAAGgADANBgkqhkiG9w0BAQQFAANBAD0jThCE
Ff3yHCGkOlfENBCH1STryh+vhKMoG9u1RdqlTkmDzYtxDUMWcfC7eK4vrzUSjG+N
LAQPVuXLgZFRIQU=
-----END CERTIFICATE REQUEST-----
```

6. 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-----.”

7. 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.

8. Download the digital certificate file from the CA and store it on your computer.
9. Return to the Certificates screen and locate the Self Certificate Requests section.
10. Select the check box next to the self-signed certificate request.
11. Click the **Browse** button and navigate to the digital certificate file from the CA that you just stored on your computer.
12. Click the **Upload** table button.

    If the verification process on the VPN firewall approves the digital certificate for validity and purpose, the digital certificate is added to the Active Self Certificates table.

➢ **To delete one or more SCRs:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Certificates**.

   The Certificates screen displays.

3. 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.
4. Click the **Delete** table button.

   The information is deleted.

View and Manage Self-Signed Certificates

The Active Self Certificates table on the Certificates screen 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. Renew the digital certificate before it expires.

➢ **To delete one or more self-signed certificates:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **VPN > Certificates**.

   The Certificates screen displays.
3. 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.
4. Click the **Delete** table button.

   The information is deleted.

Manage the VPN Certificate Revocation List

A Certificate Revocation List (CRL) file shows digital certificates that were revoked and are no longer valid. Each CA issues its own CRLs. It is important that you keep your CRLs up-to-date. Obtain the CRL for each CA regularly.

➢ **To view the loaded CRLs and upload a new CRL:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

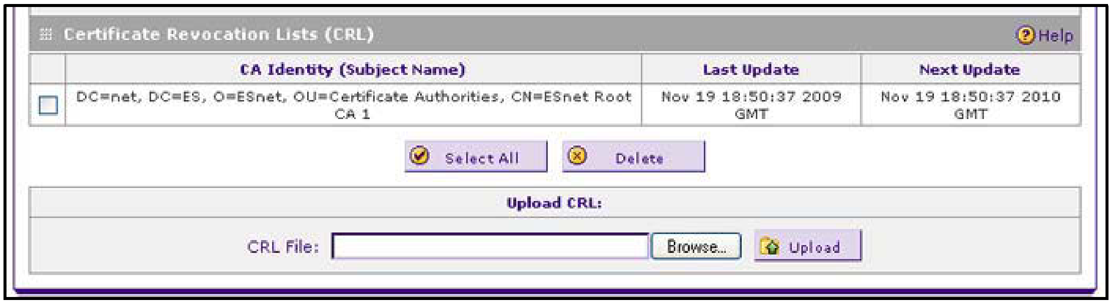
      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Certificates**.

   The Certificates screen displays. Scroll down.



Certificate Revocation Lists (CRL)

	CA Identity (Subject Name)	Last Update	Next Update
□	DC=net, DC=ES, O=ESnet, OU=Certificate Authorities, CN=ESnet Root CA 1	Nov 19 18:50:37 2009 GMT	Nov 19 18:50:37 2010 GMT

Upload CRL:

CRL File:

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.

3. In the Upload CRL section, click the **Browse** button and navigate to the CLR file that you previously downloaded from a CA.
4. Click the **Upload** table button.

   The following occurs:

   - If the verification process on the VPN firewall approves the CRL, the CRL is added to the Certificate Revocation Lists (CRL) table.
   - 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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Certificates**.

   The Certificates screen displays.

3. 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.

4. Click the **Delete** table button.

   The information is deleted.

Network and System Management 7

This chapter describes the tools for managing the network traffic to optimize its performance and the system management features of the VPN firewall. The chapter contains the following sections:

- *Performance Management*
- *System Management*

Performance Management

Performance management consists of controlling the traffic through the VPN firewall so that the necessary traffic gets through when there is a bottleneck. You can either reduce unnecessary traffic or reschedule some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The VPN firewall provides the necessary features and tools to help the network manager accomplish these goals.

This section contains the following topics:

- *Bandwidth Capacity*
- *Features That Reduce Traffic*
- *Features That Increase Traffic*
- *Use QoS and Bandwidth Assignment to Shift the Traffic Mix*
- *Monitoring Tools for Traffic Management*

Bandwidth Capacity

The maximum bandwidth capacity of the 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 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 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

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 did not define 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 sections summarize the various criteria that you can apply to outbound rules to reduce traffic.

- For more information about outbound rules, see *Outbound Rules* on page 128.
- For detailed procedures about how to configure outbound rules, see *Configure LAN WAN Rules* on page 134 and *Configure DMZ WAN Rules* on page 144.

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 must define it using the Services screen. For more information, see *Outbound Rules* on page 128 and *Add Customized Services* on page 176.
- **LAN users (or DMZ users)**. You can specify which computers on your network are affected by an outbound rule. Several options are available:
  - **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 as follows:
    - 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. For more information, see *Manage the Network Database* on page 73.
    - Computers and network devices are entered into the network database by various methods. For more information, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 71.
- **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 195.
- **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 183.
- **Bandwidth profile**. You can define bandwidth profiles and then apply the 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 180.

Content Filtering

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the VPN firewall’s content-filtering feature. By default, this feature is disabled; all requested traffic from any website is allowed.

To reduce traffic, the VPN firewall provides the following methods to filter web content:

- **Keyword blocking**. You can specify words that, if they appear in the website name (URL) or newsgroup name, cause that site or newsgroup to be blocked by the VPN firewall.
- **Web object blocking**. You can block the following web component types: embedded objects (ActiveX and Java), proxies, and cookies.

To further narrow down the content filtering, you can configure groups to which the content-filtering rules apply and trusted domains for which the content-filtering rules do not apply.

Source MAC Filtering

If you want to reduce outgoing traffic by preventing Internet access by certain computers on the LAN, you can use the source MAC filtering feature to drop the traffic received from the computers with the specified MAC addresses. By default, this feature is disabled; all traffic received from computers with any MAC address is allowed. For more information, see *Enable Source MAC Filtering* on page 196.

Features That Increase Traffic

The following features of the VPN firewall tend to increase the traffic load on the WAN side:

- LAN WAN inbound rules (also referred to as port forwarding)
- DMZ WAN inbound rules (also referred to as port forwarding)
- Port triggering
- Enabling the DMZ port
- Configuring exposed hosts

- Configuring VPN tunnels

LAN WAN Inbound Rules and DMZ WAN Inbound Rules

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 did not define 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 sections summarize the various criteria that you can apply to inbound rules and that might increase traffic.

- For more information about inbound rules, see *Inbound Rules* on page 130.
- For detailed procedures about how to configure inbound rules, see *Configure LAN WAN Rules* on page 134 and *Configure DMZ WAN Rules* on page 144.

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 must define it using the Services screen. For more information, see *Inbound Rules* on page 130 and *Add Customized Services* on page 176.
- **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, several options are available:
  - **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 as follows.
    - 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. For more information, see *Manage the Network Database* on page 73.
    - Computers and network devices are entered into the network database by various methods. For more information, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 71.
- **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 195.
- **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 180.

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 information about how to configure port triggering, see *Configure Port Triggering* on page 206.

DMZ Port

The demilitarized zone (DMZ) is a network that, by default, is configured with 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 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 96. For information about how to configure DMZ traffic rules, see *Configure DMZ WAN Rules* on page 144.

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 did not yet define. 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 165.

VPN and L2TP Tunnels

The VPN firewall supports site-to-site IPSec 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 5, Virtual Private Networking Using IPSec and L2TP Connections*.

Use QoS and Bandwidth Assignment to Shift the Traffic Mix

By setting the QoS priority and assigning bandwidth profiles to firewall rules, you can shift the traffic mix to aim for optimum performance of the VPN firewall.

Set QoS Priorities

The QoS priority settings determine the Quality of Service for the traffic passing through the VPN firewall. You can 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 would otherwise be assigned.

For more information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 183.

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 180.

Monitoring Tools for Traffic Management

The VPN firewall includes several tools that can be used to monitor the traffic conditions of the firewall and content-filtering engine and to monitor the users' access to the Internet and the types of traffic that they are allowed to send and receive. For more information about these tools, see *Chapter 8, Monitor System Access and Performance*.

System Management

This section contains the following topics:

- *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.

After a factory defaults reset, the password and time-out value are changed back to password and five minutes, respectively.

For general information about user accounts, passwords, and login settings, see *Configure User Accounts* on page 295 and *Set User Login Policies* on page 299.

➤ **To modify the administrator and guest passwords and idle time-out settings:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

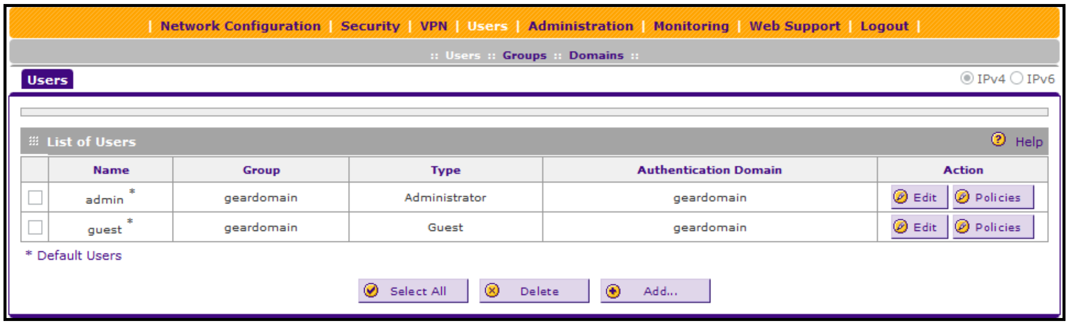
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

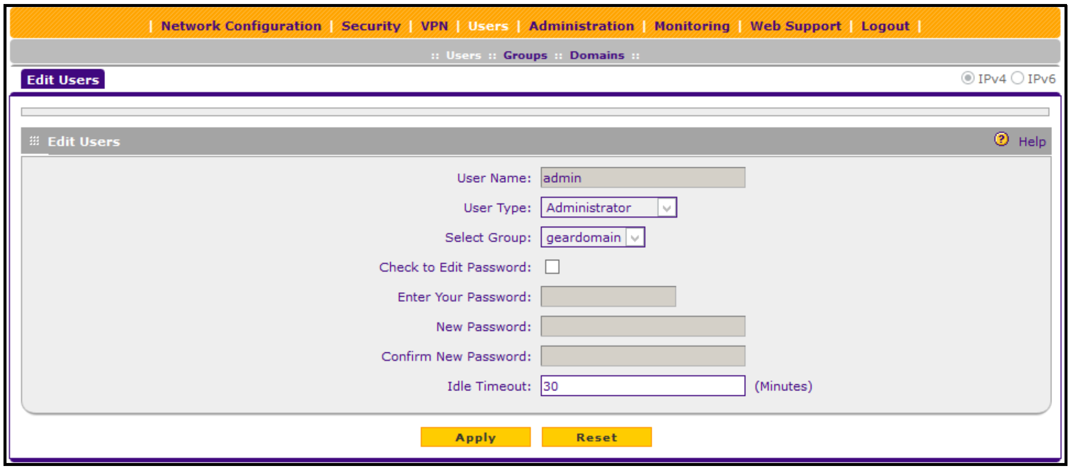
2. Select **Users > Users**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Users
● IPv4 ○ IPv6
List of Users
Help
Select All
Delete
Add...

	Name	Group	Type	Authentication Domain	Action
□	admin *	geardomain	Administrator	geardomain	Edit Policies
□	guest *	geardomain	Guest	geardomain	Edit Policies

* Default Users

3. In the Action column of the List of Users table, click the **Edit** table button for the user with the name admin.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Edit Users
● IPv4 ○ IPv6
Edit Users
Help
Apply
Reset

User Name:	admin
User Type:	Administrator
Select Group:	geardomain
Check to Edit Password:	□
Enter Your Password:	
New Password:	
Confirm New Password:	
Idle Timeout:	30 (Minutes)

You cannot modify the administrator user name, user type, or group assignment.

4. Select the **Check to Edit Password** check box.

   The password fields become available.

5. Enter the old password, enter the new password, and confirm the new password.

   The most secure password should no dictionary words from any language and is a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 32 characters.

6. To 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.

7. Click the **Apply** button.

   Your changes are saved.

8. Repeat *Step 2* through *Step 7* for the user with the name guest.

You can also change the administrator login policies:

- **Disable login**. Deny login access.

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.

  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. For more information, see *Set User Login Policies* on page 299.

Configure Remote Management Access

When remote management is enabled and administrative access through a WAN interface is granted, the VPN firewall's web management interface is accessible to anyone who knows its IP address and default password. Because a malicious WAN user can reconfigure the VPN firewall and misuse it in many ways, NETGEAR recommends that you change the admin and guest default passwords before continuing. For more information, see *Configure Login Policies* on page 299 and *Change Passwords and Administrator and Guest Settings* on page 326.

➢ **To configure the VPN firewall for remote management:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

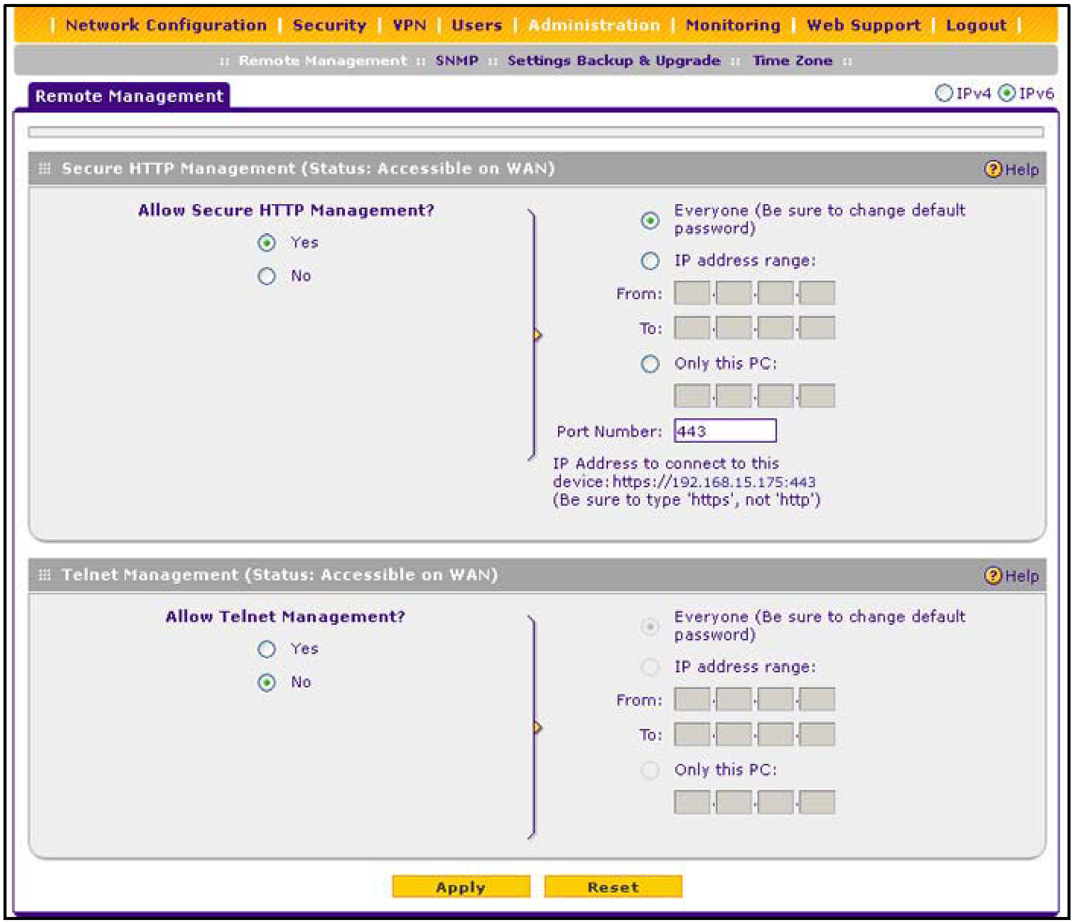
      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Administration > Remote Management**.

   The Remote Management screen displays the IPv4 settings.
3. 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 4*.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Remote Management
○ IPv4 ● IPv6
Help
Help
Apply
Reset

Secure HTTP Management (Status: Accessible on WAN)

Allow Secure HTTP Management?

● Yes

○ No

● Everyone (Be sure to change default password)

○ IP address range:

From:

To:

○ Only this PC:

Port Number: 443

IP Address to connect to this device: https://192.168.15.175:443
(Be sure to type 'https', not 'http')

Telnet Management (Status: Accessible on WAN)

Allow Telnet Management?

○ Yes

● No

● Everyone (Be sure to change default password)

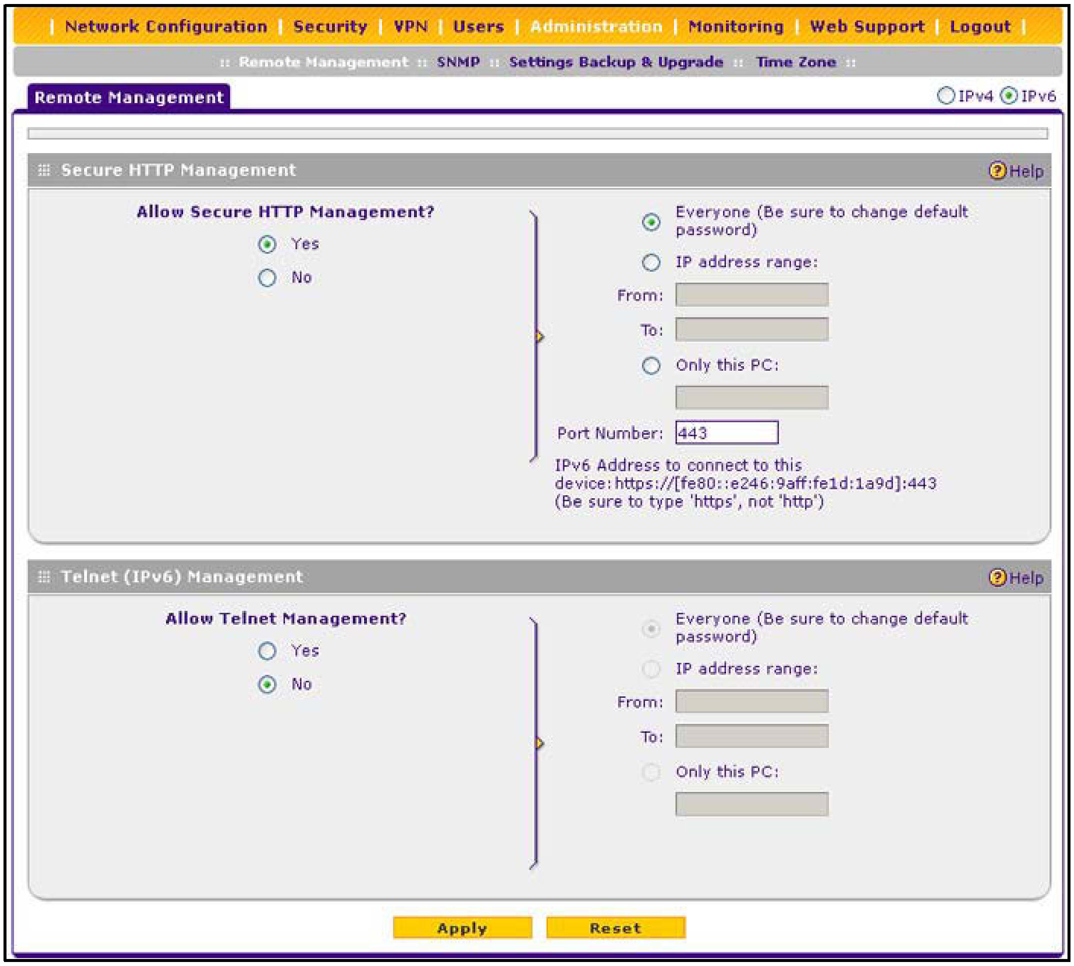
○ IP address range:

From:

To:

○ Only this PC:

- **IPv6**. Select the **IPv6** radio button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Remote Management
○ IPv4 ● IPv6
Help
Help
Apply
Reset

Secure HTTP Management

Allow Secure HTTP Management?
● Yes
○ No

● Everyone (Be sure to change default password)
○ IP address range:
From:
To:
○ Only this PC:

Port Number: 443

IPv6 Address to connect to this device: https://[fe80::e246:9aff:fe1d:1a9d]:443
(Be sure to type 'https', not 'http')

Telnet (IPv6) Management

Allow Telnet Management?
○ Yes
● No

● Everyone (Be sure to change default password)
○ IP address range:
From:
To:
○ Only this PC:

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

Table 73. 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.
	Select the addresses through which access is allowed: • **Everyone**. No IP addresses are restricted. • **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 73. 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.	
	Select the addresses through which access is allowed: • **Everyone**. No IP addresses are restricted. • **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.	

5. Click the **Apply** button.

   Your changes are saved.

Use the Command-Line Interface

You can access the command-line interface (CLI) using the console port on the rear panel of the VPN firewall. For more information, see *Rear Panel* on page 16.

You can access the CLI from a communications terminal when the VPN firewall is still set to its factory defaults (or use your own settings if you changed them).

➤ **To access the CLI:**

1. From your computer’s command-line prompt, enter the following command:

   ```
   telnet <ip address>
   ```

   in which *ip address* is the IP address of the VPN firewall.
2. Enter **admin** and **password** when prompted for the login and password information (or enter **guest** and **password** to log in as a read-only guest).
3. Enter **exit** to end the CLI session.

Any configuration changes made through the CLI are not preserved after a reboot or power cycle unless you issue the CLI **save** command after making the changes.

Use a Simple Network Management Protocol Manager

Simple Network Management Protocol (SNMP) forms part of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems such as the NETGEAR ProSafe Network Management Software

(NMS200) to monitor network-attached devices for conditions that warrant administrative attention.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SNMP lets you monitor and manage your VPN firewall from an SNMP manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. The VPN firewall supports SNMPv1, SNMPv2c, and SNMPv3.

➢ **To configure the SNMP settings:**

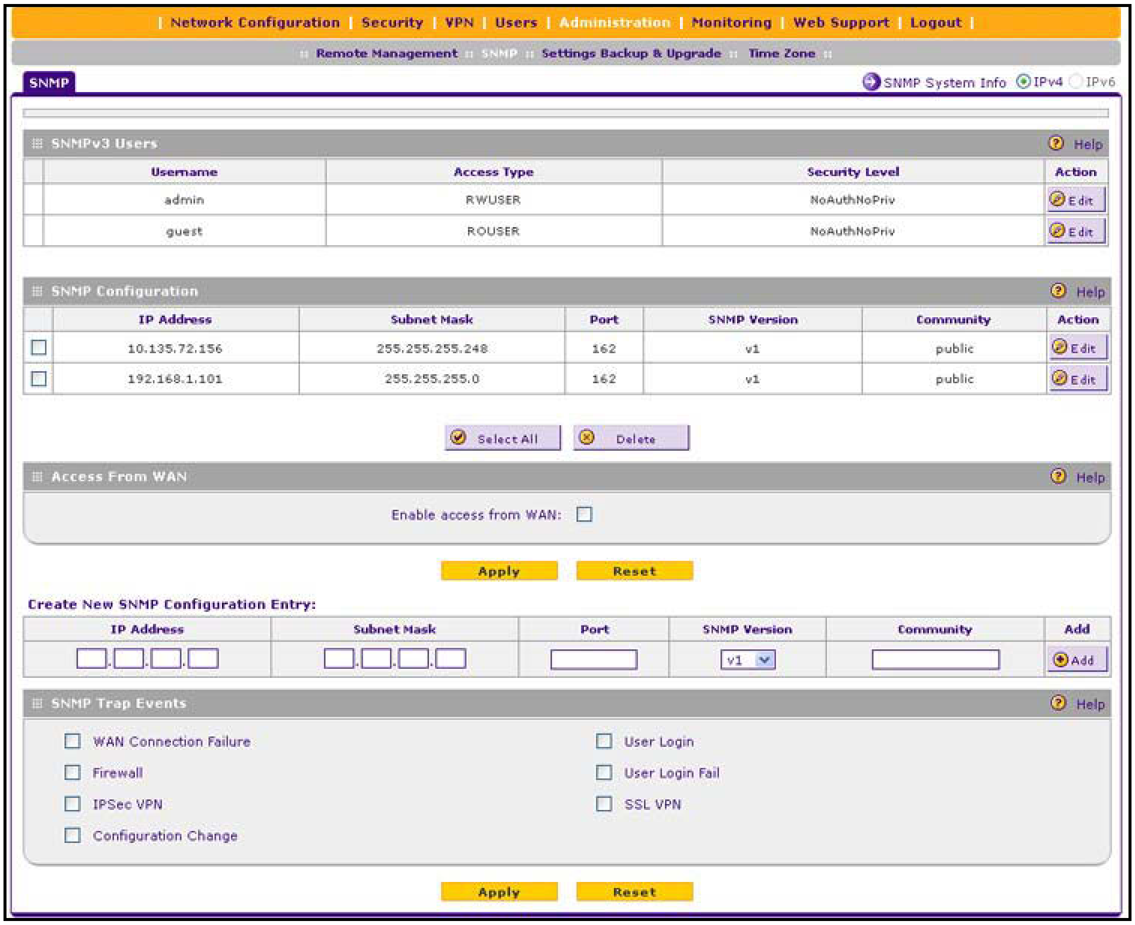
1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > SNMP**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
SNMP
SNMP System Info
● IPv4 ○ IPv6
Help

SNMPv3 Users

Username	Access Type	Security Level	Action
admin	RWUSER	NoAuthNoPriv	Edit
guest	ROUSER	NoAuthNoPriv	Edit

SNMP Configuration

	IP Address	Subnet Mask	Port	SNMP Version	Community	Action
□	10.135.72.156	255.255.255.248	162	v1	public	Edit
□	192.168.1.101	255.255.255.0	162	v1	public	Edit

Select All　Delete

Access From WAN

Enable access from WAN: □

Apply　Reset

Create New SNMP Configuration Entry:

IP Address	Subnet Mask	Port	SNMP Version	Community	Add
__.__.__.__	__.__.__.__		v1		Add

SNMP Trap Events

□ WAN Connection Failure　□ User Login
□ Firewall　□ User Login Fail
□ IPSec VPN　□ SSL VPN
□ Configuration Change

Apply　Reset

The SNMPv3 Users table includes the default SNMPv3 users that are preconfigured on the VPN firewall. The SNMPv3 Users table shows the following columns:

- **Username**. The default user names (admin or guest).
- **Access Type**. Read-write user (RWUSER) or read-only user (ROUSER). By default, the user Admin is an RWUSER and the user guest is an ROUSER.
- **Security Level**. The level of security that indicates whether security is disabled:
  - **NoAuthNoPriv**. Both authentication and privacy are disabled.
  - **AuthNoPriv**. Authentication is enabled but privacy is disabled.
  - **AuthPriv**. Both authentication and privacy are enabled.

The SNMP Configuration table shows the following columns:

- **IP Address**. The IP address of the SNMP manager.
- **Subnet Mask**. The subnet mask of the SNMP manager.
- **Port**. The trap port number of the SNMP manager.
- **SNMP Version**. The SNMP version (v1, v2c, or v3).
- **Community**. The trap community string of the SNMP manager.

3. 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 74. SNMP screen settings

Setting	Description
Access From WAN	
Enable access from WAN	To enable SNMP access by an SNMP manager through the WAN interface, select the **Enable access from WAN** check box. By default, this check box is cleared and access is disabled.
Create New SNMP Configuration Entry	
IP Address	Enter the IP address of the new SNMP manager.
Subnet Mask	Enter the subnet mask of the new SNMP manager. Note the following: • If you want to narrow down the number of devices that can access the VPN firewall through the host IP address and receive traps, enter an IP address with a subnet mask of 255.255.255.252. • If you want to allow a subnet to access the VPN firewall through the host IP address and receive traps, enter an IP address with a subnet mask of 255.0.0.0. The traps are received at the IP address, but almost the entire subnet is allowed access through the community string.
SNMP Version	From the 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 VPN firewall for the purpose of reading only.
SNMP Trap Events	
Select the check boxes to specify which SNMP trap events are sent to an SNMP manager: • **WAN Connection Failure**. Sent when the WAN connection fails. • **Firewall**. Sent when a new connection is initiated through addition of a custom firewall rule. • **IPSec VPN**. Sent when an IPSec VPN tunnel is established or disconnected. • **Configuration Change**. Sent when the configuration of the VPN firewall changes. • **User Login**. Sent when a user logs in to the VPN firewall. • **User Login Fail**. Sent when a user attempts to log in to the VPN firewall but fails to do so.	

4. Click the **Add** button to add the new SNMP configuration to the SNMP Configuration table.

➢ To edit an SNMP configuration:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

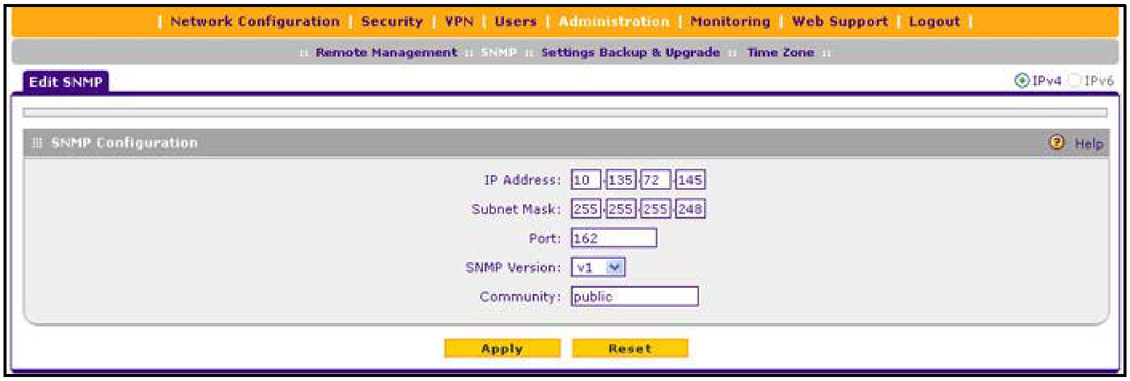
c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > SNMP**.

   The SNMP screen displays.

3. In the Action column of the SNMP Configuration table for the SNMP configuration that you want to modify, click the **Edit** button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Edit SNMP
● IPv4 ○ IPv6
SNMP Configuration
Help
Apply
Reset

IP Address: 10 . 135 . 72 . 145

Subnet Mask: 255 . 255 . 255 . 248

Port: 162

SNMP Version: v1

Community: public

4. Modify the settings as described in *Table 74* on page 334.
5. Click the **Apply** button.

   Your changes are saved.

➤ To delete one or more SNMP configurations:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > SNMP**.

   The SNMP screen displays.

3. 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.
4. Click the **Delete** table button.

   The information is deleted.

➢ To edit the SNMPv3 default users:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

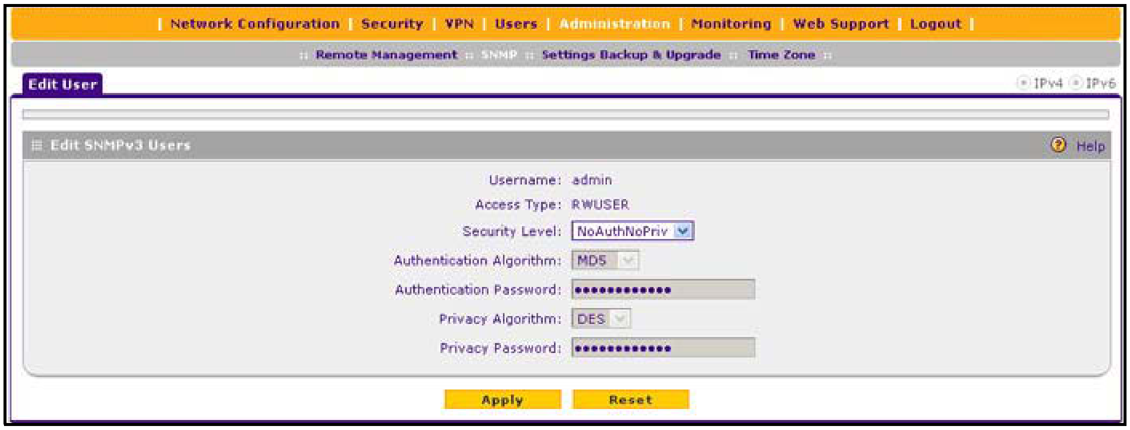
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Administration > SNMP**.

   The SNMP screen displays.
3. In the Action column of the SNMPv3 User table for the SNMPv3 default user that you want to modify, click the **Edit** button.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Edit User
IPv4 IPv6
Edit SNMPv3 Users
Help
Apply
Reset

Username: admin
Access Type: RWUSER
Security Level: NoAuthNoPriv
Authentication Algorithm: MD5
Authentication Password: ●●●●●●●●●●●●●
Privacy Algorithm: DES
Privacy Password: ●●●●●●●●●●●●●

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

Table 75. Edit User screen settings for SNMPv3 users

Setting	Description
Username	The default user name (admin or guest) for information only.
Access Type	The default access type (RWUSER or ROUSER) for information only.

Table 75. Edit User screen settings for SNMPv3 users (continued)

Setting	Description
Security Level	From the list, select the security level for communication between the SNMPv3 user and the SNMP agent that collects the MIB objects from the VPN firewall: • **NoAuthNoPriv**. Both authentication and privacy are disabled. This is the default setting. • **AuthNoPriv**. Authentication is enabled but privacy is disabled. Make a selection from the **Authentication Algorithm** list and enter an authentication password. • **AuthPriv**. Authentication and privacy are enabled. Make a selection from the **Authentication Algorithm** list and enter an authentication password. In addition, make a selection from the **Privacy Algorithm** list and enter a privacy password.
Authentication Algorithm	From the 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 must enter to be granted access to the SNMP agent that collects the MIB objects from the VPN firewall.
Privacy Algorithm	From the list, select the encryption method for the communication between an SNMPv3 user and the SNMP agent that collects the MIB objects from the VPN firewall: • **DES**. Data Encryption Standard. • **AES**. Advanced Encryption Standard.
Privacy Password	The privacy password that an SNMPv3 user must enter to allow decryption of the MIB objects that the SNMP agent collects from the VPN firewall.

5. Click the **Apply** button.

   Your changes are saved.

➢ To configure the SNMP system information:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

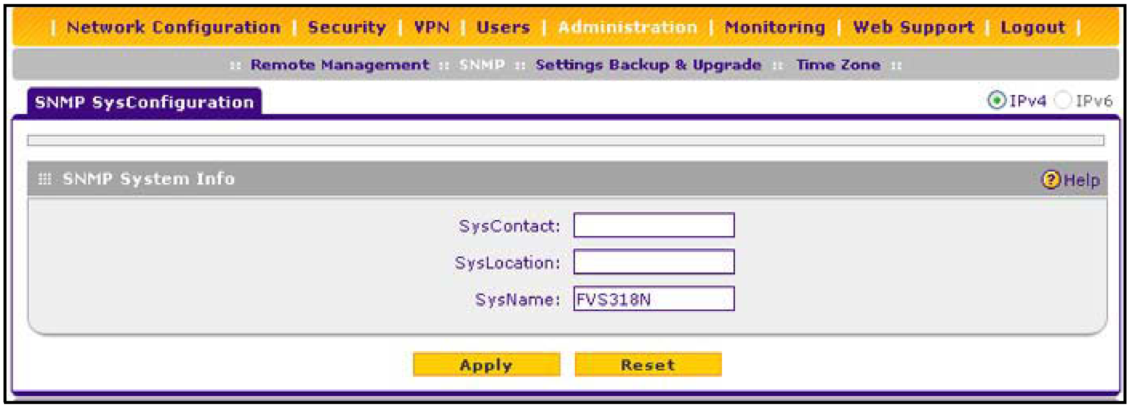
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > SNMP**.

The SNMP screen displays.

3. In the upper right of the screen, click the **SNMP System Info** option arrow.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
SNMP SysConfiguration
● IPv4 ○ IPv6
SNMP System Info
Help
Apply
Reset

SysContact:

SysLocation:

SysName: FVS318N

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

Table 76. SNMP SysConfiguration screen settings

Setting	Description
SysContact	Enter the SNMP system contact information that is available to the SNMP manager. This setting is optional.
SysLocation	Enter the physical location of the VPN firewall. This setting is optional.
SysName	Enter the name of the VPN firewall for SNMP identification purposes. The default name is FVS318N.

5. Click the **Apply** button.

Your changes are saved.

Manage the Configuration File

The configuration settings of the VPN firewall are stored in a configuration file on the VPN firewall. This file can be saved (backed up) to a computer, retrieved (restored) from the computer, cleared to factory default settings, or upgraded to a new version.

Once the VPN firewall is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the VPN firewall settings from this file.

The Backup & Restore Settings screen lets you do the following:

- Back up and save a copy of the current settings (see *Back Up Settings* on page 339)
- Restore saved settings from the backed-up file (see *Restore Settings* on page 340)
- Revert to the factory default settings (see *Revert to Factory Default Settings* on page 341)
- Update the firmware (see *Update the Firmware* on page 343)

Back Up Settings

The backup feature saves all VPN firewall settings to a file. Back up your settings periodically, and store the backup file in a safe place.

You can use a backup file to export all settings to another VPN firewall that uses the same language and management software versions. Change the IP address of the second VPN firewall before deploying it to eliminate IP address conflicts on the network.

➢ **To back up settings:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

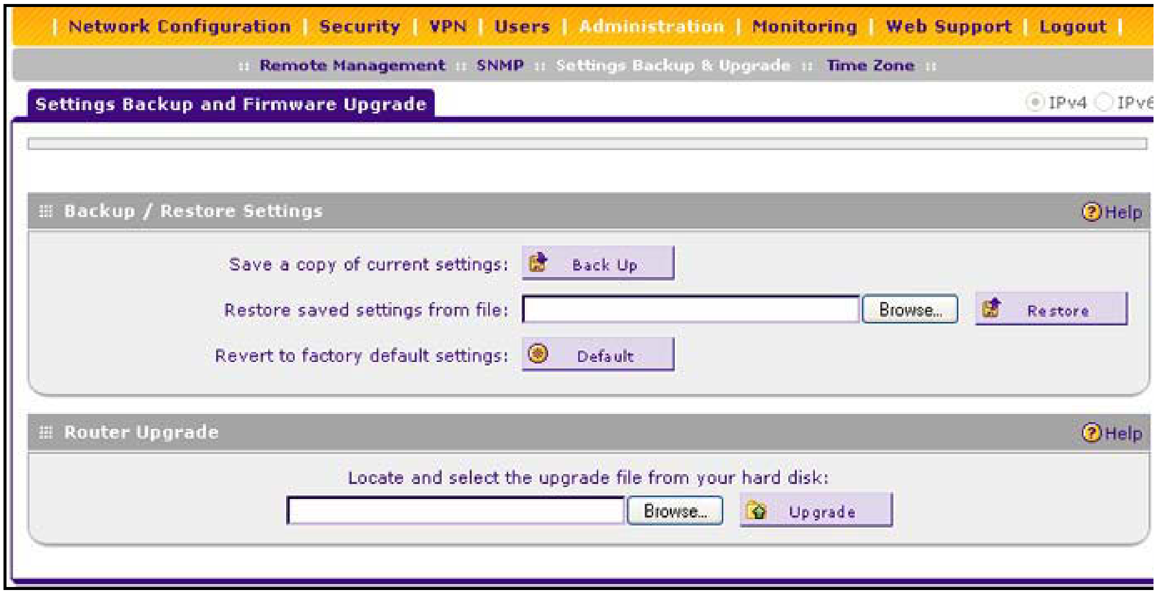
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > Settings Backup & Upgrade**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Settings Backup and Firmware Upgrade
● IPv4 ○ IPv6
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
Upgrade

3. To save a copy of your current settings, next to Save a copy of current settings, click the **Backup** button.

   A screen displays, showing the file name of the backup file (`FVS318G.cfg`).

4. Click the **Save file** button and then click the **OK** button.
5. Open the folder in which you saved the backup file, and verify that it was saved successfully.

Note the following:

- If your browser is not configured to save downloaded files automatically, locate the folder in which you want to save the file, specify the file name, and save the file.
- If your browser is configured to save downloaded files automatically, the file is saved to your browser's download location on the hard disk.

Restore Settings

⚠ WARNING:

Restore only settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the VPN firewall system software.

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

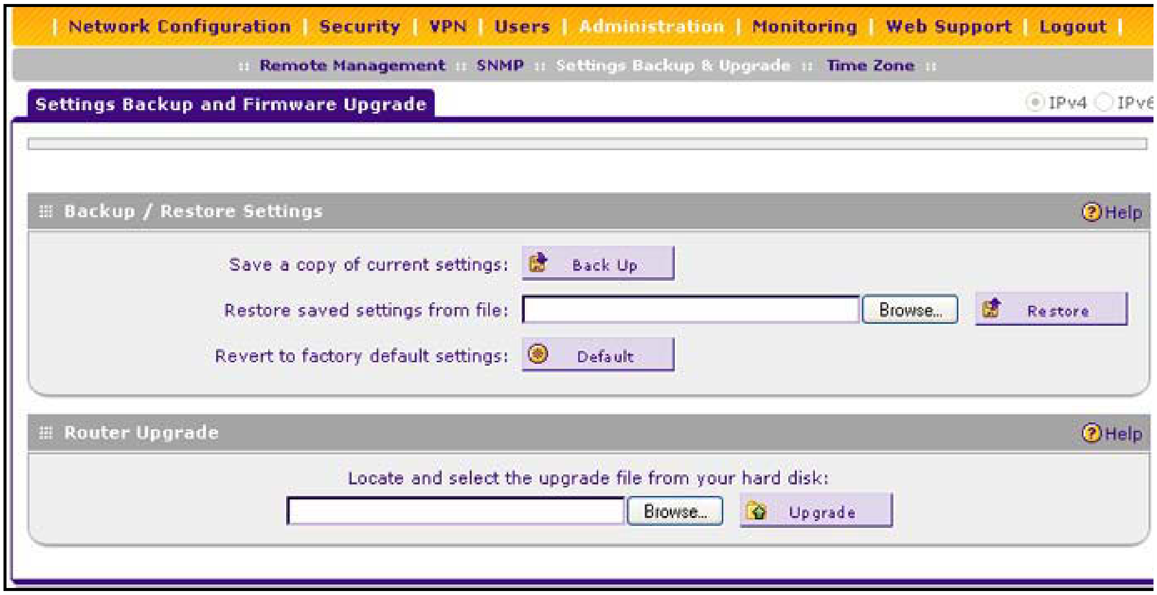
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > Settings Backup & Upgrade**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Settings Backup and Firmware Upgrade
● IPv4 ○ IPv6
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
Upgrade

3. Next to Restore saved settings from file, click the **Browse** button.
4. Locate and select the previously saved backup file (by default, `FVS318G.cfg`).
5. Click the **Restore** button.

   A warning message might display, and you must confirm that you want to restore the configuration.

WARNING:

Once you start restoring settings, do *not* interrupt the process. Do not try to go online, turn off the VPN firewall, shut down the computer, or do anything else to the VPN firewall until the settings are fully restored.

The VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 165 seconds. If you can see the unit, the reboot process is complete when the Test LED on the front panel goes off.

Revert to Factory Default Settings

You can use either of the following methods:

- **Reset button method**. For information about how to locate the **Reset** button, see *Rear Panel* on page 16.
- **Management interface method**. To use the management interface, you must know the administration password and IP address. Otherwise, you must use the factory default **Reset** button method.

⚠ **WARNING:**

When you press the hardware factory default Reset button or click the software Default button, the VPN firewall settings are erased. All firewall rules, VPN policies, LAN and WAN settings, and other settings are lost. Back up your settings if you intend to use them.

After you reboot with factory default settings, the VPN firewall's password is **password**, and the LAN IP address is **192.168.1.1**.

Reset Button Method

➤ **To reset the VPN firewall to the original factory defaults settings:**

Using a sharp object, press and hold for about eight seconds the factory default **Reset** button on the rear panel of the VPN firewall.

The Test LED lights and blinks for about 30 seconds.

The VPN firewall reboots. The reboot process takes about 165 seconds. The reboot process is complete when the Test LED on the front panel turns off.

Management Interface Method

➤ **To reset the VPN firewall to the original factory defaults settings:**

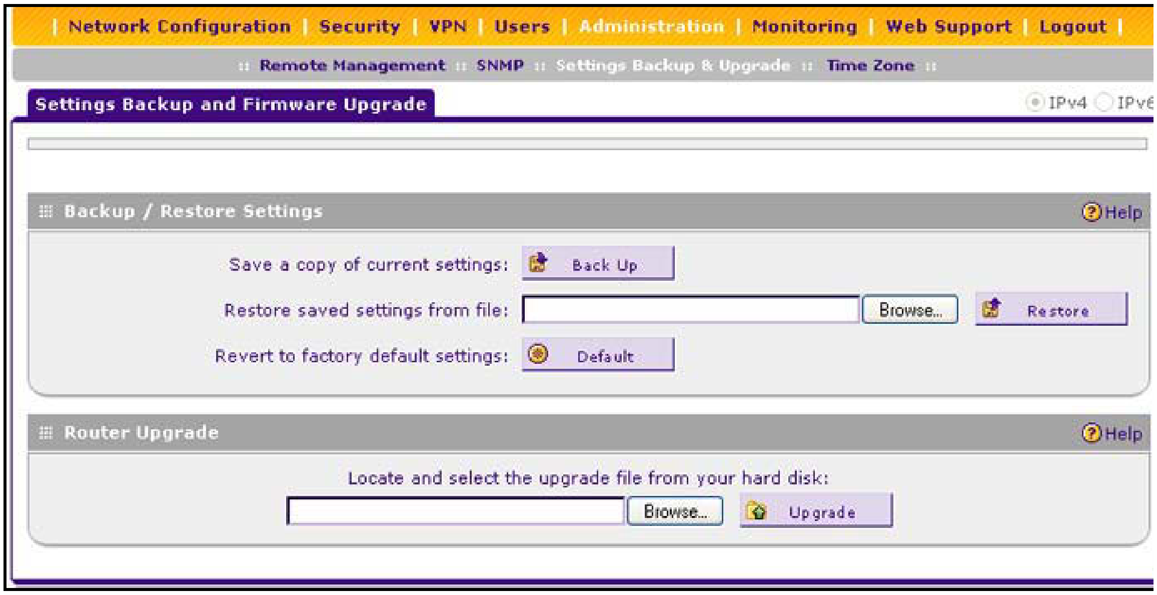
1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > Settings Backup & Upgrade**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Settings Backup and Firmware Upgrade
● IPv4 ○ IPv6
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
Upgrade

3. Next to Revert to factory defaults settings, click the **Default** button.
4. Confirm your selection.

   The VPN firewall reboots. 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. The reboot process is complete when the Test LED on the front panel turns off.

Update the Firmware

You can install a different version of the VPN firewall firmware from the Settings Backup and Firmware Upgrade screen. To view the current version of the firmware that the VPN firewall is running, log in to the unit and 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 update the firmware, the new firmware version is displayed.

In some cases, such as a major upgrade, it might be necessary to erase the configuration and manually reconfigure your VPN firewall after upgrading it. See the firmware release notes that NETGEAR makes available.

➤ **To download a firmware version and upgrade the firmware:**

1. Visit the NETGEAR website at *http://support.netgear.com*.
2. Navigate to the FVS318G v2 support page, and click the **Downloads** tab.
3. Click the desired firmware version to reach the download page.

   Be sure to read the release notes on the download page before upgrading the VPN firewall’s software.

1. Log in to the unit:

a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

The NETGEAR Configuration Manager Login screen displays.

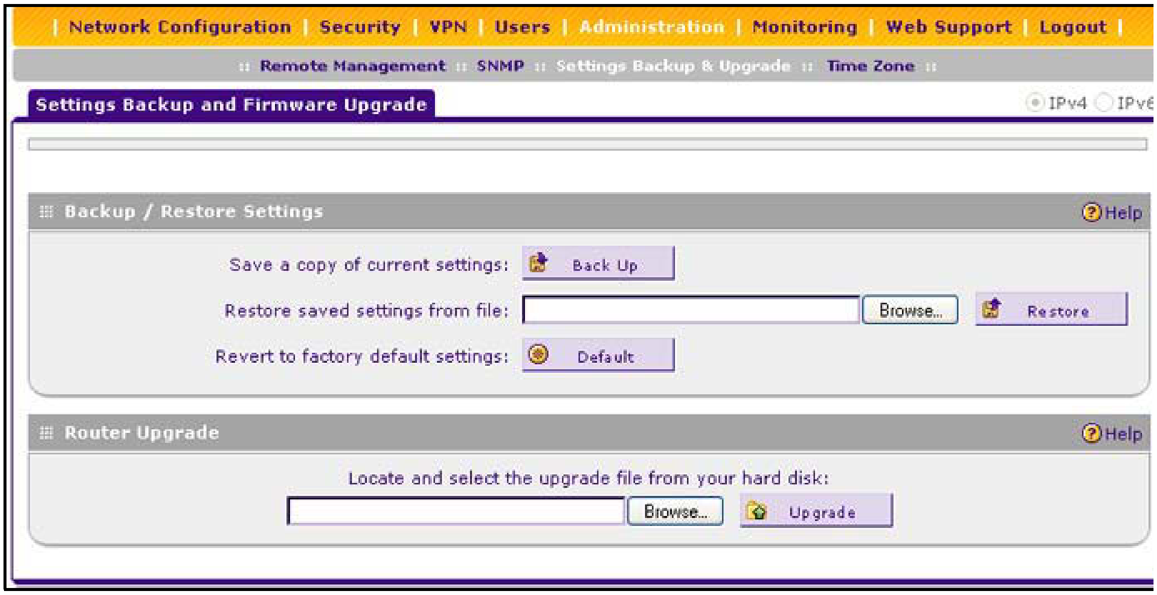
b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > Settings Backup & Upgrade**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Settings Backup and Firmware Upgrade
● IPv4 ○ IPv6
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
Upgrade

3. In the Router Upgrade section, click the **Browse** button.
4. Locate and select the downloaded firmware file.
5. Click **Upload**.

The upgrade process starts.

During the upgrade process, the Settings Backup and Firmware Upgrade screen remains visible and a status bar shows the progress of the upgrade process. The upgrade process can take up to 10 minutes. When the status bar shows that the upgrade process is complete, it can take another 10 minutes before the VPN firewall reboots.

WARNING:

After you start the firmware installation process, do *not* interrupt the process. Do not try to go online, turn off the VPN firewall, or do anything else to the VPN firewall until the VPN firewall m fully reboots.

6. When the reboot process is complete, log in to the VPN firewall again.

   The reboot process is complete when the Test LED on the front panel turns off.

7. Select **Monitoring**.

   The Router Status screen displays, showing the new firmware version in the System Info section of the screen.

Configure Date and Time Service

Configure date, time, and NTP server designations on the System Date & Time screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Setting the correct system time and time zone ensures that the date and time recorded in the VPN firewall logs and reports are accurate.

If you select the default NTP servers or if you enter a custom server FQDN, the VPN firewall determines the IP address of the NTP server by performing a DNS lookup. Before the VPN firewall can perform this lookup, you must configure a DNS server address on the Broadband ISP Settings screen. For more information, see *Manually Configure an IPv4 Internet Connection* on page 31.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

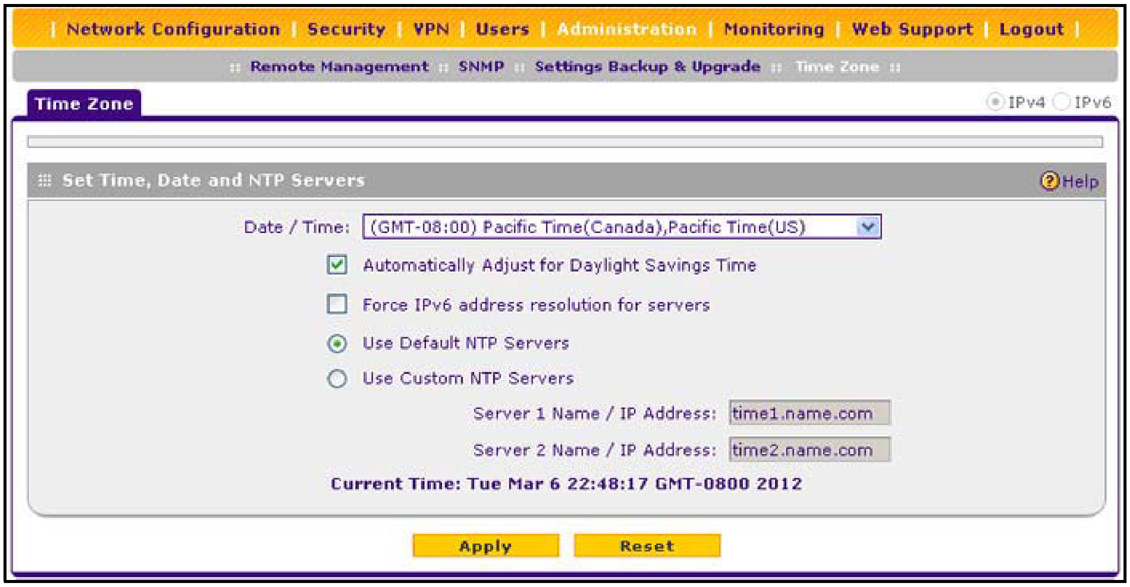
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Administration > Time Zone**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Time Zone
○ IPv4 ○ IPv6
Set Time, Date and NTP Servers
Help
Apply
Reset

Date / Time: (GMT-08:00) Pacific Time(Canada),Pacific Time(US)

☑ Automatically Adjust for Daylight Savings Time

□ Force IPv6 address resolution for servers

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: time1.name.com

Server 2 Name / IP Address: time2.name.com

Current Time: Tue Mar 6 22:48:17 GMT-0800 2012

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).

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

Table 77. Time Zone screen settings

Setting	Description
Date/Time	From the list, select the local time zone in which the VPN firewall operates. The correct time zone is required 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 cleared.
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 select the **Use Custom NTP Servers** radio button.
NTP Servers (default or custom)	Select a NTP server option: • **Use Default NTP Servers**. The VPN firewall regularly updates its RTC by contacting a default NETGEAR NTP server on the Internet. • **Use Custom NTP Servers**. The VPN firewall regularly updates its RTC by contacting one of two custom NTP servers (primary and backup), both of which you must specify in the fields that become available with this selection. **Note:** If you select the **Use Custom NTP Servers** option but leave either the **Server 1** or **Server 2** field blank, both fields are set to the default NETGEAR NTP servers. **Note:** A list of public NTP servers is available at *http://support.ntp.org/bin/view/Servers/WebHome*.

Table 77. Time Zone screen settings (continued)

Setting	Description	
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.

4. Click the **Apply** button.

   Your changes are saved.

Monitor System Access and Performance

8

This chapter describes the system-monitoring features of the VPN firewall. You can be alerted to important events such WAN traffic limits reached, login failures, and attacks. You can also view status information about the firewall, WAN ports, LAN ports, active VPN users and tunnels, and more. In addition, the diagnostics utilities are described. The chapter contains the following sections:

- *Enable the WAN Traffic Meter*
- *Configure Logging, Alerts, and Event Notifications*
- *View the Status*
- *Diagnostics Utilities*

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. For more information, see *Configure Logging, Alerts, and Event Notifications* on page 353.

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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

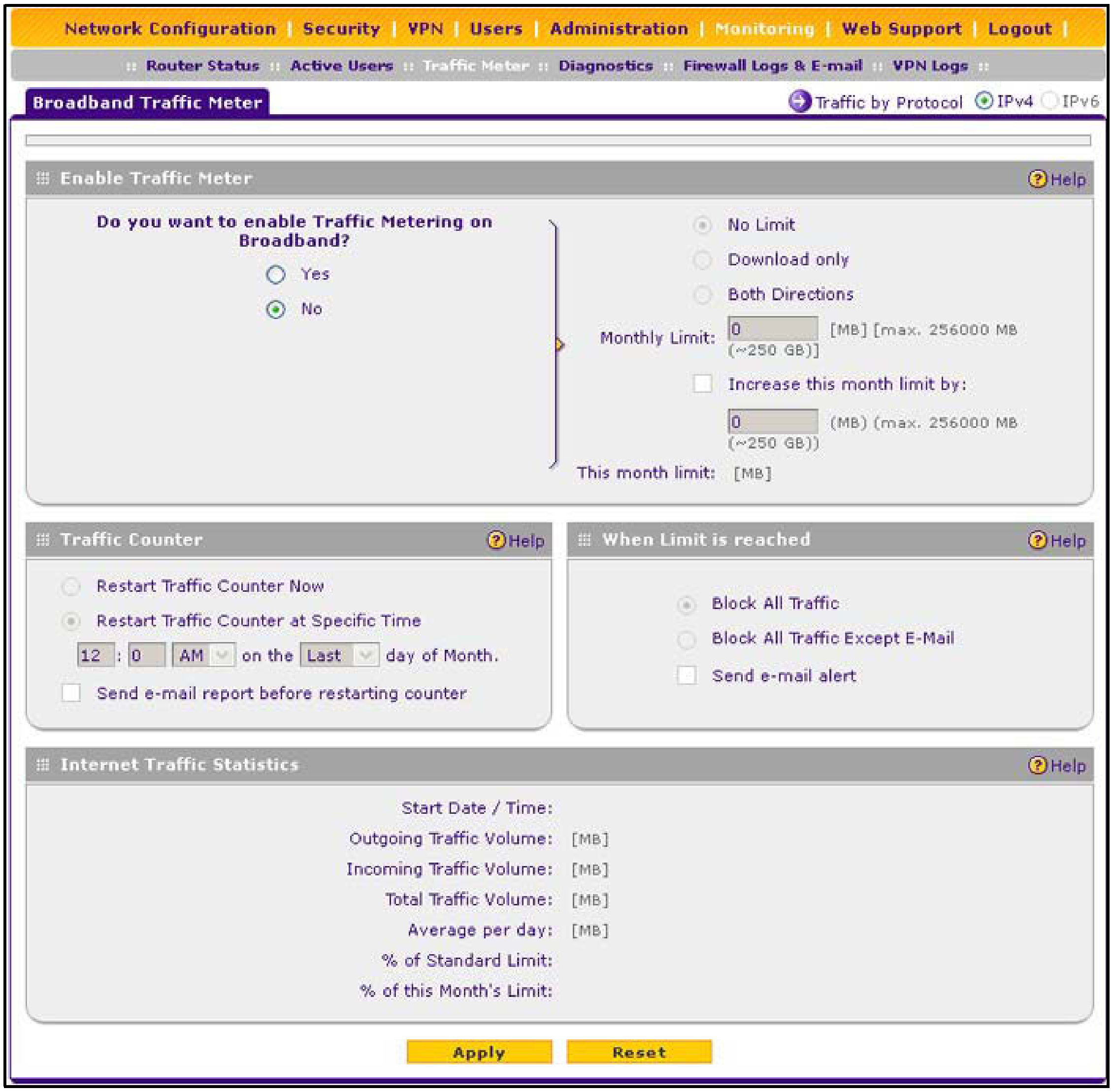
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Traffic Meter**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Broadband Traffic Meter
Traffic by Protocol
Help
Apply
Reset

● IPv4 ○ IPv6

Enable Traffic Meter

Do you want to enable Traffic Metering on Broadband?

○ Yes
● No

● No Limit
○ Download only
○ Both Directions

Monthly Limit: 0 [MB] [max. 256000 MB (~250 GB)]

□ Increase this month limit by:

0 (MB) (max. 256000 MB (~250 GB))

This month limit: [MB]

Traffic Counter

○ Restart Traffic Counter Now
● Restart Traffic Counter at Specific Time

12 : 0 AM on the Last day of Month.

□ Send e-mail report before restarting counter

When Limit is reached

● Block All Traffic
○ Block All Traffic Except E-Mail
□ Send e-mail alert

Internet Traffic Statistics

Start Date / Time:
Outgoing Traffic Volume: [MB]
Incoming Traffic Volume: [MB]
Total Traffic Volume: [MB]
Average per day: [MB]
% of Standard Limit:
% of this Month's Limit:

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

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

Table 78. Broadband Traffic Meter screen settings

Setting	Description	
Enable Traffic Meter		
Do you want to enable Traffic Metering on Broadband?	Select a traffic metering option: • **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 how the VPN firewall applies restrictions when the traffic limit is reached: • **No Limit**. No restrictions are applied when the traffic limit is reached. • **Download only**. Restrictions are applied to incoming traffic when the traffic limit is reached. Complete the **Monthly Limit** field. • **Both Directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached. Complete 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 the **Apply** button 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 when the traffic counter restarts: • **Restart Traffic Counter Now**. Select this option, and click the **Apply** button 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. Complete the time fields, and select **AM** or **PM** and the day of the month from the 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 353).	

Table 78. Broadband Traffic Meter screen settings (continued)

Setting	Description
When Limit is reached	
Block Traffic	Select which action the VPN firewall performs when the traffic limit is 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 353).

4. Click the **Apply** button.

   Your changes are saved.

➢ **To display a report of the Internet traffic by type:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

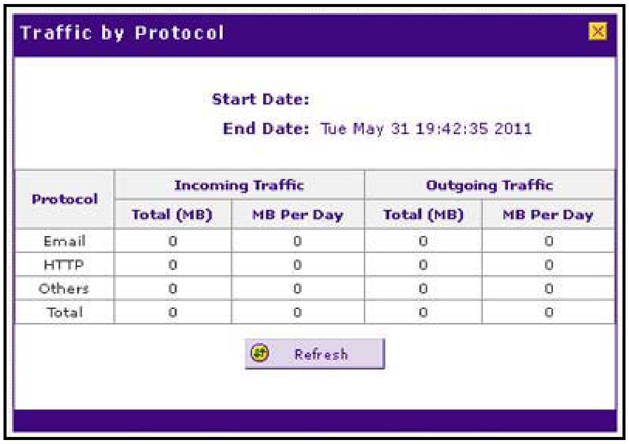
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Traffic Meter**.

   The Broadband Traffic Meter screen displays.

3. Click the **Traffic by Protocol** option arrow.



Start Date:
End Date: Tue May 31 19:42:35 2011

Protocol	Incoming Traffic		Outgoing Traffic	
	Total (MB)	MB Per Day	Total (MB)	MB Per Day
Email	0	0	0	0
HTTP	0	0	0	0
Others	0	0	0	0
Total	0	0	0	0

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.

Configure Logging, Alerts, and Event Notifications

You can configure the VPN firewall to log routing events such as dropped and accepted packets, to log system events such as a change of time by an NTP server, secure login attempts, and reboots, and to log other events. You can also schedule logs to be sent to the administrator and enable logs to be sent to a syslog server on the network.

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.

Note: This release does not support sending the NTP and DNS logs to the syslog server or the mail server.

➤ **To configure and activate logs:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

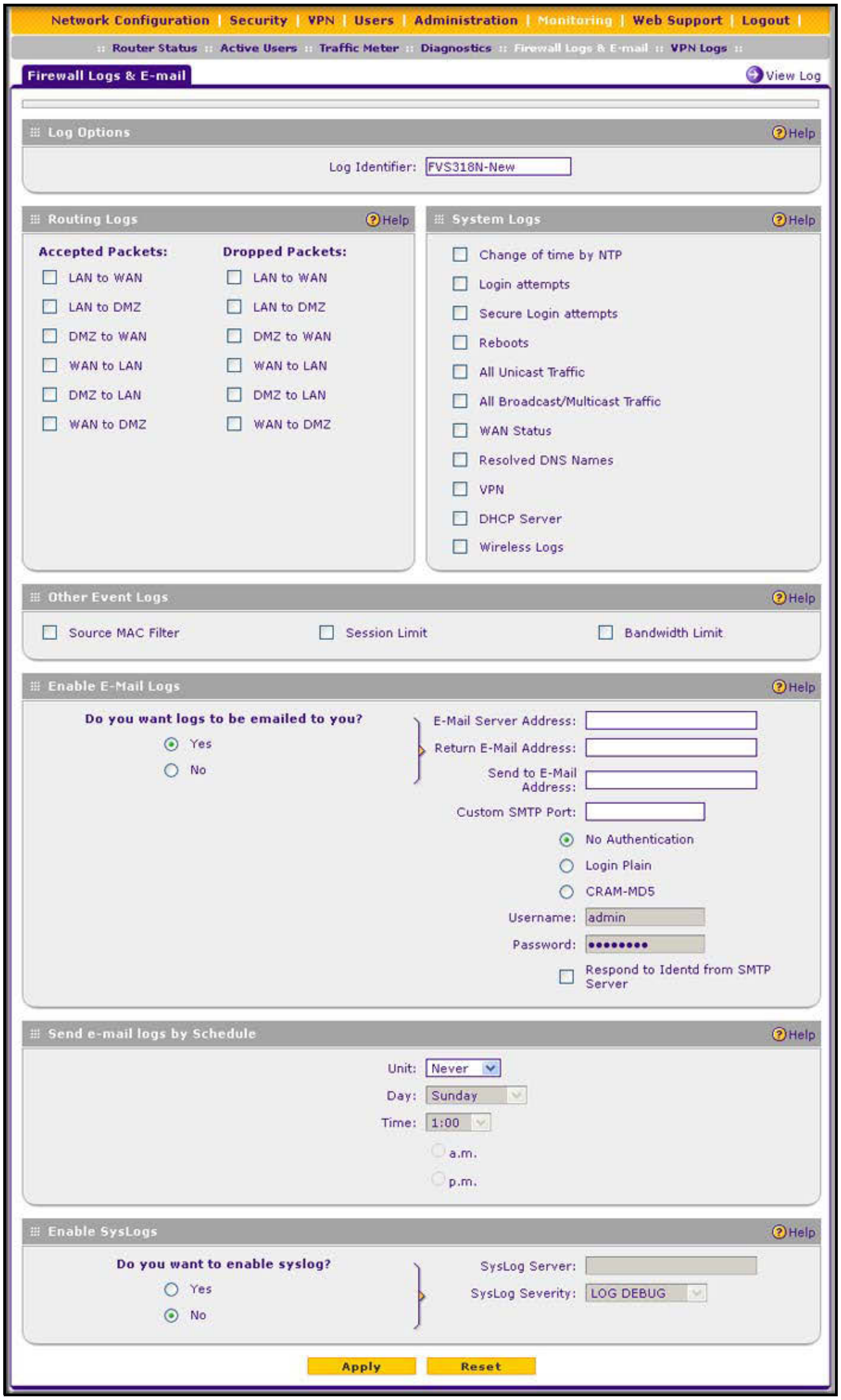
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Firewall Logs & E-mail**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Firewall Logs & E-mail
View Log
Help
Apply
Reset

Log Options

Log Identifier: FVS318N-New

Routing Logs

Accepted Packets:	Dropped Packets:
□ LAN to WAN	□ LAN to WAN
□ LAN to DMZ	□ LAN to DMZ
□ DMZ to WAN	□ DMZ to WAN
□ WAN to LAN	□ WAN to LAN
□ DMZ to LAN	□ DMZ to LAN
□ WAN to DMZ	□ WAN to DMZ

System Logs

- □ Change of time by NTP
- □ Login attempts
- □ Secure Login attempts
- □ Reboots
- □ All Unicast Traffic
- □ All Broadcast/Multicast Traffic
- □ WAN Status
- □ Resolved DNS Names
- □ VPN
- □ DHCP Server
- □ Wireless Logs

Other Event Logs

□ Source MAC Filter □ Session Limit □ Bandwidth Limit

Enable E-Mail Logs

Do you want logs to be emailed to you?

● Yes
○ No

E-Mail Server Address:
Return E-Mail Address:
Send to E-Mail Address:
Custom SMTP Port:
● No Authentication
○ Login Plain
○ CRAM-MD5
Username: admin
Password: ••••••••
□ Respond to Identd from SMTP Server

Send e-mail logs by Schedule

Unit: Never
Day: Sunday
Time: 1:00
○ a.m.
○ p.m.

Enable SysLogs

Do you want to enable syslog?

○ Yes
● No

SysLog Server:
SysLog Severity: LOG DEBUG

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

Table 79. 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.	
System Logs Option	
Select which system events are logged: • **Change of Time by NTP**. Logs a message when the system time changes after a request from an NTP server. • **Login Attempts**. Logs a message when a login is attempted. Both successful and failed login attempts are logged. • **Secure Login Attempts**. Logs a message when a secure login is attempted. Both successful and failed secure login attempts are logged. • **Reboots**. Logs a message when the VPN firewall is rebooted through the web management interface. (No message is logged when the factory default **Reset** button is 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.	
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 was exceeded.
Bandwidth Limit	Select this check box to log packets that are dropped because the bandwidth limit was exceeded.

Table 79. Firewall Logs & E-mail screen settings (continued)

Setting	Description	
Enable E-mail Logs		
Do you want logs to be emailed to you?	Select the **Yes** radio button to enable the VPN firewall to email logs to a specified email address. Complete the fields that are shown on the right side of the screen. Select the **No** radio button to prevent the logs from being emailed, which is the default setting.	
	E-Mail Server Address	The IP address or Internet name of your ISP's outgoing email SMTP server. **Note:** If you leave this field blank, the VPN firewall cannot send email logs and alerts.
	Return E-Mail Address	The email address of the sender for email identification purposes. For example, enter 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 the SMTP server authentication for 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** 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** list, select the day on which the logs are sent.	
Time	From the **Time** list select the hour on which the logs are sent, and select either the **a.m.** or **p.m.** radio button.	

Table 79. Firewall Logs & E-mail screen settings (continued)

Setting	Description	
Enable SysLogs		
Do you want to enable syslog?	To enable the VPN firewall to send logs to a specified syslog server, select the **Yes** radio button. Complete the fields that are shown on the right side of the screen. To prevent the logs from being sent, select the **No** radio button, which is the default setting.	
	SysLog Server	The IP address or FQDN of the syslog server.
	SysLog Severity	All the logs with a severity that is equal to and above the severity that you specify are logged on the specified syslog server. For example, if you select LOG_CRITICAL as the severity, the logs with the severities LOG_CRITICAL, LOG_ALERT, and LOG_EMERG are logged. Select the syslog severity from the list: • **LOG DEBUG**. Debug-level messages. • **LOG INFO**. Informational messages. • **LOG NOTICE**. Normal but significant conditions exist. • **LOG WARNING**. Warning conditions exist. • **LOG ERROR**. Error conditions exist. • **LOG CRITICAL**. Critical conditions exist. • **LOG ALERT**. An action must be taken immediately. • **LOG EMERG**. The VPN firewall is unusable.

4. Click the **Apply** button.

   Your changes are saved.

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 sends 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

Type of Address	Gateway 1 at Site 1	Gateway 2 at Site 2
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*
- *Configure Gateway 2 at Site 2*

Configure Gateway 1 at Site 1

➢ **To create a gateway-to-gateway VPN tunnel to Gateway 2, using the IPSec VPN wizard:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays.

3. 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

4. Click the **Apply** button.

   Your changes are saved.

➢ **To change the remote IP address in the VPN policy:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policy screen displays.

3. Next to the policy name for the Gateway 1–to–Gateway 2 autopolicy, click the **Edit** button.

   The Edit VPN Policy screen displays.

4. In the General section of the screen, clear the **Enable NetBIOS** check box.
5. In the Traffic Selector section of the screen, make the following changes:
   - From the **Remote IP** list, select **Single**.
   - In the **Start IP** fields, type **10.0.0.2**, which is the WAN IP address of Gateway 2.
6. Click the **Apply** button.

   Your changes are saved.

Configure Gateway 2 at Site 2

➤ **To create a gateway-to-gateway VPN tunnel to Gateway 1, using the IPSec VPN wizard:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays.

3. 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

4. Click the **Apply** button.

   Your changes are saved.

➢ To change the local IP address in the VPN policy:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policy screen displays.
3. Next to the policy name for the Gateway 2–to–Gateway 1 autopolicy, click the **Edit** button.

   The Edit VPN Policy screen displays.
4. In the General section, clear the **Enable NetBIOS** check box.
5. In the Traffic Selector section, make the following changes:
   - From the **Local IP** list, select **Single**.
   - In the **Start IP** fields, type **10.0.0.2**, which is the WAN IP address of Gateway 2.
6. Click the **Apply** button.

   Your changes are saved.

➢ To specify the syslog server that is connected to Gateway 1:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Firewall Logs & E-mail**.

The Firewall Logs & E-mail screen displays.

3. Enable the syslog server and enter **192.168.10.2** as the IP address. at Site 1
4. Click the **Apply** button.

Your changes are saved.

The VPN tunnel is established automatically, and the syslogs are sent to the syslog server at Site 1. You can use the IPSec VPN Connection Status screen to verify the connection.

View the Status

This section contains the following topics:

- *View the System Status*
- *View the VPN Connection Status and L2TP Users*
- *View the VPN Logs*
- *View the Port Triggering Status*
- *View the WAN Port Status*
- *View the Attached Devices and the DHCP Log*

View the System Status

When you start the VPN firewall, the default screen that displays is the Router Status screen.

The Router Status screen and Detailed Status screen provide real-time information about the following important components of the VPN firewall:

- Firmware version
- Both IPv4 and IPv6 WAN and LAN port information
- Interface statistics
- VLAN status, including port memberships

The Tunnel Status screen provides real-time information about the IPv6 tunnels.

These status screens are described in the following sections:

- *Router Status*
- *Router Statistics*
- *Detailed Status*
- *VLAN Status*

- *Tunnel Status*

Router Status

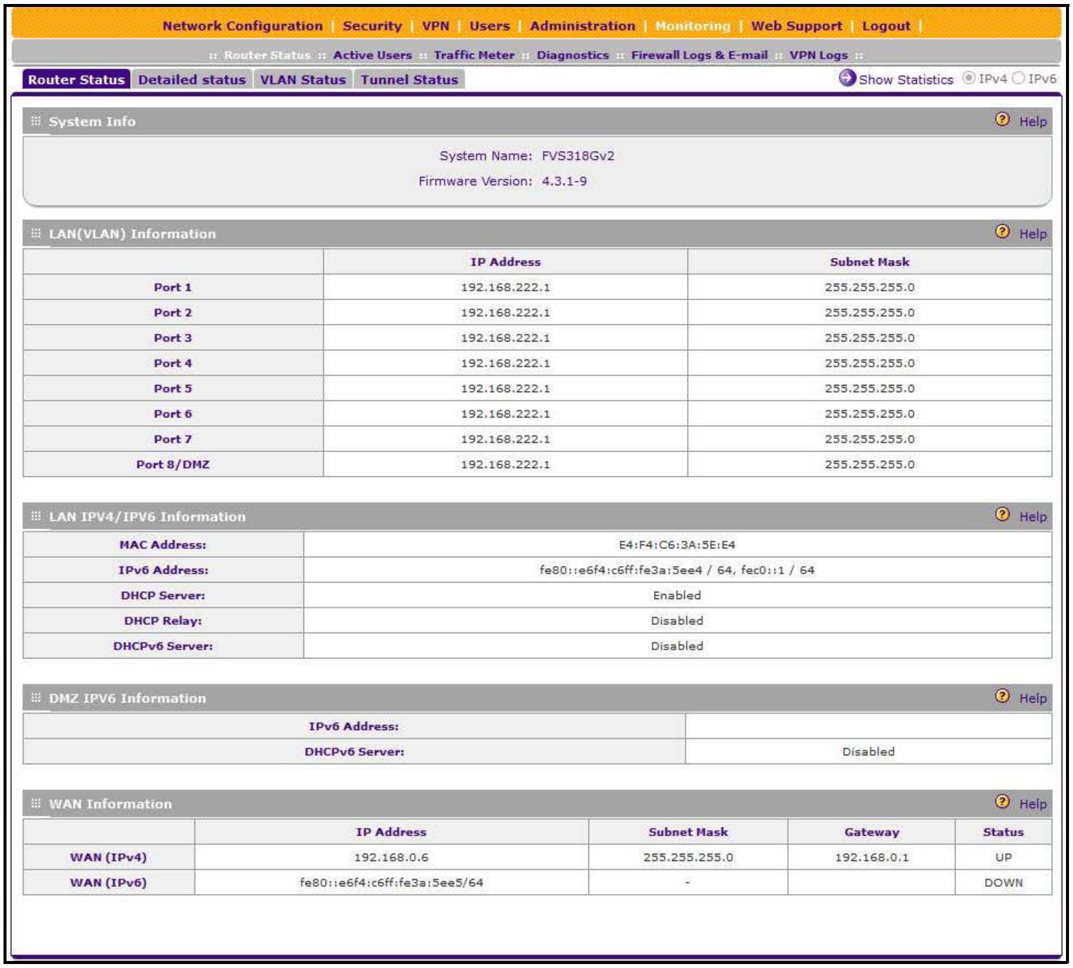
➢ To view the Router Status:

1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Monitoring > Router Status**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
VLAN Status
Tunnel Status
Show Statistics
● IPv4 ○ IPv6
Help

System Info

System Name: FVS318Gv2

Firmware Version: 4.3.1-9

LAN(VLAN) Information

	IP Address	Subnet Mask
Port 1	192.168.222.1	255.255.255.0
Port 2	192.168.222.1	255.255.255.0
Port 3	192.168.222.1	255.255.255.0
Port 4	192.168.222.1	255.255.255.0
Port 5	192.168.222.1	255.255.255.0
Port 6	192.168.222.1	255.255.255.0
Port 7	192.168.222.1	255.255.255.0
Port 8/DMZ	192.168.222.1	255.255.255.0

LAN IPV4/IPV6 Information

MAC Address:	E4:F4:C6:3A:5E:E4
IPv6 Address:	fe80::e6f4:c6ff:fe3a:5ee4 / 64, fec0::1 / 64
DHCP Server:	Enabled
DHCP Relay:	Disabled
DHCPv6 Server:	Disabled

DMZ IPV6 Information

IPv6 Address:	
DHCPv6 Server:	Disabled

WAN Information

	IP Address	Subnet Mask	Gateway	Status
WAN (IPv4)	192.168.0.6	255.255.255.0	192.168.0.1	UP
WAN (IPv6)	fe80::e6f4:c6ff:fe3a:5ee5/64	-		DOWN

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

Table 80. 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 82* on page 367.	
LAN IPv4/IPv6 Information	
MAC Address	The MAC address of the VPN firewall.
IPv6 Address	The IPv6 address that is assigned to the VPN firewall. For information about configuring the IPv6 address, see *Configure the IPv6 Internet Connection and WAN Settings* on page 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 61.
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 61.
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 78.
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 96.
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 96.
WAN Information	
WAN (IPv4)	The IPv4 address, subnet mask, gateway, and status of the port (UP or Down). For more detailed information, see *Table 82* on page 367.
WAN (IPv6)	The IPv6 address, gateway, and status of the port (UP or Down). For more detailed information, see *Table 82* on page 367.

Router Statistics

➢ To view the Router Statistics:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

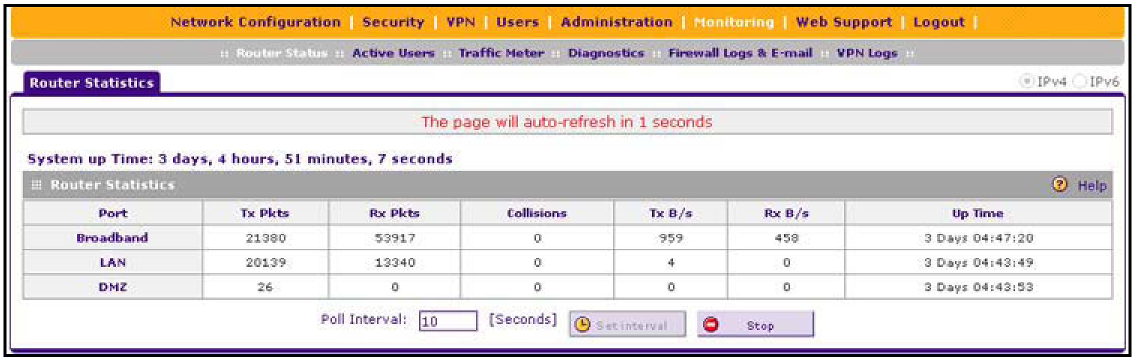
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Router Status**.

   The Router Status screen displays.

3. Click the **Show Statistics** option arrow.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Statistics
○ IPv4 ○ IPv6

The page will auto-refresh in 1 seconds

System up Time: 3 days, 4 hours, 51 minutes, 7 seconds

Router Statistics

Port	Tx Pkts	Rx Pkts	Collisions	Tx B/s	Rx B/s	Up Time
Broadband	21380	53917	0	959	458	3 Days 04:47:20
LAN	20139	13340	0	4	0	3 Days 04:43:49
DMZ	26	0	0	0	0	3 Days 04:43:53

Poll Interval: 10 [Seconds]

The following table explains the fields of the Router Statistics screen.

Table 81. Router Statistics screen information

Item	Description
System up Time. The period since the last time that the VPN firewall was started.	
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.

Table 81. Router Statistics screen information (continued)

Item	Description
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 is active since it was restarted.

To change the poll interval period, enter a new value (in seconds) in the **Poll Interval** field, and click the **Set interval** button.

To stop polling, click the **Stop** button.

Detailed Status

➤ **To view the status details:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

   The NETGEAR Configuration Manager Login screen displays.

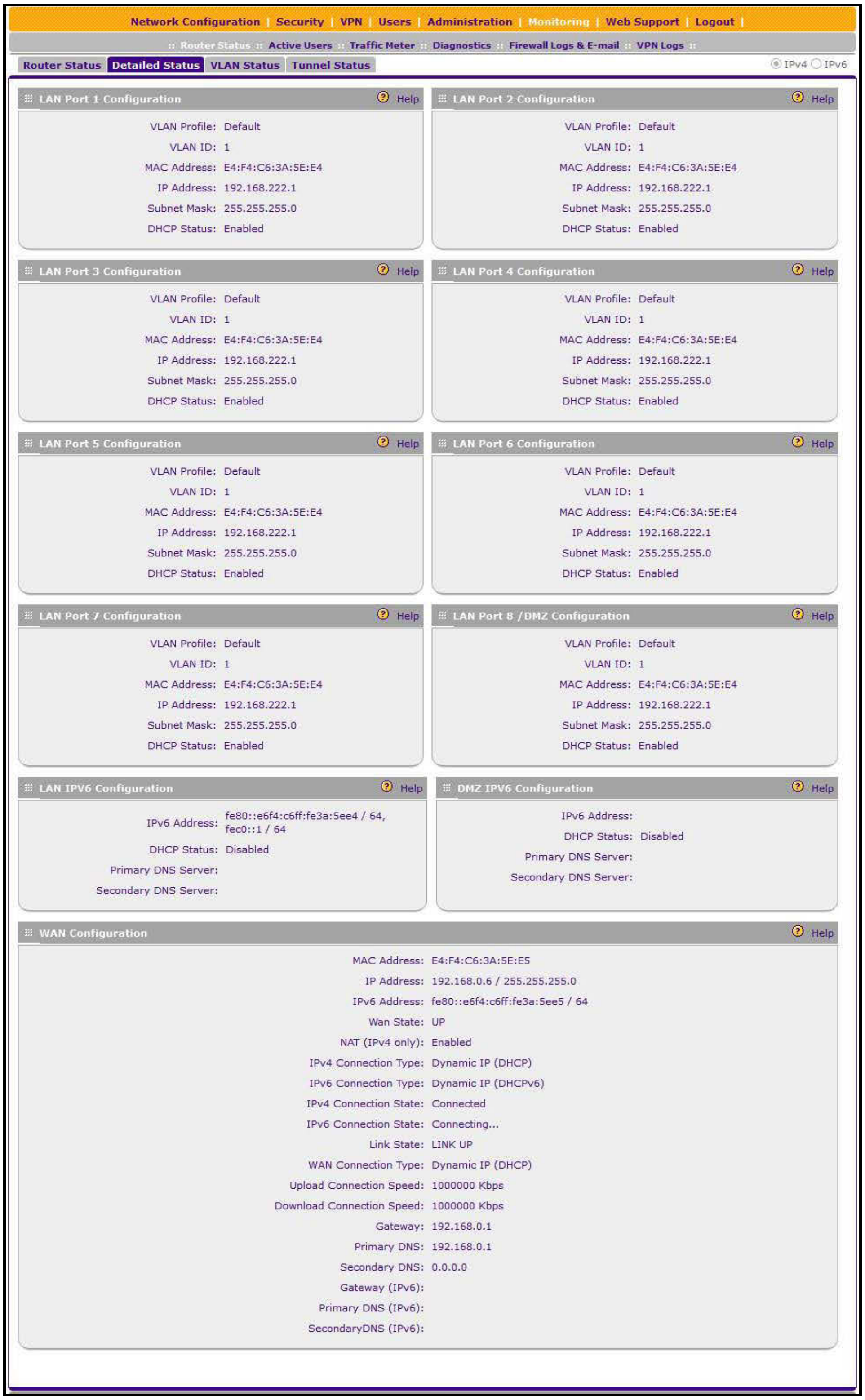
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

   Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

   The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Router Status > Detailed Status**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed Status
VLAN Status
Tunnel Status
● IPv4 ○ IPv6
Help

LAN Port 1 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: E4:F4:C6:3A:5E:E4
IP Address: 192.168.222.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 2 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: E4:F4:C6:3A:5E:E4
IP Address: 192.168.222.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 3 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: E4:F4:C6:3A:5E:E4
IP Address: 192.168.222.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 4 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: E4:F4:C6:3A:5E:E4
IP Address: 192.168.222.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 5 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: E4:F4:C6:3A:5E:E4
IP Address: 192.168.222.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 6 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: E4:F4:C6:3A:5E:E4
IP Address: 192.168.222.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 7 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: E4:F4:C6:3A:5E:E4
IP Address: 192.168.222.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 8 /DMZ Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: E4:F4:C6:3A:5E:E4
IP Address: 192.168.222.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN IPV6 Configuration

IPv6 Address: fe80::e6f4:c6ff:fe3a:5ee4 / 64,
fec0::1 / 64
DHCP Status: Disabled
Primary DNS Server:
Secondary DNS Server:

DMZ IPV6 Configuration

IPv6 Address:
DHCP Status: Disabled
Primary DNS Server:
Secondary DNS Server:

WAN Configuration

MAC Address: E4:F4:C6:3A:5E:E5
IP Address: 192.168.0.6 / 255.255.255.0
IPv6 Address: fe80::e6f4:c6ff:fe3a:5ee5 / 64
Wan State: UP
NAT (IPv4 only): Enabled
IPv4 Connection Type: Dynamic IP (DHCP)
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Connected
IPv6 Connection State: Connecting...
Link State: LINK UP
WAN Connection Type: Dynamic IP (DHCP)
Upload Connection Speed: 1000000 Kbps
Download Connection Speed: 1000000 Kbps
Gateway: 192.168.0.1
Primary DNS: 192.168.0.1
Secondary DNS: 0.0.0.0
Gateway (IPv6):
Primary DNS (IPv6):
SecondaryDNS (IPv6):

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

Table 82. 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 61). 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 specified that each VLAN must be assigned a unique MAC address (see *Configure VLAN MAC Addresses and LAN Advanced Settings* on page 68). • LAN ports that use 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 was assigned 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 96.
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 61.
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 61.
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 61.
WAN Configuration	
MAC Address	The default MAC address for the port or the MAC address that you 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 52.
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 26.

Table 82. Detailed Status screen information (continued)

Item	Description	
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.	
NAT (IPv4 only)	The NAT state can be either Enabled or Disabled, depending on whether NAT is enabled (see *Network Address Translation* on page 27) or classical routing is enabled (see *Classical Routing* on page 27).	
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 26.	
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 26.	
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 *NETGEAR ProSAFE VPN Firewall FVS318G v2 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 31).
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.	

VLAN Status

You can display the current settings of the router's configured VLAN ports.

➢ **To view the status of the configured VLAN ports:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

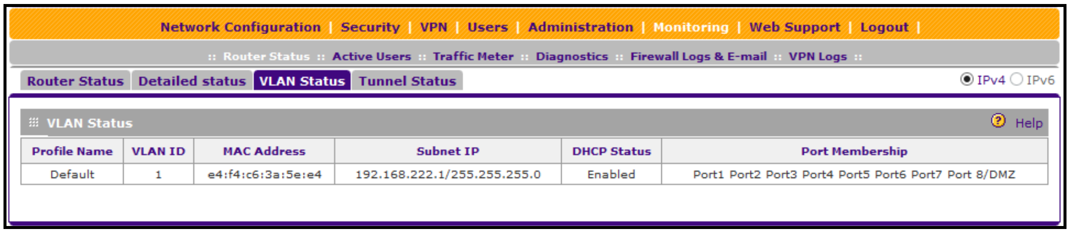
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Router Status > VLAN Status**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
VLAN Status
Tunnel Status
● IPv4 ○ IPv6
VLAN Status
Help

Profile Name	VLAN ID	MAC Address	Subnet IP	DHCP Status	Port Membership
Default	1	e4:f4:c6:3a:5e:e4	192.168.222.1/255.255.255.0	Enabled	Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port 8/DMZ

The VLAN Status table contains a list of configured VLANs, both enabled and disabled. The VLAN Status table shows the following fields:

- **Profile Name**. The unique identifier assigned to this VLAN profile.
- **VLAN ID**. The VLAN tag associated with this profile, between 2 and 4089. 1 is the default VLAN ID.
- **MAC Address**. Configured VLAN's can be assigned the same MAC address as the associated LAN port or they can be assigned unique MAC addresses.
- **Subnet IP**. Displays the unique IP address and subnet mask of the configured VLAN profile.
- **DHCP Status**. Each VLAN supports a DHCP server to assign IP addresses to DHCP clients on this network.
- **Port Membership**. Displays the ports 1 through 8 that are members of this VLAN profile.

Tunnel Status

You can display the status of all active 6to4 and ISATAP tunnels and their IPv6 addresses.

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

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

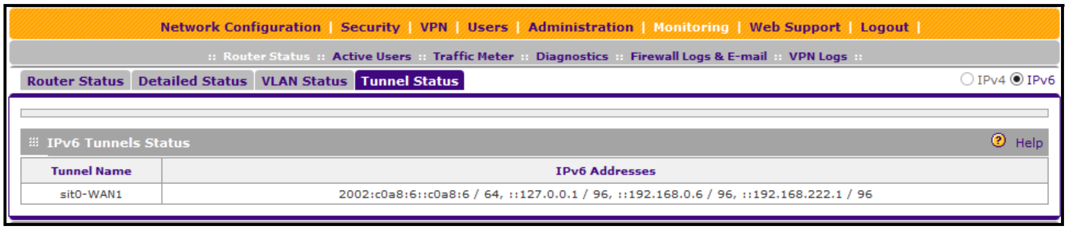
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Router Status > Tunnel Status**.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed Status
VLAN Status
Tunnel Status
○ IPv4 ● IPv6
Help

IPv6 Tunnels Status

Tunnel Name	IPv6 Addresses
sit0-WAN1	2002:c0a8:6::c0a8:6 / 64, ::127.0.0.1 / 96, ::192.168.0.6 / 96, ::192.168.222.1 / 96

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 and L2TP users who are logged in to the VPN firewall.

➢ To view the active IPSec VPN connections:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

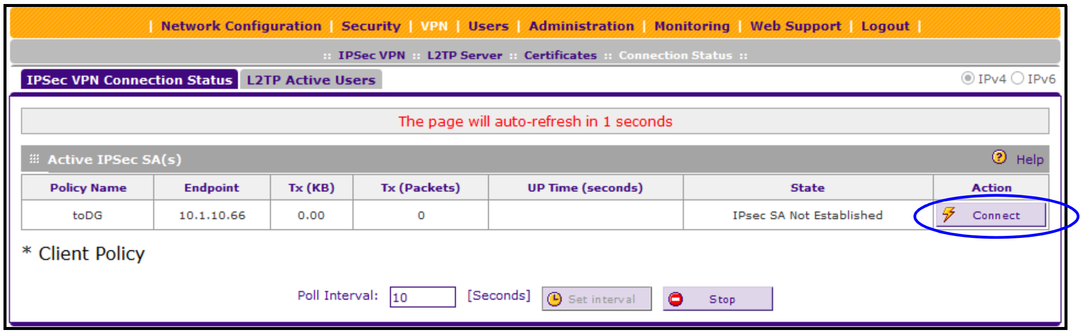
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Connection Status**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
L2TP Active Users
● IPv4 ○ IPv6
Help
Connect
Set interval
Stop

The page will auto-refresh in 1 seconds

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	UP Time (seconds)	State	Action
toDG	10.1.10.66	0.00	0		IPsec SA Not Established	Connect

* Client Policy

Poll Interval: 10 [Seconds]

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.

3. To activate a tunnel, to the right of the policy's table entry, click the **Connect** table button.
4. To disconnect an active connection, to the right of the policy's table entry, click the **Disconnect** table button.

➢ To view the active L2TP tunnel users:

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

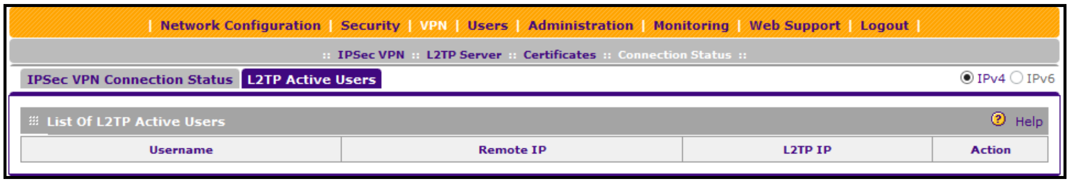
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **VPN > Connection Status > L2TP Active Users**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
L2TP Active Users
● IPv4 ○ IPv6
Help

List Of L2TP Active Users

Username	Remote IP	L2TP IP	Action

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

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

View the VPN Logs

➢ To display the IPSec VPN log:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

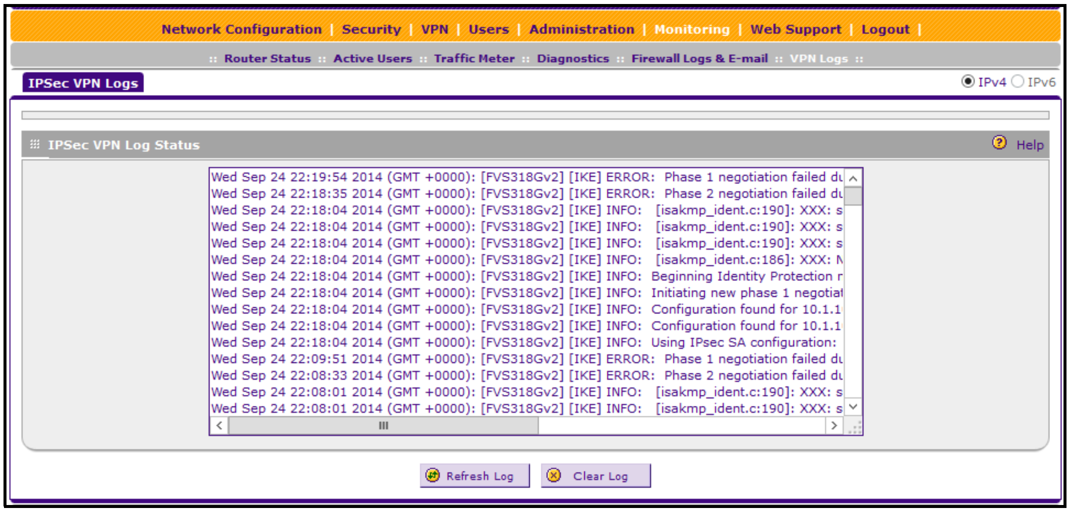
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > VPN Logs**.


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
● IPv4 ○ IPv6
IPSec VPN Log Status
Help
Refresh Log
Clear Log

```
Wed Sep 24 22:19:54 2014 (GMT +0000): [FVS318Gv2] [IKE] ERROR:  Phase 1 negotiation failed du
Wed Sep 24 22:18:35 2014 (GMT +0000): [FVS318Gv2] [IKE] ERROR:  Phase 2 negotiation failed du
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:186]: XXX: N
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Beginning Identity Protection r
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Initiating new phase 1 negotiat
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Configuration found for 10.1.1
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Configuration found for 10.1.1
Wed Sep 24 22:18:04 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:  Using IPsec SA configuration:
Wed Sep 24 22:09:51 2014 (GMT +0000): [FVS318Gv2] [IKE] ERROR:  Phase 1 negotiation failed du
Wed Sep 24 22:08:33 2014 (GMT +0000): [FVS318Gv2] [IKE] ERROR:  Phase 2 negotiation failed du
Wed Sep 24 22:08:01 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
Wed Sep 24 22:08:01 2014 (GMT +0000): [FVS318Gv2] [IKE] INFO:   [isakmp_ident.c:190]: XXX: s
```

View the Port Triggering Status

➢ To view the status of the port triggering feature:

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

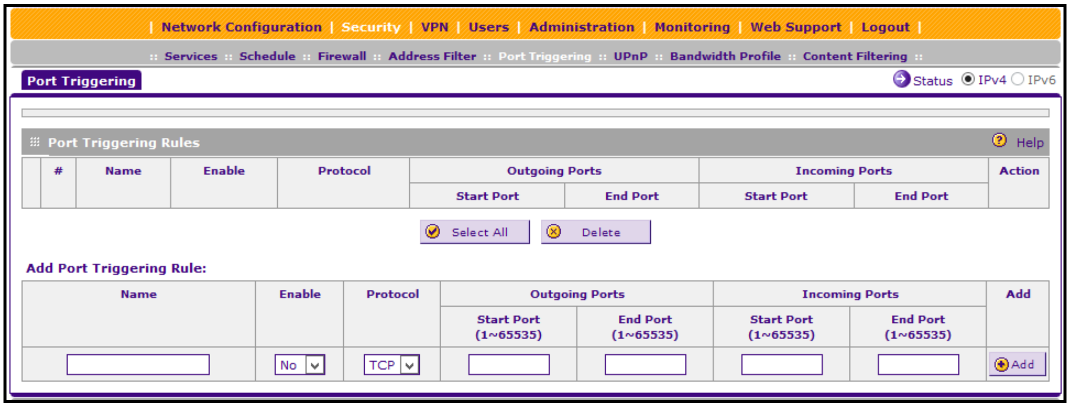
   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

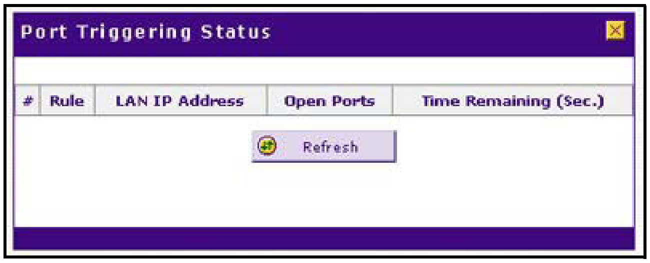
c. Click the **Login** button.

The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Security > Port Triggering**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Port Triggering
Status ● IPv4 ○ IPv6
Port Triggering Rules
Help
# Name Enable Protocol Outgoing Ports Incoming Ports Action
Start Port End Port Start Port End Port
Select All
Delete
Add Port Triggering Rule:
Name Enable Protocol Outgoing Ports Incoming Ports Add
Start Port (1~65535) End Port (1~65535) Start Port (1~65535) End Port (1~65535)
No
TCP
Add

3. In the upper right of the screen, click the **Status** option arrow.



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

Table 83. 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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

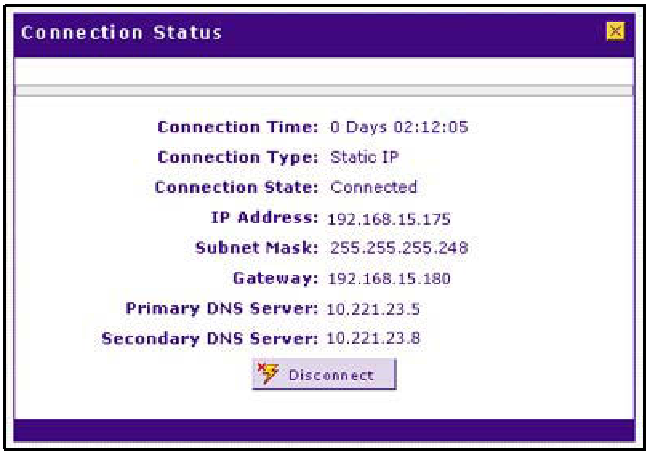
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv4)**.

   The Broadband ISP Settings (IPv4) screen displays.

3. In the upper right of the screen, click the **Broadband Status** option arrow.



Connection Time: 0 Days 02:12:05
Connection Type: Static IP
Connection State: Connected
IP Address: 192.168.15.175
Subnet Mask: 255.255.255.248
Gateway: 192.168.15.180
Primary DNS Server: 10.221.23.5
Secondary DNS Server: 10.221.23.8

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 84. Connection Status screen information for an IPv4 connection

Item	Description
Connection Time	The period that the VPN firewall is 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.

Table 84. Connection Status screen information for an IPv4 connection (continued)

Item	Description
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 VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 28 and *Manually Configure an IPv4 Internet Connection* on page 31.
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 configured these ISP settings on the Broadband ISP Settings screen. **Note:** For more information, see *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 28 and *Manually Configure an IPv4 Internet Connection* on page 31.
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.

To establish the connection, click the **Connect** button.

To disconnect the connection, click the **Disconnect** button.

IPv6 WAN Port Status

➢ **To view the IPv6 status of the WAN port:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

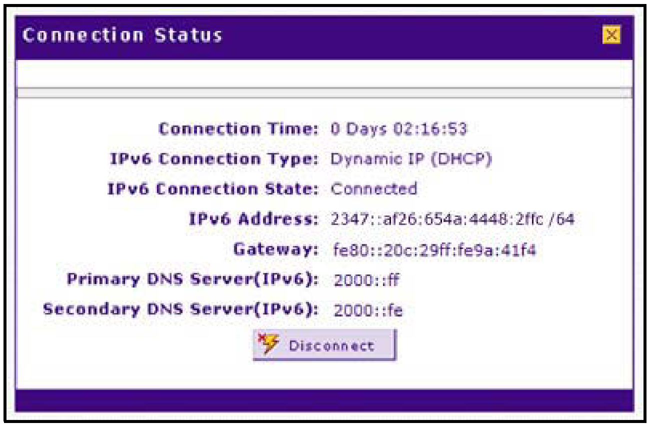
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv6)**.

   The Broadband ISP Settings (IPv6) screen displays.

3. In the upper right of the screen, click the **Status** option arrow.



Connection Time: 0 Days 02:16:53
IPv6 Connection Type: Dynamic IP (DHCP)
IPv6 Connection State: Connected
IPv6 Address: 2347::af26:654a:4448:2ffc /64
Gateway: fe80::20c:29ff:fe9a:41f4
Primary DNS Server(IPv6): 2000::ff
Secondary DNS Server(IPv6): 2000::fe

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 85. Connection Status screen information for an IPv6 connection

Item	Description
Connection Time	The period that the VPN firewall is 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)	

To establish the connection, click the **Connect** button.

To disconnect the connection, click the **Disconnect** button.

View the Attached Devices and the DHCP Log

The LAN Groups screen shows the network database, which is the Known PCs and Devices table, which contains all IP devices that VPN firewall discovered on the local network. The LAN Setup screen lets you access the DHCP log.

View the Attached Devices

The Known PCs and Devices table contains a list of all known computers and network devices that are assigned dynamic IP addresses by the VPN firewall, were 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 73.

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

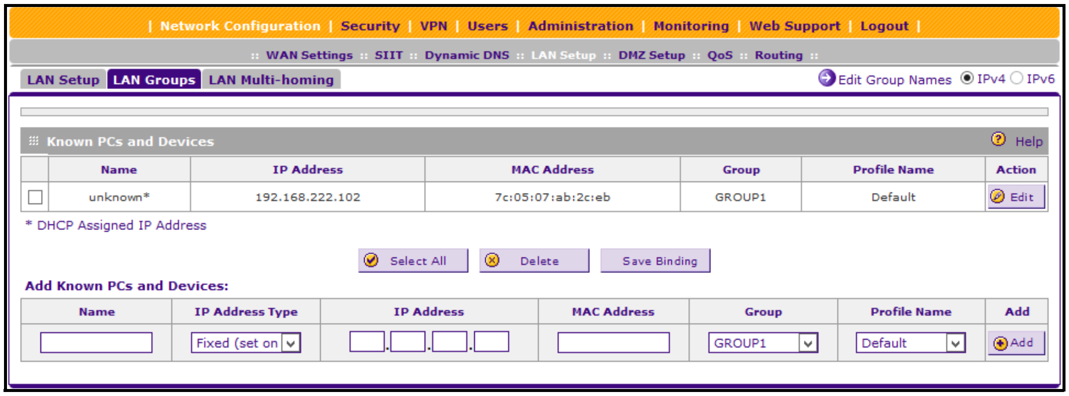
➢ To view the attached devices on the LAN Groups screen:

1. Log in to the unit:
   - **a.** In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.
   - **b.** In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).
   - **c.** Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.
2. Select **Network Configuration > LAN Setup > LAN Groups**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
Edit Group Names
● IPv4 ○ IPv6
Help
Select All
Delete
Save Binding

Known PCs and Devices

	Name	IP Address	MAC Address	Group	Profile Name	Action
□	unknown*	192.168.222.102	7c:05:07:ab:2c:eb	GROUP1	Default	Edit

* DHCP Assigned IP Address

Add Known PCs and Devices:

Name	IP Address Type	IP Address	MAC Address	Group	Profile Name	Add
	Fixed (set on	. . .		GROUP1	Default	Add

For each attached computer or device, the Known PCs and Devices table displays the following fields:

- **Check box**. Allows you to select the computer or device in the table.
- **Name**. The name of the computer or device. For computers that do not support the NetBIOS protocol, the name is displayed as *Unknown* (you can edit the entry manually to add a meaningful name). If the computer or device was assigned an IP address by the DHCP server, the name is appended by an asterisk.
- **IP Address**. The current IP address of the computer or device. For DHCP clients of the VPN firewall, this IP address does not change. If a computer or device is assigned a static IP address, you must update this entry manually after the IP address on the computer or device changes.
- **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** 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.

View the DHCP Log

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

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

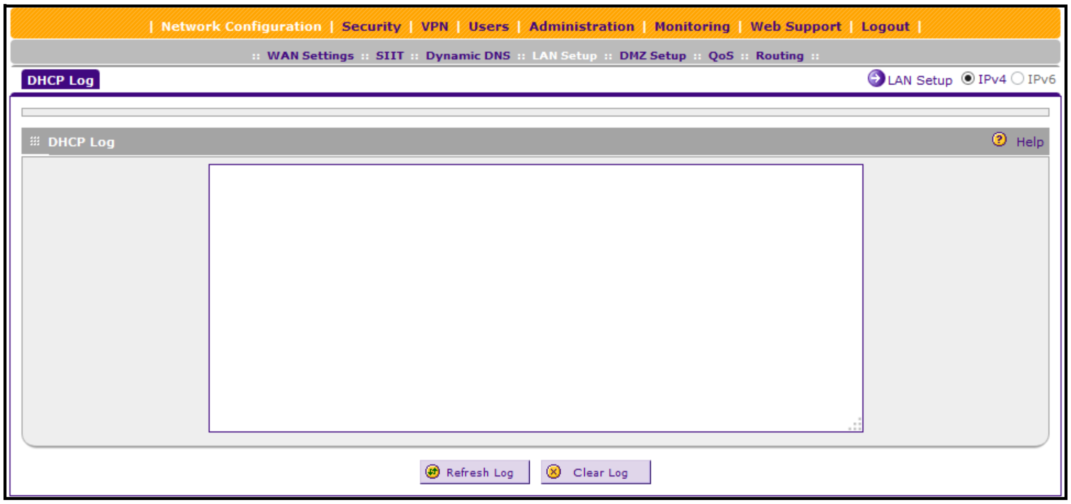
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > LAN Setup**.

   The LAN Setup screen displays the IPv4 settings.

3. Click the **DHCP Log** option arrow to the right of the LAN Setup tab.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Dynamic DNS :: LAN Setup :: DMZ Setup :: QoS :: Routing ::
DHCP Log
LAN Setup
◉ IPv4 ○ IPv6
DHCP Log
Help
Refresh Log
Clear Log

   To view the most recent entries, click the **Refresh Log** button.

   To delete all the existing log entries, click the **Clear Log** button.

4. To modify the DHCP settings, click the **LAN Setup** option arrow.

The LAN Setup screen displays. For more information, see *Configure a VLAN Profile* on page 61.

Diagnostics Utilities

The VPN firewall provides diagnostic tools that help you analyze the status of the network and traffic conditions. Two types of tools are available:

- **Network diagnostic tools**. These tools include a ping utility, traceroute utility, and DNS lookup utility, and the option to display the routing tables.
- **Packet capture tool**. This tool lets you capture packets per interface in real time for a short period and download the packet information.

For normal operation, diagnostic tools are not required.

➤ **To display the Diagnostics screen:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

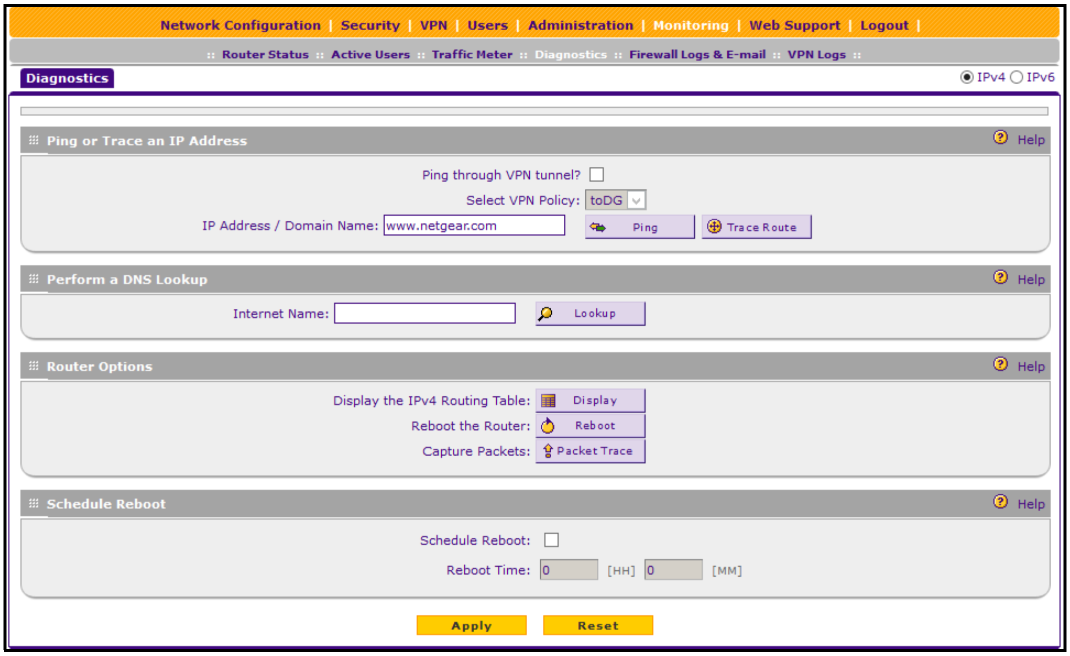
      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.

3. Specify the IP version for the screen that you want.

- **IPv4**. In the upper right of the screen, the **IPv4** radio button is already selected by default.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Diagnostics
Help
Ping
Trace Route
Lookup
Display
Reboot
Packet Trace
Apply
Reset

● IPv4 ○ IPv6

Ping or Trace an IP Address

Ping through VPN tunnel? □

Select VPN Policy: toDG

IP Address / Domain Name: www.netgear.com

Perform a DNS Lookup

Internet Name:

Router Options

Display the IPv4 Routing Table:

Reboot the Router:

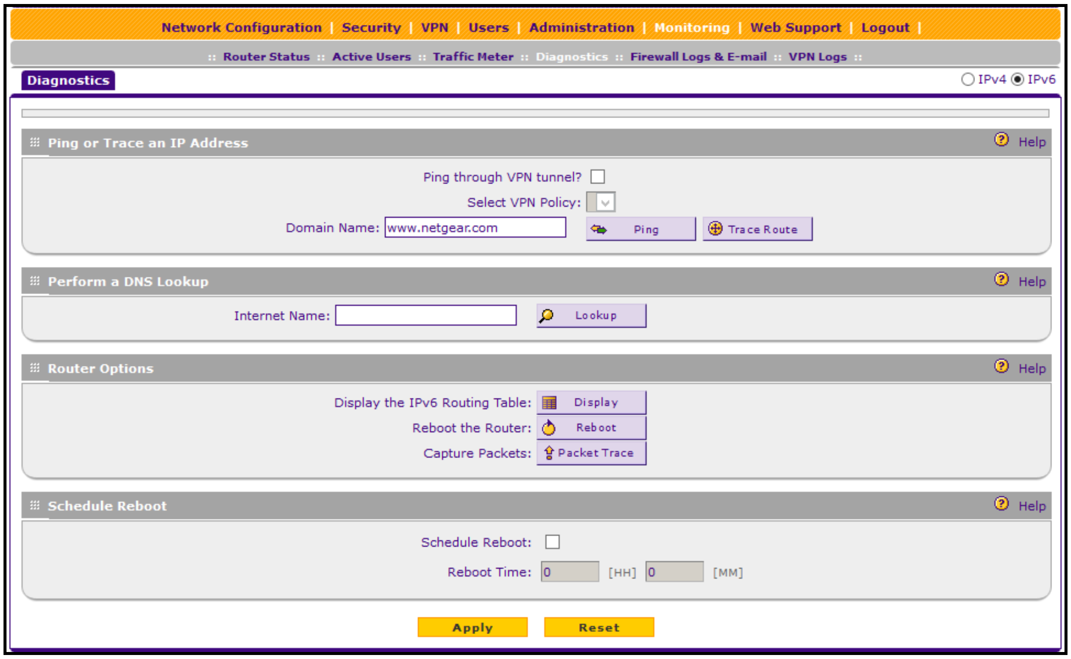
Capture Packets:

Schedule Reboot

Schedule Reboot: □

Reboot Time: 0 [HH] 0 [MM]

- **IPv6**. Select the **IPv6** radio button.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Diagnostics
Help
Ping
Trace Route
Lookup
Display
Reboot
Packet Trace
Apply
Reset

○ IPv4 ● IPv6

Ping or Trace an IP Address

Ping through VPN tunnel? □

Select VPN Policy:

Domain Name: www.netgear.com

Perform a DNS Lookup

Internet Name:

Router Options

Display the IPv6 Routing Table:

Reboot the Router:

Capture Packets:

Schedule Reboot

Schedule Reboot: □

Reboot Time: 0 [HH] 0 [MM]

The various tasks that you can perform on the Diagnostics screen are described in the following sections:

- *Send a Ping Packet*
- *Trace a Route*
- *Look Up a DNS Address*

- *Display the Routing Tables*
- *Capture Packets in Real Time*
- *Reboot the VPN Firewall Remotely*

Send a Ping Packet

Use the ping utility to send a ping packet request to check the connection between the VPN firewall and a specific IP address or FQDN. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results are displayed on a new screen.

➢ **To send a ping:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.

3. Specify the IP version for the screen that you want:
   - 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.
   - For IPv6, in the **Domain Name** field, enter the domain name that you want to ping.

     You cannot enter an IP address.

4. If the specified address is reached through a VPN tunnel, select the **Ping through VPN tunnel?** check box and then select a VPN policy from the **Select VPN Policy** list.
5. Click the **Ping** button.

   The results of the ping are displayed in a new screen.

To return to the Diagnostics screen, on the browser menu bar, click the **Back** button.

Trace a Route

A traceroute lists all routers between the source (the VPN firewall) and the destination IP address.

➢ **To send a traceroute:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.

3. Specify the IP version for the screen that you want:

   - 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.
   - For IPv6, in the **Domain Name** field, enter the domain name that you want to trace.

     You cannot enter an IP address.

4. If the specified address is reached through a VPN tunnel, select the **Ping through VPN tunnel?** check box and then select a VPN policy from the **Select VPN Policy** list.

5. Click the **Trace Route** button.

   The results of the traceroute are displayed in a new screen.

To return to the Diagnostics screen, on the browser menu bar, click the **Back** button.

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. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.

3. Specify the IP version for the screen that you want.
   - In the **Internet Name** field, enter a domain name.
   - Click the **Lookup** button.

   The results of the lookup action are displayed in a new screen.

To return to the Diagnostics screen, on the browser menu bar, click the **Back** button.

Display the Routing Tables

Displaying the internal routing table can assist NETGEAR technical support in diagnosing routing problems.

➢ **To display the routing table:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.

3. Specify the IP version for the screen that you want:
   - For IPv4, in the Router Options section of the screen, next to Display the IPv4 Routing Table, click the **Display** button.

     The routing table is shown in the Route Display pop-up screen.

   - For IPv6, in the Router Options section of the screen, next to Display the IPv6 Routing Table, click the **Display** button.

     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. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

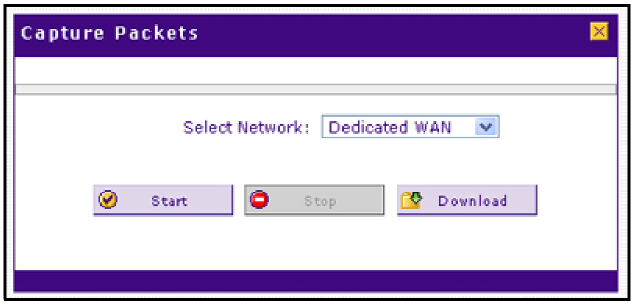
   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.

3. Specify the IP version for the screen that you want.
4. In Router Options section, next to Capture Packets, click the **Packet Trace** button.



Capture Packets

Select Network: Dedicated WAN

5. From the **Select Network** list, select the physical or virtual interface for which you want to capture packets.
6. Click the **Start** button.

   After a few seconds, the packet-tracing process starts, which is indicated by a message onscreen.

7. When you want to stop the packet-tracing process, click the **Stop** button.

   After a few seconds, the packet-tracing process stops, which is indicated by a message onscreen.

8. Click the **Download** button.
9. 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.

10. When the download is complete, browse to the download location you specified, and verify that the file was downloaded successfully.
11. (Optional) Send the file to NETGEAR technical support for analysis.

Reboot the VPN Firewall Remotely

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

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

➢ **To reboot the VPN firewall:**

1. Log in to the unit:
   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.

3. Specify the IP version for the screen that you want.
4. In Router Options section of the screen, next to Reboot the Router, click the **Reboot** button.

   The VPN firewall reboots. The Diagnostics screen might remain visible during the reboot process, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 165 seconds.

Troubleshooting

9

This chapter provides troubleshooting tips and information for the VPN firewall. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the VPN firewall on?

  Go to *Basic Functioning* on page 387.

- Did I connect the VPN firewall correctly?

  Go to *Basic Functioning* on page 387.

- I cannot access the VPN firewall's web management interface.

  Go to *Troubleshoot the Web Management Interface* on page 388.

- A time-out occurs.

  Go to *When You Enter a URL or IP Address, a Time-Out Error Occurs* on page 389.

- I cannot access the Internet or the LAN.

  Go to *Troubleshoot the ISP Connection* on page 389.

- I am experiencing problems with the IPv6 connection.

  Go to *Troubleshooting the IPv6 Connection* on page 391

- I am experiencing problems with the LAN connection.

  Go to *Troubleshoot a TCP/IP Network Using a Ping Utility* on page 395.

- I want to clear the configuration and start over again.

  Go to *Restore the Default Configuration and Password* on page 397.

- The date or time is not correct.

  Go to *Address Problems with Date and Time* on page 398.

- I need more information.

  Go to *Access the Knowledge Base and Documentation* on page 398.

The VPN firewall's diagnostic tools are described in *Diagnostics Utilities* on page 379.

Basic Functioning

After you turn on power to the VPN firewall, you can verify that the correct sequence of events occurs.

➢ **To verify the power-on sequence of events:**

1. When power is first applied, verify that the Power LED is on.
2. After approximately two minutes, verify the following:
   - **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 was 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*
- *Test LED Never Turns Off*
- *LAN or WAN Port LEDs Not On*

Power LED Not On

If the Power and other LEDs are off when your VPN firewall is turned on, make sure that the power cord is correctly connected to your VPN firewall and that the power supply adapter is correctly connected to a functioning power outlet.

If the error persists, a hardware problem occurred. Contact NETGEAR technical support.

Test LED Never Turns Off

When the VPN firewall is powered on, the Test LED turns on for approximately two minutes and then turns off when the VPN firewall completes its initialization. If the Test LED remains on, a fault occurred within the VPN firewall.

If all LEDs are still on more than several minutes minute after power-up, do the following:

- Turn off the power, and turn it on again to see if the VPN firewall recovers.
- Reset the VPN firewall’s configuration to factory default settings.

  Doing so sets the VPN firewall’s IP address to **192.168.1.1**. This procedure is described in *Restore the Default Configuration and Password* on page 397.

If the error persists, it is possible that a hardware problem occurred. Contact NETGEAR technical support.

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the VPN firewall and at the hub, router, or workstation.
- Make sure that power is turned on to the connected hub, router, or workstation.
- Be sure that you are using the correct cables.

  When connecting the VPN firewall's WAN ports to one or two devices that provide the Internet connections, use the cables that are supplied with the devices. These cables could be standard straight-through Ethernet cables or Ethernet crossover cables.

Troubleshoot the Web Management Interface

If you cannot access the VPN firewall's web management interface from a computer on your local network, check the following:

- Check the Ethernet connection between the computer and the VPN firewall.

  For more information, see *LAN or WAN Port LEDs Not On* on page 388.

- If your computer's IP address is shown as 169.254.x.x: Windows and Mac operating systems generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the VPN firewall and reboot your computer.
- If your VPN firewall's IP address was changed and you do not know the current IP address, reset the VPN firewall's configuration to factory default settings.

  This sets the VPN firewall's IP address to **192.168.1.1**. For more information, see *Restore the Default Configuration and Password* on page 397.

  Tip: If you do not want to revert to the factory default settings and lose your configuration settings, you can reboot the VPN firewall and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the VPN firewall's LAN interface address.

- Make sure that Java, JavaScript, or ActiveX is enabled in your browser.

  If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.

- Try quitting the browser and launching it again.
- Clear the browser's cache.
- Make sure that you are using the correct login information.

The factory default login name is admin, and the password is password. Make sure that Caps Lock is off when entering this information.

Note: To be able to configure the VPN firewall, your computer's IP address does not need to be on the same subnet as the VPN firewall.

If the VPN firewall does not save changes you made in the web management interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser.

  The changes 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 31.

- If the computer is configured correctly but still not working, ensure that the VPN firewall is connected and turned on.

  Connect to the web management interface and check the VPN firewall's settings. If you cannot connect to the VPN firewall, see *Troubleshoot the Web Management Interface* on page 388.

- If the VPN firewall is configured correctly, check your Internet connection (for example, your modem, dish, or router) to make sure that it is working correctly.

Troubleshoot the ISP Connection

If your VPN firewall is unable to access the Internet, first determine whether the VPN firewall is able to obtain a WAN IP address from the ISP. Unless you were assigned a static IP address, your VPN firewall requests an IP address from the ISP. You can determine whether the request was successful using the web management interface.

➢ **To check the WAN IP address:**

1. Log in to the unit:

   a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

      The NETGEAR Configuration Manager Login screen displays.

   b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

      Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

   c. Click the **Login** button.

      The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

2. Select **Network Configuration > WAN Settings > Broadband ISP Settings**.

   The Broadband ISP Settings screen for IPv4 displays.

3. Take one of the following actions:
   - **For IPv4**. Click the **Broadband Status** option arrow. The Connection Status pop-up screen for IPv4 displays.
   - **For IPv6**:

     a. In the upper right of the screen, select the **IPv6** radio button.

        The ISP Broadband Settings screen displays the IPv6 settings.

     b. Click the **Status** option arrow.

        The Connection Status pop-up screen for IPv6 displays.

4. Check that an IP address is shown for the WAN port.

   If an IP address with zeros only is shown, or if no IP address is shown, the VPN firewall did not obtain an IP address from your ISP, or for IPv6, did not obtain or generate an IP address.

If your VPN firewall is unable to obtain an IP address from the ISP, you might need to force your modem, dish, or router to recognize your new VPN firewall by performing the following procedure:

1. Turn off the power to the modem, dish, or router.
2. Turn off the power to your VPN firewall.
3. Wait 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 occurred, turn on the power to your VPN firewall.

If your VPN firewall is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your ISP might require a login program.

  For IPv4 connections, ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.

- For IPv4 connections, if your ISP requires a login, the login name and password might be incorrectly set.
- 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 need to enter additional information. For more information, see *Manually Configure an IPv4 Internet Connection* on page 31.
- 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 are using a new network device, and ask them to use the VPN firewall's MAC address.
  - Configure your VPN firewall to spoof your computer's MAC address. You can do this in the Router's MAC Address section on the Broadband Advanced Options screen. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 52.

If your VPN firewall can obtain an IP address, but an attached computer is unable to load any web pages from the Internet, it might be for one of the following reasons:

- 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.
- The VPN firewall might not be configured as the TCP/IP gateway on your computer.

Troubleshooting the IPv6 Connection

If you experience difficulty connecting over an IPv6 connection, the VPN firewall or the computer from which you are trying to connect to the VPN firewall might not be configured correctly:

Check the VPN firewall:

- By default, the VPN firewall is set to IPv4-only mode.

  Make sure that the VPN firewall is set to IPv4/IPv6 mode. For more information, see *Configure the IPv6 Routing Mode* on page 39.
- Make sure that the ISP settings are correct.

  For more information, see *Configure a Static IPv6 Internet Connection* on page 42. The VPN firewall cannot receive a valid IPv6 address if the Internet connection is not correctly configured.

- Make sure that the VPN firewall can provide IPv6 addresses to the computers on the LAN.

  For more information, see *Manage the IPv6 LAN* on page 78. 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:

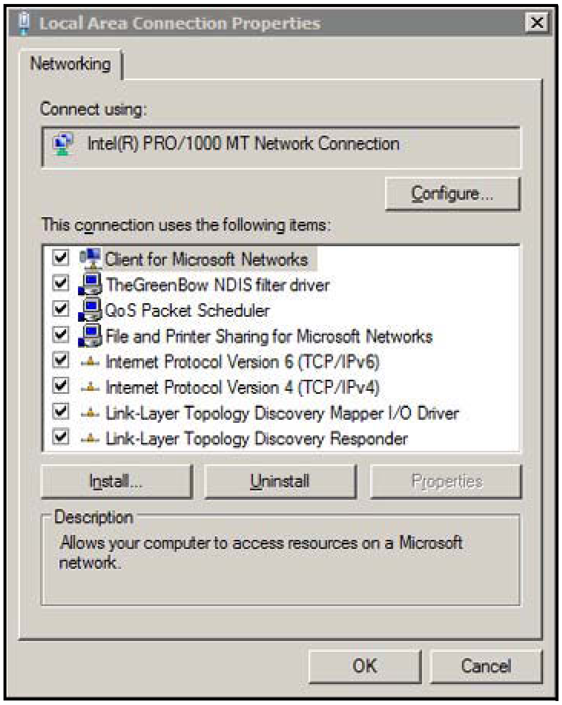
  - Windows 7, all 32-bit and 64-bit versions
  - Windows Vista, all 32-bit and 64-bit versions
  - Windows XP Professional SP3 (32-bit and 64-bit)
  - Windows Server 2008, all versions
  - Windows Server 2008 R2, all versions
  - Windows Server 2003, all versions
  - Windows Server 2003 R2, all versions
  - Linux and other UNIX-based systems with a correctly configured kernel
  - MAC OS X
- Make sure that IPv6 is enabled on the computer.

  On a computer that runs a Windows-based operating system, do the following (note that the steps might differ on the various Windows operating systems):

  a. Open the Network Connections screen or the Network and Sharing Center screen.

  For example, on the Windows taskbar, click **Start**, select **Control Panel**, and select **Network Connections**.

b. Click or double-click **Local Area Connection** for the connection to the VPN firewall.



Connect using:
Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ TheGreenBow NDIS filter driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description
Allows your computer to access resources on a Microsoft network.

c. Make sure that Internet Protocol Version 6 (TCP/IPv6) displays.

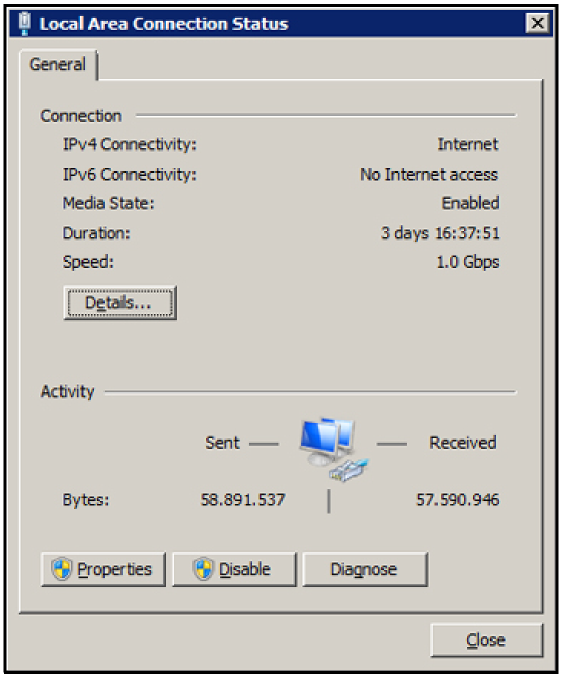
- Make sure that the computer is using an IPv6 address.

  If the computer uses a link-local address only, it cannot reach the VPN firewall or the Internet. On a computer that runs a Windows-based operating system, do the following (the steps might differ on the various Windows operating systems):

a. Open the Network Connections screen or the Network and Sharing Center screen. For example, on the Windows taskbar, click **Start**, select **Control Panel**, and select **Network Connections**.

b. Click or double-click **Local Area Connection** for the connection to the VPN firewall.

c. Click or double-click **View status of this connection**.



Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	3 days 16:37:51
Speed:	1.0 Gbps

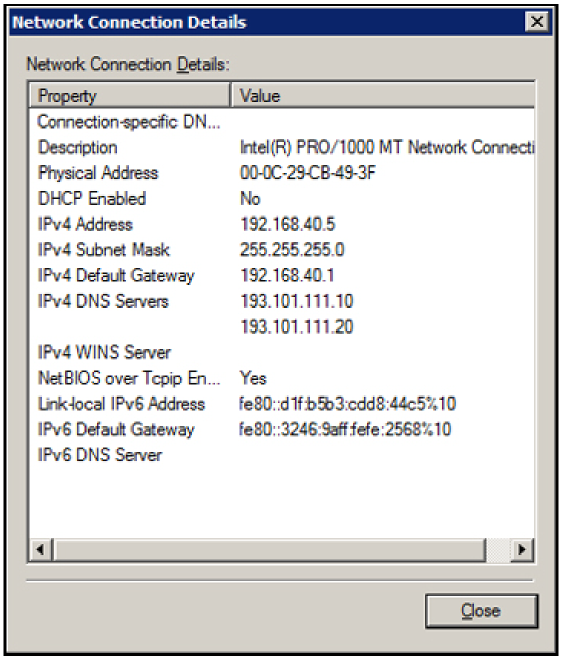
Activity

	Sent	Received
Bytes:	58.891.537	57.590.946

d. Make sure that Internet access shows for the IPv6 connection.

The previous figure shows that the device is not connected to the Internet.

e. Click the **Details** button.



Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/1000 MT Network Connecti
Physical Address	00-0C-29-CB-49-3F
DHCP Enabled	No
IPv4 Address	192.168.40.5
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.40.1
IPv4 DNS Servers	193.101.111.10 193.101.111.20
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::d1f:b5b3:cdd8:44c5%10
IPv6 Default Gateway	fe80::3246:9aff:fefe:2568%10
IPv6 DNS Server	

f. Make sure that an IPv6 address shows.

The previous figure does not show an IPv6 address for the computer but only a link-local IPv6 address and an IPv6 default gateway address, both of which start, in this case, with fe80.

Troubleshoot a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer or workstation.

This section discussion the following topics:

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

Test the LAN Path to Your VPN Firewall

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

➤ **To ping the VPN firewall from a computer running Windows 95 or later:**

1. From the Windows taskbar, click **Start** and select **Run**.
2. In the field provided, type **`ping`** followed by the IP address of the VPN firewall.

   For example:

   ```
   ping 192.168.1.1
   ```
3. Click the **OK** button. A message similar to the following displays:

   ```
   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, it might be for one of the following reasons:

   - 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 388.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and VPN firewall.

- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
  - Verify that the IP address for your VPN firewall and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows Run dialog box, type

```
ping -n 10 <IP address>
```

in which `<IP address>` is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in *Test the LAN Path to Your VPN Firewall* on page 395 are displayed. If you do not receive replies, do the following:

- Check that your computer is using the IP address of your VPN firewall 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 need to enter additional information. For more information, see *Manually Configure an IPv4 Internet Connection* on page 31.
- 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 this is the case, you must configure your VPN firewall to *clone* or *spoof* the MAC address from the authorized computer. You can do this in the Router's MAC Address section on the WAN Advanced Options screen. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 52.

Restore the Default Configuration and Password

To reset the VPN firewall to the original factory default settings, you can use one of the following two methods:

- Press the factory default **Reset** button on the rear panel of the VPN firewall and hold the button for about eight seconds until the Test LED turns on and begins to blink (about 30 seconds).

  For information about how to locate the **Reset** button, see *Rear Panel* on page 16. To restore the factory default settings when you do not know the administration password or IP address, you must use the factory default **Reset** button method.

- Use the **Default** button on the Settings Backup and Firmware Upgrade screen:

  1. Log in to the unit:

     a. In the address field of any of the qualified web browsers, enter **https://192.168.1.1**.

     The NETGEAR Configuration Manager Login screen displays.

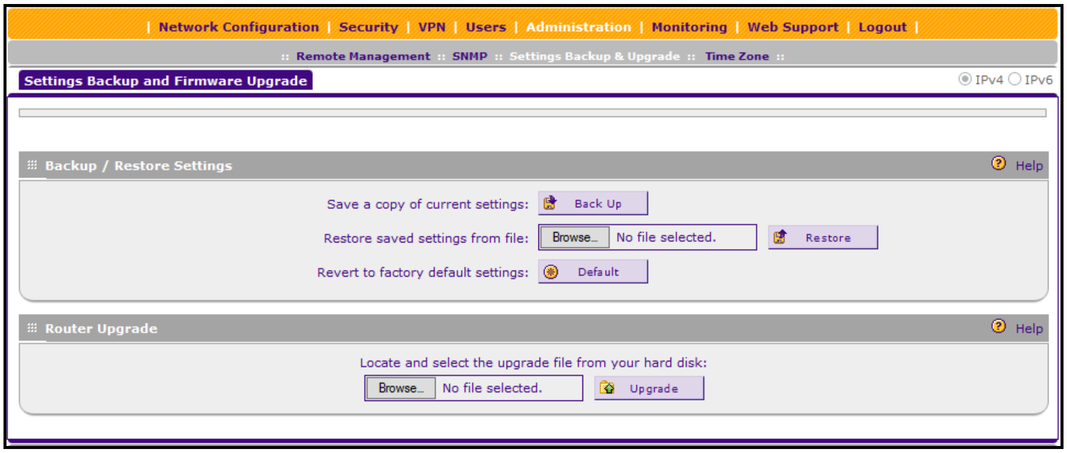
     b. In the **Username** field, enter **admin** and in the **Password / Passcode** field, enter **password**.

     Use lowercase letters. If you changed the password, enter your personalized password. Leave the domain as it is (geardomain).

     c. Click the **Login** button.

     The Router Status screen displays. After five minutes of inactivity, which is the default login time-out, you are automatically logged out.

  2. Select **Administration > Settings Backup & Upgrade**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Settings Backup and Firmware Upgrade
● IPv4 ○ IPv6
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
No file selected.
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
No file selected.
Upgrade

  3. Click the **Default** button.

  The VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible, or a status message with a counter might show the number of seconds left until the reboot process is complete.

The reboot process takes about 165 seconds. The reboot process is complete when the Test LED on the front panel goes off.

WARNING:

When you press the hardware factory default Reset button or click the software Default button, the VPN firewall settings are erased. All firewall rules, VPN policies, LAN and WAN settings, and other settings are lost. Back up your settings if you intend to use them.

Note: After you reboot with factory default settings, the VPN firewall's password is **password**, and the LAN IPv4 address is **192.168.1.1**.

Address Problems with Date and Time

The System Date & Time screen displays the current date and time of day (see *Configure Date and Time Service* on page 345). The VPN firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day.

Problems with the date and time function can include the following:

- Date shown is January 1, 2000.

  Cause: The VPN firewall did not yet successfully reach a network time server. Check that your Internet access settings are configured correctly. If you just completed configuring the VPN firewall, wait at least five minutes, and check the date and time again.

- Time is off by one hour.

  Cause: The VPN firewall does not automatically sense daylight saving time. Go to the Time Zone screen (**Administration > Time Zone**), and select or clear the **Automatically Adjust for Daylight Savings Time** check box.

Access the Knowledge Base and Documentation

➢ **To access NETGEAR's knowledge base for the VPN firewall:**

Select **Web Support > Knowledgebase**.

➢ **To access NETGEAR's documentation library for your VPN firewall model:**

Select **Web Support > Documentation**.

A
Default Settings and Technical Specifications

This appendix provides the default settings and the physical and technical specifications of the VPN firewall in the following sections:

- *Factory Default Settings*
- *Physical and Technical Specifications*

Factory Default Settings

You can use the factory default **Reset** button on the rear panel to reset all settings to their factory defaults. This is called a hard reset (for more information, see *Revert to Factory Default Settings* on page 341).

To perform a hard reset, press and hold the factory default **Reset** button for approximately eight seconds (until the Test LED blinks rapidly). The VPN firewall returns to the factory configuration settings that are shown in the following table.

Pressing the factory default **Reset** button for a shorter period causes the VPN firewall to reboot.

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

Table 86. 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 VPN firewall
	WAN MTU size	1500 bytes 1492 bytes for PPPoE connections
	Port speed	AutoSense
	Dynamic DNS for IPv4	Disabled

Table 86. 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 86. 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 86. 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
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)
	Lifetime	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 86. 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)
	Lifetime	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
User, group, and domain settings		
	default domain	geardomain
	default group	geardomain
	default users, default passwords	admin, password
		guest, password

Table 86. 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

Physical and Technical Specifications

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

Table 87. 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	12 VDC @ 1A output
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)

Table 87. VPN firewall physical and technical specifications (continued)

Feature		Specification
Environmental specifications		
	Operating temperatures	0° to 40°C
		32° to 104°F
	Storage temperatures	–20° to 70°C
		–4° to 158°F
	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 *Compliance* on page 2.	
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 VPN firewall:

Table 88. 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
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

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 are now 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 recognized the need to go beyond the traditional authentication process by introducing and requiring additional factors in the authentication process. NETGEAR also recognizes the need to provide more than just a firewall to protect the networks. NETGEAR implements 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 VPN firewall products.
- **Proven regulatory compliance**. Two-factor authentication is 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. Several factors are used to validate the users to make sure that you are who you say you are. These factors are as follows:

- Something you know—for example, your password or your PIN.
- Something you possess—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 possess. This security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you possess. A common example of two-factor authentication is a bank (ATM) card that was issued by a bank institute:

- The PIN to access your account is *something you know.*
- The ATM card is *something you possess.*

You must use 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 implements 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 VPN firewall products.

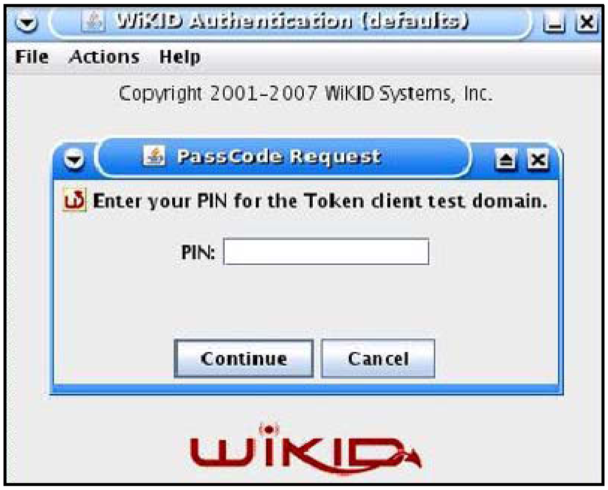
The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), which is time-synchronized with the authentication server, is generated and sent to the user after the validity of a user credential is confirmed by the server.

The request-response architecture is capable of self-service initialization by end users, dramatically reducing implementation and maintenance costs.

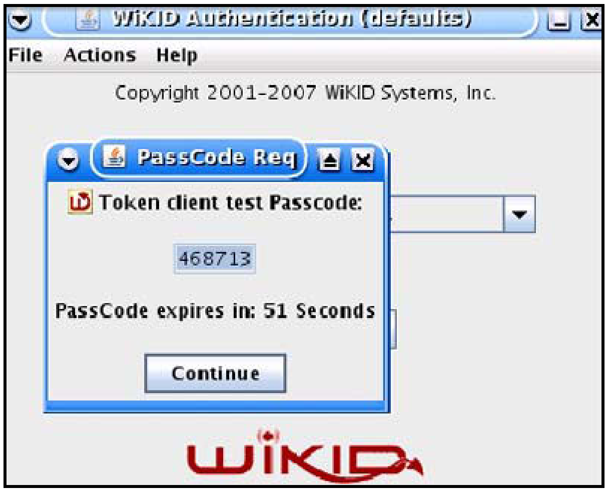
Here is an example of how WiKID works:

➢ **To use WiKID (for end users):**

1. Launch the WiKID token software, enter the PIN that was provided (*something the user knows*), and click the **Continue** button to receive the OTP from the WiKID authentication server:


WiKID Authentication (defaults)
File
Actions
Help
Copyright 2001-2007 WiKID Systems, Inc.
PassCode Request
Enter your PIN for the Token client test domain.
PIN:
Continue
Cancel
WiKID

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


WiKID Authentication (defaults)
File Actions Help
Copyright 2001-2007 WiKID Systems, Inc.
PassCode Req
Continue
WiKID

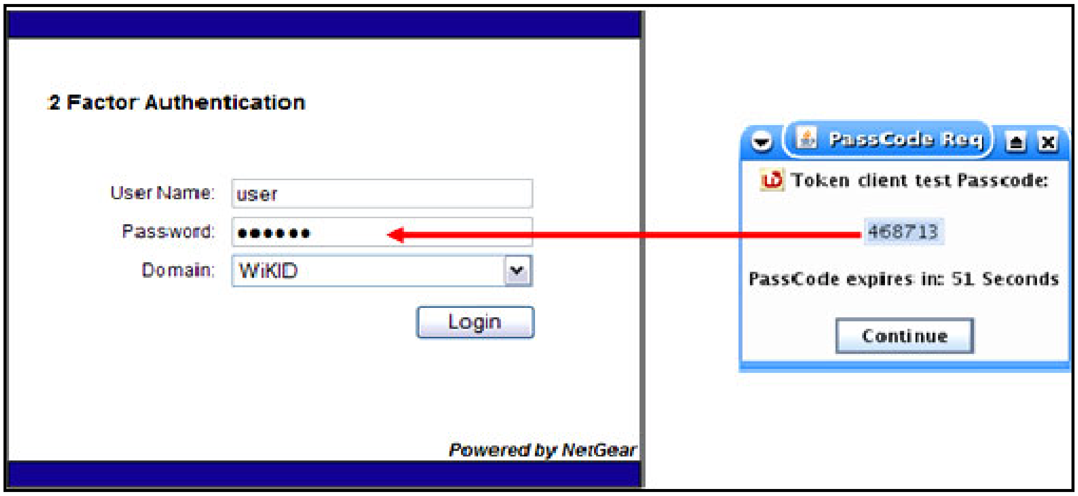
Token client test Passcode:

468713

PassCode expires in: 51 Seconds

Note: The one-time passcode is time-synchronized to the authentication server so that the OTP can be used only once and must be used before the expiration time. If a user does not use this passcode before it expires, the user must 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.



User Name: user

Password: ●●●●●●

Domain: WiKID

Token client test Passcode:

468713

PassCode expires in: 51 Seconds

Index